



Cybersecurity Industry Market Analysis

CIMA

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:



This study was carried out for the European Commission by



This document is the final report published in November 2018 of the Cybersecurity Industry Market Analysis (CIMA) by PwC and LSEC – Leaders in Security.

Internal identification

Contract number: 30-CE-0720593/00-72 CS 000180

SMART number 2015/0042

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-76-08859-2

doi:10.2759/018751

© European Union, 2019. All rights reserved. Certain parts are licensed under conditions to the EU.

This page has been intentionally left blank

Cybersecurity Industry Market Analysis

CIMA

July 2019

Introduction

This document is the final report published in November 2018 of the Cybersecurity Industry Market Analysis (CIMA) performed by LSEC in collaboration with PwC in 2017 and 2018 on market data of 2016, and contains information about:

- The European Cybersecurity market and its comparison with other relevant markets.
- The Cybersecurity products and services catalogue and an analysis of what products and services require attention taking into account the NIS directive, the existing gaps in the market and the upcoming trends and threats.
- The topology of the European Cybersecurity market including the sector's segmentation and the market segmentation. It also includes an analysis of the demand patterns and the geographical market fragmentation.
- The intra and extra Europe market flows and the main barriers providers find when selling their products and services inside and outside the European market.
- The strengths, weaknesses, opportunities and threats of the European Cybersecurity market and also the main findings of this study.

This is the final report of the study, on the basis of factual data and a proven methodology. Datasets are complex and wide and are still subject to further interpretation and analysis.

This report was developed on the basis of earlier drafts, discussions and debates from earlier results, in trying to better understand Cybersecurity industry market dynamics. The report seeks to support policy-making by the European Commission DG CONNECT in the area of cybersecurity research and industrial policy.

Record of Modifications					
Version	Description [or description of changes]	Author	Date of creation	Approved by	Date of Approval
1.9	Initial update of the 2016 document	PwC and LSEC partnership	30.06.2017	US	03.07.2017
2	Update draft v2	PwC and LSEC	13.07.2017	DV	26.07.2017
2.1	Revision of updates and comments	PwC and LSEC	15.08.2017	US	27.08.2017
2.2	Data Additions	PwC and LSEC	15.09.2017	US	19.09.2017
2.3	Workshop Methodology	PwC and LSEC	19.09.2017	US	22.09.2017
3.0	Revision of methodology and additional analysis	PwC and LSEC	25.09.2017	DV	27.09.2017
3.1	Integration of Debates	PwC and LSEC	01.10.2017	US	06.10.2017
3.2	Adding Analysis results	PwC and LSEC	08.10.2017	US	10.10.2017
3.3	Reviewing Taxonomy	PwC and LSEC	16.10.2017	EC SO	16.10.2017
3.4	Adding Workshop Results	PwC and LSEC	26.10.2017	US	28.10.2017
4.0	Final Draft	PwC and LSEC	07.11.2017	US	15.11.2017
5.0	Final Draft small changes	PwC and LSEC	29.11.2017	US	07.12.2017
5.1	Final Draft revision comments	LSEC based upon EC comments	17.12.2017	RC/CP	20.12.2017
5.2	New Exec. Summary and other revisions	LSEC based upon EC comments	01.03.2018	NA/RC/C P/US	10.08.2018
6.	Final	LSEC, PwC based upon EC comments	14.08.2018	ALL	23.08.2018
6.1	Revision on Chapter 9, 10, 11	LSEC, PwC based upon EC comments	10.09.2018	ALL	15.09.2018
6.2	Revision minor changes all chapters	LSEC, PwC based upon EC comments	25.10.2018	ALL	29.10.2018
6.3	Final quality check and removal of overhead	LSEC, PwC based upon EC comments	03.11.2018	ALL	07.11.2018
6.4	Final review	EC	09.11.2018	EC	15.11.2018

Distribution List	
Name	Area
Florent FREDERIX	DG CONNECT
James CAFFREY	DG CONNECT
Jakub BORATYNSKI	DG CONNECT
Nineta POLEMI	DG CONNECT
Rosa BARCELO	DG CONNECT
Malgorzata FIGWER	DG CONNECT
Gemma CAROLILLO	DG CONNECT
Rafael TESORO-CARRETERO	DG CONNECT
Martin SPAET	DG CONNECT
Martin UBELHOR	DG CONNECT
Jean-Francois JUNGER	DG CONNECT
Miguel GONZALEZ-SANCHO-BODERO	DG CONNECT
Aristotelis TZAFALIAS	DG CONNECT
Despina SPANOU	DG CONNECT
Konstantinos NTANTINOS	DG CONNECT

Disclaimer

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

The research was based upon 2016 trade data collected from over 900 sources, analysed mainly from April through November 2017 and validated in different industry workshops in different European Member States in the same period. Please do take into consideration that all data has been copyright protected and should not be used publicly without prior written consent of the author (cima2018@lsec.eu). We welcome any additional comments and findings, that could help us elaborate and deepen the further discussion and recommendations.

This report was submitted for final review in August 2018, accepted in October 2018 following further changes, and published in November 2018.

Abstract [EN]

This Cybersecurity Industry Market Analysis (CIMA) report documents the market research of the European Cybersecurity industry and its comparison with other relevant markets. PwC and LSEC – Leaders In Security performed the study for the European Commission in 2017 – 2018.

The report results from a quantitative research for gathering, categorising and analysing the Cybersecurity Industry Market data of 2016, by applying a big data approach to extracting economic and market values from over 900, mainly transactional data sources. Its methodology considers all relevant Cybersecurity sales, including products and services that are distributed and resold by system integrators, and represents genuine economic activities. The study considers companies that solely provide Cybersecurity products and services; companies that (amongst other activities) provide Cybersecurity products and services; and companies that provide products and services that form part of the Cybersecurity supply/value chain. It was challenged by teams of experts in different Member States during interactive workshops detailing market insights.

The report builds a Cybersecurity products and services catalogue and analyses what products and services require attention taking into account the Network Information Security directive, the existing gaps in the market and the upcoming trends and threats.

It documents the strengths of the European Cybersecurity market in supply and demand, including the sector's segmentation, vertical market insights and comprises an analysis of the demand patterns per category and the geographical market fragmentation. Furthermore, the intra and extra European market flows and the main barriers that providers find when selling their products and services inside and outside the European market are documented.

The report concludes with a wrap-up of the main findings of the study and an overview of the strengths, weaknesses, opportunities and threats of the European Cybersecurity market.

Abstract [FR]

Le présent rapport d'analyse du marché de l'industrie de la cybersécurité (CIMA - Cybersecurity Industry Market Analysis) reprend les études de marché de l'industrie européenne de la cybersécurité et les compare avec d'autres marchés pertinents. PwC et LSEC – Leaders in Security ont réalisé cette étude pour la Commission européenne en 2017 – 2018.

Le rapport résulte en une recherche quantitative pour le rassemblement, le classement et l'analyse des données du marché de l'industrie de la cybersécurité en 2016, en appliquant une approche big data pour extraire les valeurs économiques et les valeurs du marché de plus de 900 sources de données, principalement transactionnelles. La méthodologie de l'étude prend en compte toutes les ventes pertinentes de produits de cybersécurité, y compris les produits et services qui sont distribués et revendus par les intégrateurs de systèmes, et représente de véritables activités économiques. L'étude prend en compte les sociétés qui fournissent uniquement des produits et services de cybersécurité, les sociétés qui fournissent des produits et services de cybersécurité (et qui effectuent d'autres activités) et les sociétés qui fournissent des produits et services faisant partie de la chaîne d'approvisionnement/de valeur du secteur de la cybersécurité.

Le rapport établit un catalogue de produits et services de cybersécurité et analyse les produits et services qui nécessitent une attention particulière en tenant compte de la directive sur la sécurité des réseaux et des systèmes d'information, des lacunes existantes sur le marché et des tendances et menaces à venir.

Il reprend les forces du marché européen de la cybersécurité en termes d'offre et de demande (notamment la segmentation du secteur et les perspectives verticales du marché) et comprend une analyse des tendances des demandes par catégorie et de la fragmentation géographique du marché. En outre, le rapport reprend également les flux de marché dans et en dehors de l'Europe et les principaux obstacles rencontrés par les fournisseurs lors de la vente de leurs produits et services au sein du marché européen et en dehors.

Le rapport conclut par un résumé des principales conclusions de l'étude et un aperçu des forces, faiblesses, opportunités et menaces du marché européen de la cybersécurité.

Abstract [DE]

Dieser Bericht über die Marktanalyse der Cyber-Sicherheitsbranche (CIMA) dokumentiert die Marktforschung der europäischen Cyber-Sicherheitsbranche und ihren Vergleich mit anderen entsprechenden Märkten. PwC und LSEC – Leaders In Security führten die Studie 2017–2018 für die Europäische Kommission durch.

Der Bericht beruht auf quantitativer Marktforschung zur Erfassung, Kategorisierung und Analyse der Marktdaten 2016 der Cyber-Sicherheitsbranche im Form eines Big-Data-Ansatzes, mit dem Wirtschafts- und Marktzahlen aus mehr als 900 Quellen, vor allem Transaktionsdatenquellen, gewonnen wurden. Diese Methodik berücksichtigt alle entsprechenden Cybersicherheitsverkäufe, darunter Produkte und Dienstleistungen, die von Systemintegratoren vertrieben und weiterverkauft werden, und die tatsächliche wirtschaftliche Aktivitäten abbilden. Die Studie berücksichtigt Unternehmen, die ausschließlich Cyber-Sicherheitsprodukte und -dienstleistungen anbieten, Unternehmen die (neben anderen Aktivitäten) Cyber-Sicherheitsprodukte und -dienstleistungen anbieten sowie Unternehmen, die Produkte und Dienstleistungen anbieten, die Teil der Liefer- oder Wertschöpfungskette für Cyber-Sicherheit sind.

Der Bericht enthält einen Katalog von Cyber-Sicherheitsprodukten und -dienstleistungen und analysiert unter Berücksichtigung der Richtlinie über die Sicherheit von Netzen und Informationssystemen, der vorhandenen Lücken auf dem Markt und der sich abzeichnenden Trends und Bedrohungen, welche Produkte und Dienstleistungen Aufmerksamkeit benötigen.

Er dokumentiert die Stärken des europäischen Cyber-Sicherheitsmarkts bei Angebot und Nachfrage sowie die Segmentierung der Branche und vertikale Markteinblicke. Außerdem enthält er eine Analyse der Nachfragemuster nach Kategorie und die geografische Marktfragmentierung. Darüber hinaus werden die Marktbewegungen innerhalb und außerhalb des Europäischen Marktes sowie die wichtigsten Hindernisse dokumentiert, vor denen Anbieter stehen, wenn sie ihre Produkte und Dienstleistungen innerhalb und außerhalb von Europa vertreiben.

Der Bericht schließt mit einer Zusammenfassung der Hauptergebnisse der Studie und einem Überblick der Stärken, Schwächen, Chancen und Bedrohungen des europäischen Cyber-Sicherheitsmarktes.

Glossaries

Glossary 1 : Sector and Category Definition

The Cybersecurity sector definition below includes short descriptions of each sub-sector. These are described in more detail within the report and at Appendix H.

Cybersecurity Sub- sectors	Description
Anti- Malware	Includes development and supply of anti- malware, anti- spam, antivirus/ worm and forensic software/ services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Application Security	Includes development and supply of application code security/ patch management/ content filtering & monitoring/ vulnerability assessment software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Business Continuity	Includes development and supply of business continuity & recovery/ IT & Cyber forensics/ computer forensics software and services (manual and automated) for corporate/ small business/ public/ cloud/ smart communications and other networks.
Cyber Consultancy	Includes consulting for cyber audit/ insider threat/ security policy/ risk & compliance/ training & awareness/ legislation, standards and strategy for threat avoidance, threat detection and compliance. Also includes consultancy conducted in support of activities within the other twelve sub-sectors of Cybersecurity.
Encryption	Includes development and supply of digital signature/ digital certificate/ detection/ prevention software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Cyber Insurance	First Party Insurance includes loss or damage to digital assets, business interruption from network downtime, cyber extortion, reputational damage and theft of money or digital assets. Third Party Cyber Insurance includes security and privacy breaches, investigation of privacy breach, third party breach notification, multi-media liability and loss of third party data.
Identity & Access	Includes development and supply of access management/ intrusion & anomaly prevention/ messaging security software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Infrastructure	Includes development and supply of infrastructure monitoring/ intrusion detection/ firewall security/ data management/ network security/ infrastructure resilience testing/ security applications/ web services

	security/ enterprise risk assessment for corporate/ small business/ public/ cloud/ smart communications and other networks.
Mobile	Includes development and supply of mobile endpoint security/ mobile device management/ VPN/ Wireless security software and services (local/ remote access) for corporate/ small business/ public/ cloud/ smart communications and other networks.
Outsourced/ Managed Services	Includes development and supply of cyber threat/ internet platform/ systems access/ mobile systems/ network & hub/ systems integration/ cloud services for corporate/ small business/ public/ cloud/ smart communications and other networks. Also includes the management of services that are specific to the other twelve sub-sectors of Cybersecurity.
Situational Awareness	Includes development and supply of high & low level situational awareness/ internal & external cyber threat intelligence/ proactive cyber surveillance/ social media monitoring/ darkweb investigations software and services (both automated and manual) for corporate/ small business/ public/ cloud/ smart communications and other networks.
System Recovery & Data Cleansing	Includes development and supply of system recovery/ data recovery/ data cleansing/ data validation & verification software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Training & Education	Includes training and education activities carried out across all twelve sub-sectors of Cybersecurity for corporate/ small business/ public/ cloud/ smart communications and other networks.

Glossary 2 : Metrics

This report applies a range of economic and market measures to Cybersecurity products and services. Each measure is defined briefly below and in the research methodology.

Measures	Description
Sales (m EUR)	Measure of economic activity by identified companies and their supply chain within a defined country, based upon where the economic activity is delivered from rather than where it is reported.
Employment	Measure of the level of employment, in Whole Time Equivalents (WTEs), across core and supply chain companies involved in delivering sector products/ services.
Companies	Measure of the total number of companies in a country that are either core to the delivery of sector products & services or form an integral part of the supply/ value chain.
Exports (m EUR)	Measure of goods and services that travel from a source country to another country that may either be complete or become incorporated into a new product or service. Exports are measured globally and individually for the top 96 economies, including all EU countries.
Imports (m EUR)	Measure of goods and services that originate from sources outside of the country that may either be complete or become incorporated into a new product or service. Imports are measured globally and individually for the top 96 economies, including all EU countries.
Market Growth	Historical and forecast measure of the annual percentage rate of change in sales. Currently, historical growth trends are recorded for sales, companies, employment, imports and exports, but forecast growth is only applied to sales and exports.
New Product Sales (m EUR)	The value of new products or services entering the market on an annual basis. This gives an indication of the rate of new technology adoption and the introduction of new concepts and provides a better measure of market size for start-up businesses.
New Product Sales as % of Sales	Derived from the above, this provides an indication of the flexibility of the market and its relative demand for new products/ services compared with other sector activities i.e. a measure of market- driven innovation.
New Products per annum	This is the number of new products or services introduced on average by businesses on an annual basis. In conjunction with other "Product" measures, this provides a "proxy" measure for market- driven innovation.
Spend on R&D as a % of Sales	A measure of the budget expended by businesses on research and development on an annual basis, expressed as a percentage of sales. This is a "push" measure for business innovation that we often compare with "pull" measures like % of new product.

GDP (m EUR)	National Gross Domestic Product (GDP) is a common measure of global/national economic performance and is used in this report to contextualise the size of the Cybersecurity sector.
No of Sources	Total number of data sources used to generate the values for each product/service line in the data set. A list of over 800 sources are included at Appendix I.
Confidence Levels	Confidence levels are a mathematical function of the spread of values across the range of sources that we include in our analysis. Confidence levels are applied to sales, employment, growth and exports. Levels vary by activity, geography and by forecast year.
Domestic Market (m EUR)	A derived measure of the domestic market (i.e. consumption) within a country, based upon a formula of Sales - Exports + Imports.
Sales as a % of GDP	A derived measure comparing sector sales with country GDP. This provides a metric for the relative importance of the sector to each EU country.
% Share of Global Market	A measure derived from comparing country sales with global sales.
Global Share of Exports %	A measure derived from comparing country exports with global exports.
Market Share by Country %	Value of national exports to a specific country compared with total exports to that country.

Glossary 3 : End-User Markets

A brief description of vertical or end- user markets for Cybersecurity products and services.

Vertical Market	Description
Chemicals & Pharma Processing	Includes all aspects of chemicals and pharmaceuticals processing including both batch and continuous production. Examples are drugs, paint, solvents, cleaning products, cosmetics etc.
Commercial Facilities	Includes office and operational facilities for all commercial sectors. Examples are call centres, sorting centres, administrative centres, head office functions, R&D centres and laboratories.
Communications	Includes telephone exchanges, mobile and static phone engineering, land line maintenance and installation, transmitter maintenance and installation, WIFI and blue tooth systems and development, networking systems and consultancy.
Manufacturing & Assembly	Includes all aspects of manufacture, both batch and continuous by both hand assembly and automated systems. Examples are automotive, white goods, brown goods, toys, computers, medical instruments etc.
Emergency Services	Includes, fire, ambulance, police and all civil emergency services such as flood abatement and earth quake rapid response.
Defence Industries	Includes security aspects only of the defence sector that are not covered by the defence sector definition
Construction	Includes home building, commercial buildings, civil engineering, design and architectural design, planning, project management, highways etc.
Financial Services	Includes banking, insurance, fund management, futures, private equity, trading, analysis and reporting, trading floor operations, etc.
Food and Agriculture	Includes food processing both batch and inline process, food packaging and refrigeration, the crop growing supply chain, through to retail sales. The sector includes both time sensitive and non-time- sensitive products and the operational chains of supply.
Energy	Includes electricity, gas and all forms of generation including coal gas, natural gas, fracking, bio-gas and other bio fuels, wind and tidal energy, photovoltaic energy, solar energy, nuclear energy,
Government Facilities	Includes government buildings and facilities in the public sector. Facilities include storage facilities, laboratory facilities, training establishments etc.
Healthcare and Public Health	Includes hospitals and mobile healthcare capabilities, not included in the emergency services. This sector also includes Doctors surgeries and other healthcare establishments in the network of supply. In addition, the sector

	includes pharmacies, alternative health establishments, home care networks and other specialist health units in both the public and private sectors.
Information Technology	Includes software development, design and development of networking equipment (not covered in manufacturing). Outsourced computing services and centres, cloud provision, mobile computing and data management, consultancy and systems implementation.
Education Sector	Includes schools and universities as well as specialist training centres, outward bound centres, distance- learning establishments, early learning establishments, the generation and production of learning materials, educational publishing, and consultancy.
Transportation & Logistics	This sector includes transport vehicles and networks, logistics operations and planning, warehousing and distribution centres, ERP (enterprise requirements planning) and DRP (distribution requirements planning) systems and implementation, passenger transport and goods transport by road, rail, sea and air for both the public and private sectors.
Water and Wastewater Utilities	This sector includes utilities of potable water supply, sewage treatment, potable, grey and black water distribution and management, water treatment facilities, and infield engineering.
Other	"Other" category includes all consumer related sales for the vertical markets listed above and for other vertical markets (not listed) that are not considered critical, most retail activity and a proportion of transactions that are either too small to identify or that (for commercial or other reasons) are not traceable to any of the vertical markets.

Index

<u>GLOSSARIES</u>	11
Glossary 1 : Sector and Category Definition	11
Glossary 2 : Metrics	13
Glossary 3 : End-User Markets	15
<u>INDEX</u>	17
<u>TABLE OF FIGURES</u>	20
<u>TABLE OF TABLES</u>	22
<u>1 EXECUTIVE SUMMARY</u>	24
<u>2 BACKGROUND</u>	35
<u>3 CONTEXT AND CONSIDERATIONS</u>	36
<u>4 ABOUT THE AUTHORS</u>	39
<u>5 INTRODUCTION TO THE CIMA REPORT : SCOPE, CONSIDERATIONS, SOURCES, STRUCTURE, TARGET AUDIENCE</u>	40
5.1 <u>Scope of the study</u>	40
5.2 <u>Main considerations</u>	42
5.3 <u>Sources</u>	42
5.4 <u>Document structure</u>	43
5.5 <u>Intended audience for this document</u>	44
<u>6 QUANTITATIVE CYBERSECURITY RESEARCH</u>	45
6.1 <u>Defining the Cybersecurity Market, Taxonomy and Scope</u>	45
6.2 <u>Methodology</u>	46
6.3 <u>Cybersecurity Industry Models</u>	48
<u>7 GLOBAL CYBERSECURITY MARKET</u>	50
7.1 <u>Introduction</u>	50
7.2 <u>Global Cybersecurity Key Metrics</u>	50
7.3 <u>Global Cybersecurity by Sub-sector</u>	53
7.4 <u>Global Cybersecurity Sales by Geography</u>	57
<u>8 EU CYBERSECURITY MARKET</u>	63
8.1 <u>Introduction</u>	63
8.2 <u>EU Cybersecurity Key Metrics</u>	63
8.3 <u>EU Cybersecurity by Sub-sector</u>	66
8.4 <u>EU Cybersecurity by Country</u>	73
8.5 <u>EU Cybersecurity Supply</u>	86
8.6 <u>EU Cybersecurity End- Users</u>	94
8.7 <u>EU Cybersecurity Imports</u>	99
8.8 <u>EU Cybersecurity Exports</u>	107
<u>9 EU COMPETITIVENESS</u>	115
9.1 <u>Introduction</u>	115

9.2	<u>Trade Flow Analysis</u>	115
9.3	<u>Market Share Analysis</u>	125
9.4	<u>EU Supplier Analysis</u>	130
10	<u>WORKSHOPS</u>	137
10.1	<u>Introduction</u>	137
10.2	<u>Workshop Methodology</u>	137
11	<u>ANALYSIS RELATED TO THE PRE-DEFINED STUDY REQUIREMENTS</u>	142
11.1	<u>Potential impact from Critical Infrastructure operators on the Cybersecurity Industry</u>	142
11.2	<u>Who are the large exporters and who are their clients?</u>	143
11.3	<u>What does cross border trade flow in EU look like and how can it be improved?</u>	144
11.4	<u>What does the products & services landscape in Europe look like?</u>	145
11.5	<u>What is the Role of standardization, certification, audit, trust labels</u>	148
11.6	<u>What are the key learnings from the data on the role of government?</u>	149
12	<u>SWOT ANALYSIS OF THE EUROPEAN CYBERSECURITY INDUSTRY</u>	151
12.1	<u>Cybersecurity market SWOT</u>	151
13	<u>CONCLUSIONS AND RECOMMENDATIONS ON THE CYBERSECURITY INDUSTRY MARKET ANALYSIS OF THE EUROPEAN MARKET</u>	153
13.1	<u>State of Play</u>	153
13.2	<u>Overall Conclusions</u>	153
13.3	<u>Priorities and Needs</u>	158
13.4	<u>Recommendations to be considered from the CIMA analysis findings</u>	159
13.5	<u>Recommendations to be considered from the discussions and workshops</u>	160
14	<u>APPENDIX A : EU COUNTRY LEVEL DATA</u>	163
14.1	<u>Introduction</u>	163
14.2	<u>Individual Member State data</u>	163
15	<u>APPENDIX B : EU SALES BY SUB-SECTOR AND PURCHASER INDUSTRY</u>	212
16	<u>APPENDIX C : IMPORTS BY COUNTRY OF ORIGIN PER EU MEMBER STATE</u>	224
17	<u>APPENDIX D : EXPORTS BY COUNTRY OF ORIGIN PER EU MEMBER STATE</u>	230
18	<u>APPENDIX E : COMPETITIVE DASHBOARDS</u>	236
18.1	<u>Individual data dashboards</u>	236
19	<u>APPENDIX F : TRADE FLOWS BY SUB-SECTOR</u>	254
19.1	<u>EU28</u>	254
19.2	<u>USA</u>	254
19.3	<u>China</u>	255
19.4	<u>Japan</u>	255
19.5	<u>India</u>	256
20	<u>APPENDIX G : RESEARCH METHODOLOGY CONFIDENCE LEVELS</u>	257
21	<u>APPENDIX H : TAXONOMY – CYBERSECURITY DATA LEVEL 2 – 4 DEFINITIONS</u>	260
22	<u>APPENDIX I : DATA SOURCES</u>	265
23	<u>APPENDIX J : LIST OF ACRONYMS</u>	274

<u>24</u>	<u>APPENDIX K : TOP 500 GLOBAL CYBERSECURITY COMPANIES</u>	275
<u>25</u>	<u>APPENDIX L : PARTICIPANT ORGANISATIONS IN THE CIMA WORKSHOPS</u>	285
<u>26</u>	<u>APPENDIX M : RESULTS FROM WORKSHOPS</u>	293
26.1	<u>Workshop Recommendations Summary</u>	293
<u>27</u>	<u>APPENDIX N : CYBERSECURITY RESEARCH METHODOLOGY 2017</u>	297
27.1	<u>Introduction to Research Methodology</u>	297
27.2	<u>Defining Cybersecurity</u>	300
27.3	<u>Geographic Analysis</u>	306
27.4	<u>The Quantitative Research Methodology</u>	309
27.5	<u>Managing Boundaries</u>	313
27.6	<u>Creating a “Language”</u>	314
27.7	<u>Developing the Rule- Sets</u>	315
27.8	<u>Generating the Values</u>	316
27.9	<u>Data Sources</u>	319
27.10	<u>Source Management</u>	320
27.11	<u>Source Usage</u>	322
27.12	<u>Multi- Source Process for Deriving Values- an Example</u>	324
27.13	<u>Companies</u>	342
27.14	<u>International Trade Data and Analysis</u>	351

Table of Figures

Figure 1 : Phases of the study	41
Figure 2 : Global Cybersecurity Sales 2014 to 2016 (m EUR).....	51
Figure 3 : Global Total Number of Cybersecurity Companies 2014 to 2016	51
Figure 4 : Global Cybersecurity Employment 2014 to 2016	51
Figure 5 : Global Cybersecurity Forecast Sales Growth 2016 to 2021.....	52
Figure 6 : Global Cybersecurity Sub Level 2 Category Spread for 2016 in %	54
Figure 7 : Global Cybersecurity Forecast Growth 2016 to 2021 by Sub-sector.....	56
Figure 8 : Cybersecurity Sales by Global Region 2016 (m EUR) and %	57
Figure 9 : Cybersecurity Sales market share on a global basis, top 20 countries.....	59
Figure 10 : Cybersecurity Forecast Sales Growth % by Top 20 Country	61
Figure 11 : EU Cybersecurity Sales 2014 to 2016 (m EUR)	64
Figure 12 : Number of Cybersecurity Companies in EU (28) 2014 to 2016	64
Figure 13 : EU Cybersecurity Employment (nr of people) 2014 to 2016	64
Figure 14 : EU Cybersecurity Forecast Growth 2016 to 2021.....	65
Figure 15 : EU Cybersecurity Forecast Growth 2016 to 2021 by Country	65
Figure 16 : EU Cybersecurity Sub-level 2 Category Spread for 2016 in %	67
Figure 17 : EU Cybersecurity Key Measures by Sub-sector 2016	70
Figure 18 : EU Cybersecurity sales per country, per sub category in % as proportion of total Sales per country.....	72
Figure 19 : Average employees per company for EU Member States (ordered by size).....	78
Figure 20 : Average employees per company for EU Member States between 2014 and 2016.....	80
Figure 21 : Average Company Size mapped against Member State Sales in 2016.....	82
Figure 22 : EU Sales % by EU Country 2016	83
Figure 23 : Global locations (corporate headquarters) of top 500 Cybersecurity providers.....	87
Figure 24 : EU Company Size Ranges	88
Figure 25 : EU Cybersecurity Providers Company Size Ranges by Country 2016	88
Figure 26 : Contribution into Cybersecurity by Sector in EU	90
Figure 27 : Contribution in Cybersecurity Sales by Sector, related to by Sub-sector	91
Figure 28 : Relative Contribution in Cybersecurity Sales by Sector – historical perspective (from 2011 to 2016).....	92
Figure 29 : Contribution of Cybersecurity by Sector and per Country	93
Figure 30 : EU Cybersecurity End-User Distribution according to Private, Public and other markets ..	95
Figure 31 : EU Cybersecurity End- Users- Full Break Down	96
Figure 32 : EU Cybersecurity End-Users Distribution by Sub-sector.....	97
Figure 33 : EU Cybersecurity End-Users Distribution by Country	97
Figure 34 : EU and Non- EU Imports for UK and France	101
Figure 35 : EU and Non- EU Imports for UK and France- % by Country.....	102
Figure 36 : Imports as a share of domestic demand in each EU Member State	106
Figure 37 : Top Global Exporting Nations 2016 (m EUR)	108
Figure 38 : EU Country Exports to EU and Non- EU Countries 2016.....	110
Figure 39 : EU and Non- EU Exports for Belgium and Poland	111
Figure 40 : Trade Flows for EU (m EUR) 2016	116
Figure 41 : Trade Flows for Top Four Competing Nations (m EUR) 2016	116
Figure 42 : Comparison of EU and competitor region/ country Exports	117
Figure 43 : Comparison of EU and competitor region/ country Exports relative to their Sales.....	118
Figure 44 : Comparison of EU and competitor region/ country Imports relative to their domestic demand	119
Figure 45 : EU 28 Sales by Sub-sector (m EUR) 2016.....	120

Figure 46 : Competing Nation Sales by Sub-sector (m EUR) 2016.....	121
Figure 47: EU 28 Exports by Sub-sector (m EUR) 2016.....	122
Figure 48 : Competing Nation Exports by Sub-sector (m EUR) 2016.....	123
Figure 49 : Share of Import Market for Major Global Trading Nations (non- EU) 2016.....	126
Figure 50 : Share of Import Market for Major EU Trading Nations 2016.....	127
Figure 51 : Share of Import Market for Second Tier Trading Nations (non- EU) 2016.....	127
Figure 52 : Share of Import Market for Middle Ranking EU Trading Nations 2016.....	128
Figure 53 : Number of EU Cybersecurity companies (headquartered in the EU) selling within EU Member States 2016.....	131
Figure 54 : Number of employees in EU Cybersecurity companies in EU Member States 2016.....	133
Figure 55 : Number of participating companies in the Validation and Country workshops organized by CIMA.....	140
Figure 56 : Country representation of Participating Companies.....	141
Figure 57 : comparing differences between CI sectors.....	143
Figure 58 : EU Confidence Levels Sales and Sales Growth by Country.....	257
Figure 59 : EU Confidence Levels Sales and Sales Growth by Sub-sector.....	258
Figure 60 : Multi- Layered Data Model.....	303
Figure 61 : Grouping Activities.....	305
Figure 62 : Market Research Model.....	311
Figure 63 : Disaggregation Model.....	315
Figure 64 : High Level Diagram of the Source Management System.....	321
Figure 65 : Sample Radar Diagram for Source Value Analysis.....	322
Figure 66 : Example Sources.....	323
Figure 67 : Radar Diagram all 44 Sources.....	328
Figure 68 : Radar Diagram Final 32 Sources.....	328
Figure 69 : Confidence Levels by Sub-sector.....	330
Figure 70 : Confidence Levels by Country.....	331
Figure 71 : Company Search Model.....	344
Figure 72 : Example of Ranked Purchasers.....	349
Figure 73 : Example of Ranked Suppliers.....	350
Figure 74 : EU Delivery of Cybersecurity by Sector.....	351
Figure 75 : Measuring Exports by sector and sub-sector.....	352
Figure 76 : Measuring Exports by Destination Country.....	352
Figure 77 : The Transition from Trade to Inter- Trading.....	352
Figure 78 : Inter- Trading and National Trade Flows.....	353
Figure 79 : Measuring Market Share.....	353
Figure 80 : Measuring Market Share of Country Market.....	354
Figure 81 : Comparing Market Share as a measure of Competitive Performance.....	354
Figure 82 : Identifying End User Groups for Targeting Exports.....	355
Figure 83 : Identifying In- Country Customer for Targeting Exports.....	355
Figure 84 : Challenges presented by Exports.....	357
Figure 85 : The Assessment of Import and Export Trading for Sectors.....	359

Table of Tables

Table 1 : Global Cybersecurity Sales (m EUR) 2014 to 2016.....	53
Table 2 : Global Number of Cybersecurity Companies 2014 to 2016.....	55
Table 3 : Global Cybersecurity Employment, number of people active in Cybersecurity from 2014 to 2016	55
Table 4 : Cybersecurity Country Ranking and Market Share by Sales (m EUR) 2014-2016	58
Table 5 : Cybersecurity Country Sales Growth (m EUR) 2014-2016	60
Table 6 : Cybersecurity Global – Top Growth Countries (Sales Growth) (m EUR) 2014-2016.....	60
Table 7 : EU Cybersecurity Sales (m EUR) 2014 to 2016, by sub-sector	67
Table 8 : EU Cybersecurity Number of Companies 2014 to 2016.....	68
Table 9 : EU Cybersecurity Employment 2014 to 2016	69
Table 10 : EU Cybersecurity Sales (m EUR) 2014 to 2016 by Country	74
Table 11 : EU Cybersecurity Number of Companies 2014 to 2016 by Country	75
Table 12 : EU Cybersecurity Employment 2014 to 2016 by Country.....	76
Table 13 : Average employees per company for EU Member States (ordered by size)	77
Table 14 : Average employees per company for EU Member States between 2014 and 2016.....	79
Table 15 : Average Company Size mapped against Member State Sales in 2016.	81
Table 16 : EU Cybersecurity Sales compared with GDP (m EUR) 2016.....	84
Table 17 : Global locations (corporate headquarters) of top 500 Cybersecurity providers	86
Table 18 : Example for Constructing the Typology of Cybersecurity Providers.....	89
Table 19 : EU Sales by Level 2 Sub Categories and Distributed over End-User Markets.....	98
Table 20 : Total Imports and EU Imports by EU Country in (m EUR), alphabetical order and ordered by Non-EU % imports.....	100
Table 21 : EU Imports by Sub-sector 2016 (m EUR) – alphabetical and top down non-EU % imports	102
Table 22 : Imports in EU by Country in Import as % of Sales – alphabetically and top down %	103
Table 23 : Imports as a share of domestic demand in each EU Member State.....	105
Table 24 : EU Exports by Country alphabetically and by Non-EU % export.....	109
Table 25 : EU Exports by Sub-sector 2016	112
Table 26 : EU Exports 2016 by Country – Exports vs Sales in (m EUR) – alphabetically and Exports as % of Sales.....	113
Table 27 : Comparison of EU and competitor region/ country Exports	117
Table 28 : Comparison of EU and competitor region/ country Exports relative to their Sales	118
Table 29 : Comparison of EU and top competitor region/ country Imports relative to their domestic demand	118
Table 30 : Percentage Market Share Compared.....	128
Table 31 : Percentage Market Share Compared- EU	129
Table 32 : Proportion of EU Cybersecurity suppliers (selling within the EU) that are EU headquartered companies 2016.....	132
Table 33 : Cybersecurity employment in the EU by EU and International companies 2016.....	134
Table 34 : Cybersecurity Sales activities (m EUR) by EU companies and International companies in EU Member States 2016.....	135
Table 35 : EU Cybersecurity Demand met by International companies (m EUR, %) 2016	136
Table 36 : GERMANY : Top 15 Products and Services Level 5 Category	145
Table 37 : UK : Top 15 Products and Services Level 5 Category	146
Table 38 : FRANCE : Top 15 Product and Services Level 5 Category.....	146
Table 39 : ITALY : Top 15 Products and Services Level 5 Category	146
Table 40 : SPAIN :Top 15 Products and Services Level 5 Category	147
Table 41 :The Netherlands : Top 15 Products and Services Level 5 Category	147

<u>Table 42 : BELGIUM :Top 15 Products and Services Level 5 Category.....</u>	148
<u>Table 43 : SWITZERLAND : Top 15 Products and Services Level 5 Category.....</u>	148
<u>Table 44 : Confidence Levels EU Sales and Sales Growth.....</u>	259
<u>Table 45 : List of acronyms of the 28 Member States</u>	274
<u>Table 46 : Cybersecurity Sub-sectors.....</u>	301
<u>Table 47 : Data Hierarchy Example</u>	304
<u>Table 48 : List of Countries for Research Purposes.....</u>	308
<u>Table 49 : Data sources.....</u>	326
<u>Table 50 : Rejected Sources</u>	327
<u>Table 51 : Full List of Metrics</u>	331
<u>Table 52 : Description of Key Metrics</u>	341
<u>Table 53 : Definition of End- User Markets for Cybersecurity</u>	348
<u>Table 54 : Example for Constructing the Typology of Cybersecurity Providers.....</u>	350
<u>Table 55 : Data Subset for Export Example (m GBP)</u>	362

Executive Summary [EN]

The purpose of this study is to provide the European Commission (DG CONNECT) with an independent and unbiased market analysis of the Cybersecurity industry within the European Union (EU) and globally. The study aims to provide information relevant to promoting the take-up and the supply of secure ICT solutions in the EU in order to improve the overall security of European ICT systems.

The quantitative CIMA Cybersecurity research methodology used in this study for gathering, categorising and analysing the market data uses a novel big data approach to curating economic and markets values from multiple, mainly transactional data sources. Over 900 sources have been used and tracked over time for the research, which include Cybersecurity sources, other industry sources, financial, investor, academic, insurance, legal, procurement sources as well as company sources. This multi-sourced approach can operate in areas where other approaches based on a National statistical approach or Trade/ industry approach (including survey techniques) either do not exist or are poorly aligned with the sector/ market under investigation, but has the limitation therefore of not being directly comparable with traditional statistics. The value for the Cybersecurity sector in this report is higher than in most (not all) other research reports because the search for evidence covers a very broad base which allows the accommodation of national variations in definition without losing the ability to compare results across multiple continents or countries.

This methodology takes all relevant Cybersecurity sales into account, including products and services that are distributed and resold by system integrators, etc. This is consistent with other market assessments and represents genuine economic activity. Furthermore, the research includes activities by companies that are specialists in Cybersecurity sector as well as companies that may be non-specialist but operate within the Cybersecurity supply/value chain. The source data, therefore, includes: companies that solely provide Cybersecurity products and services; companies that (amongst other activities) provide Cybersecurity products and services; and companies that provide products and services that form part of the Cybersecurity supply/value chain.

The results are based on the following **Cybersecurity market and taxonomy**:

- An initial Cybersecurity definition which was created in 2010, updated in 2013 and in 2014 to reflect significant changes in the content and reporting of Cyber activities. This history reflects the constantly changing nature of an emerging sector.
- The 13 sub-sectors of Cybersecurity used in this research are: Anti- Malware, Application Security, Business Continuity, Cyber Consultancy, Cyber Insurance, Encryption, Identity and Access, Infrastructure, Mobile, Outsourced/ Managed Services, Situational Awareness, Systems Recovery, Training & Education.
- The Cybersecurity data set used for this research includes 1,100 products and services, aggregated (by supply or value chain activity) into four data levels and then reported for the 13 Cybersecurity sub-sectors.

The **Global Cybersecurity market** is described, including the market volume, number of companies, and growth for different Cybersecurity sub-sectors, giving details for regions (Europe, Asia, Americas etc) and for major countries such as the USA, China and Japan. These statistics allow for a comparison with the European market as a whole, and with leading European Member States. The magnitude of the resulting estimates concerning market volumes, number of companies, and growth rates reflect the particular CIMA methodology, explained above.

Key points are:

- Based on this methodology, it can be said that the Cybersecurity market is globally a EUR 600 billion market, that is expected to grow in the next five years on average by approximately 17% in terms of sales, number of companies and employment. The largest market is North America, followed by Asia and Europe. The USA and the EU combined contribute more than half (over

EUR 309 billion) to the global Cybersecurity market. As mentioned above, these values are higher than in most (not all) other research reports because the search for evidence covers a particularly broad base.

- From both a sales, company and employment perspective, Situational Awareness has been the largest Cybersecurity market, followed by Infrastructure and Application Security spending. The global Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, varying from 5% for Training and Education to 25% for Identity and Access and for Outsourced/ Managed Services in 2015/16, with the number of global companies and employment growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum out to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%.
- Looking at global sales figures the USA is the dominant country (25.3% of global sales) followed by China (9%), Japan (8.3%) and Germany (5.7%). In Sales terms the EU (including the UK) represented 26% of the global market in 2016, above the USA, making the EU the single largest Cybersecurity market in the world when accounted for as a single market.
- There are multiple growth opportunities within the EU (Germany, UK, Austria, Belgium, ...) and throughout Europe and there are opportunities for European companies to seek out other global market opportunities, both from a historical perspective (Chile, UAE, ...) and from a forecast growth perspective.

The **European Cybersecurity market** is described, including the market volume, growth rate and the products and services sold across Europe as a whole and in specific Member States. Key points are:

- Based on the CIMA methodology explained above, it can be said that the total for EU Cybersecurity sales in 2016 was EUR 157,973 million, an increase of 17% on 2015 sales. Germany, the UK, France and Italy have significantly larger sales than other Member States. Forecast sales growth for the EU between 2016-2021 of 17.8%-20.3% is above the forecast global average of 16-18%. These anticipated growth rates are mainly based upon historical growth and do not yet take into account effects of additional regulations such as GDPR, NIS, PSD2 or other regulatory frameworks.
- The total number of EU Cybersecurity companies in 2016 was 60,250 (i.e. companies involved in the Cybersecurity supply/value chain as explained above), accounting for 27% of the global total number of Cybersecurity companies. EU Cybersecurity employment in 2016 was 909,600, accounting for 25% of the global employment for 2016. Looking at the sizes of EU Cybersecurity companies they comprise 39% micro, 35% small, 18% medium and 8% large companies. The distribution of company sizes varies significantly across Member States (e.g. micro-companies are 32% of Cybersecurity companies in Denmark through to 44% in Germany).
- The EU Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, varying from 4% for Training and Education to 26% for Encryption in 2015/16, with the number of EU companies and EU employment growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%. Infrastructure (19%), Situational Awareness (17%) and Application Security (17%) are the largest EU sub-sectors in sales terms.
- Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia.
- Cybersecurity activities and companies have not emerged solely from the ICT sector, but from across a range of market sectors. Looking at the sectors involved in delivering Cybersecurity products and services for the EU in 2016, 31% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 22% originates from companies whose core business is ICT, 19% originates from companies whose core business is Defence/ Aerospace and 13% from companies whose core business is Security.
- The Cybersecurity Industry Market Analysis defines 16 end user categories, based upon the Cybersecurity market flows. The EU End User markets in sales terms comprise Private users (45%

of sales), Public users (31%) and “Other” users (25%). The “Other” category is large because it includes retail activities (10%) and un-attributable activities (10%). The Public Sector Cybersecurity market ranges between 24% (Germany) to 48% (UK) and the Private sector Cybersecurity market ranges between 41% (Austria) to 49% (Czech Republic, France and Poland).

- The EU imports EUR 8.5 billion from outside the EU, which is approximately 5.3% of the total EU Cybersecurity market in 2016. The percentage of imports into each Member State from within the EU (as opposed to outside the EU) varies significantly by country, from 17% for the UK through to 53% for France (2016 figures). Member States on average import 30% of products/ services from other EU countries and 70% from outside the EU: their EU imports range from 20% for Encryption and Outsourced/ Managed Services through to 32% for Situational Awareness and System Recovery and Data Cleansing.
- Although the EU only imports 5.3% of its domestic demand (2016 figures), the proportion of EU demand met by international companies from sales by operations established within the EU lies between 21-25% (2016 figures) depending on how much of the international company sales activity in the EU is exported outside the EU. If one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the ‘effective’ imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.
- The EU exports to non-EU countries are EUR 6.1 billion representing a formal trade deficit of EUR 2.4 billion. The EU Member States with the highest export intensity (proportion of exports to sales generated within their borders) are Croatia (14%), Estonia and Germany (10%), Latvia and Bulgaria (9%), and the UK, Cyprus, Austria and Slovenia (7%). The countries with the lowest proportions of exports to sales are Romania, Hungary and Sweden (1%), and Denmark, Netherlands, Finland, Spain and Czech Republic (2%).
- The importance of the UK in this analysis should be noted. Looking at the possible implications of Brexit, the UK domestic demand of EUR 30,522 million (in 2016) is significant compared to EU-27 domestic demand of EUR 129,828 million. Currently the UK is not contributing significantly to importing from the EU-27 markets compared to exports, and the trade deficit for the EU-27 Cybersecurity Industry might therefore drop as a result of Brexit.
- If one looks at EU-27 Exports compared to Sales (i.e. taking out UK Sales and UK Exports) the EU-27 intensity of exports compared to sales drops from the EU-28 level of 3.9% to 3.4%. EU-27 exporting activity without the UK is even lower than competitors relative to the sales activities delivered from within its borders.

EU Competitiveness has been analysed, looking at trade flows between the EU and other global actors and comparing imports, exports and sales, and relative market shares. Key points are:

- The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective. The EU and these competitors are competing strongly for export share in Situational Awareness and System Recovery and Data Cleansing, followed by Infrastructure, Identity and Access and Application Security.
- Similarly, by comparing region/country domestic demand with imports it is possible to analyse to what extent the EU and other competing regions/ countries meet their Cybersecurity needs by imports rather than from internal suppliers. As mentioned above, the EU imports 5.3% of its domestic demand, which is higher than the US 4.2%, India 4.5%, Japan 4.6% but below that of China 6.1%. A further 21-25% of EU demand is met by international companies operating within the EU.
- While the USA continues to be the EU’s main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries. There are some growth markets where the EU is a stronger exporter than the USA, and similar to

China, such as South Korea, Indonesia, Russia and South Africa, which could form an opportunity for a more coordinated EU export drive in Cybersecurity products and services.

Integrating the statistical findings, a **Strengths, Weaknesses, Opportunities and Threats (SWOT)** analysis of the European Cybersecurity Industry has been performed, based on the study results and points made throughout the report. Key weaknesses and threats to address include:

- The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential.
- The EU, as a whole, imports 5.3% of its Cybersecurity products and services from non-EU sources. The EU is a net importer for all sub-sectors of Cybersecurity, except for Cyber Insurance. Major competitors (US, China, India, Japan) are net exporters in all sub-sectors.
- However, if one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.

Key opportunities based on EU strengths include:

- The global Cybersecurity market has grown rapidly over the last 3 years (above 18%) with the number of EU (and global) companies and employment growing at a similar rate, and is forecast to continue growing rapidly at a similar rate to 2021. Forecast sales growth for the EU between 2016-2021 (17.8%-20.3%) is above the forecast global average of 16-18% and is broadly in-line with historical EU growth in Cybersecurity.
- Cybersecurity activities and companies have emerged from a range of market sectors where Europe is strong (ICT, defence/ aerospace and security) – this offers future opportunities.
- The Digital Single Market will promote Cybersecurity in the EU. The NIS directive will stimulate EU critical infrastructure sectors to address Cybersecurity and this will create an opportunity for EU Industry.
- Public users form a significant part of the EU End User market in sales terms (at least 31%) and so public procurement policies can significantly influence the Cybersecurity market.
- While the USA is the EU's main competitor in global markets (followed closely by China), China followed by the US is the main competitor to EU suppliers in EU markets and specifically in the smaller EU countries.

To support the overall aim of promoting the take-up and the supply of secure ICT solutions in the EU a series of MS workshops including ECSO was conducted to disseminate the initial findings and obtain feedback from selected Cybersecurity solutions and services providers, with different backgrounds, market focus areas and levels of maturity. Key views and suggestions by workshop participants and recommendations from the analysis can be summarised as follows:

1) A European industrial policy for Cybersecurity should be created and promulgated to support the Cybersecurity Industry, and lower the dependencies on non-European markets such as the US and China. This would support the development and existence of large European Cybersecurity market operators. Mandating that all bids with Cybersecurity content contain a defined SME proportion and prohibiting national MS standards for all public procurements would also support the EU's innovation capacity. **Public Procurement could be split into two: (1) for commodity purchasing, (2) strategic with an industrial policy.**

2) EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective. The leading European technology developers and innovative SMEs need to be empowered to improve export growth. There are some growth markets (such as South Korea, Indonesia, Russia and South Africa) where the EU is strong, which could form an opportunity for a

more **coordinated EU export drive in Cybersecurity** products and services. There are also potential opportunities from a forecast growth perspective (such as Pakistan and Taiwan). **Coordinated EU export support in areas where there is strong export competition** with international competitors (Situational Awareness and System Recovery and Data Cleansing, followed by Infrastructure, Identity and Access and Application Security etc) should be considered.

3) The development of **EU Cybersecurity centres of excellence** should be strengthened by developing and further empowering the development of a NIST-like organization and supporting the development and growth at European level and by the Member States of regional and local Centres of Excellences such as the Cybersecurity clusters.

4) Baseline requirements for **certification schemes and standards** for people, products, services and other components should be defined. These schemes should be on a self-certification basis, but built upon the standards set by the EC.

5) The Venture Capital market needs to be stimulated by the provision of significant tax incentives for **higher risk investments**. Financial support from the EC for an incubator platform in the 10 leading European markets, together with financial instruments for innovative Cybersecurity investors should be considered to be additionally supported through co-investment.

6) Measures could be considered to **help smaller EU countries access EU sources of supply**, which will help to improve overall EU competitiveness.

7) Further study should be considered to examine the implications and impact of the **significant EU dependence on International suppliers** on the EU Cybersecurity market, for example what the benefits and disadvantages of such international Cybersecurity investment in Europe are.

Executive Summary [FR]

Le but de cette étude est de fournir à la Commission européenne (DG CONNECT) une analyse de marché indépendante et impartiale de l'industrie de la cybersécurité au sein de l'Union européenne (UE) et dans le monde. L'étude vise à fournir des informations utiles à la promotion de l'adoption et de la fourniture de solutions TIC sécurisées dans l'UE afin d'améliorer la sécurité globale des systèmes TIC européens.

La méthodologie utilisée dans cette étude pour collecter, catégoriser et analyser les données de marché utilise une nouvelle approche de Big Data pour le traitement des valeurs économiques et de marché à partir de multiples sources de données, principalement transactionnelles. Plus de 900 sources ont été utilisées et suivies au fil du temps pour la recherche, notamment des sources de cybersécurité, d'autres sources de l'industrie, des sources financières, des investisseurs, des universités, des compagnies d'assurance, des sources juridiques, des marchés publics et des entreprises. Cette approche multi-sources peut fonctionner dans des domaines où d'autres approches basées sur une approche statistique nationale ou une approche commerce / industrie (y compris les techniques d'enquête) n'existent pas ou sont mal alignées sur le secteur / marché considéré, mais ont donc comme limite de n'être pas directement comparable aux statistiques traditionnelles. La valeur pour le secteur de la cybersécurité dans ce rapport est plus élevée que dans la plupart des rapports de recherche (pas tous) car la recherche de preuves couvre une base très large qui permet de prendre en compte les variations nationales dans la définition sans perdre la possibilité de comparer les résultats sur plusieurs continents ou pays.

Cette méthodologie prend en compte toutes les ventes pertinentes liées à la cybersécurité, y compris les produits et services distribués et revendus par les intégrateurs de systèmes, etc. Ceci est cohérent avec les autres évaluations du marché et reflète l'activité économique réelle. En outre, la recherche inclut des activités d'entreprises spécialisées dans le secteur de la cybersécurité, ainsi que d'entreprises qui peuvent être non spécialisées mais opérer dans la chaîne d'approvisionnement. Les données sources comprennent donc: les entreprises qui fournissent uniquement des produits et services de cybersécurité; les entreprises qui (entre autres activités) fournissent des produits et des services de cybersécurité; et les entreprises qui fournissent des produits et services qui font partie de la chaîne d'approvisionnement.

Les résultats sont basés sur le marché et la taxonomie de cybersécurité suivants:

- Une définition initiale de la cybersécurité créée en 2010, mise à jour en 2013 et en 2014 afin de refléter les changements importants apportés au contenu et au reporting des activités Cyber. Cette histoire reflète la nature en constante évolution d'un secteur émergent.
- Les 13 sous-secteurs de la cybersécurité utilisés dans cette recherche sont les suivants: Anti-Malware, sécurité des applications, continuité d'activité, cyber-conseil, cyberassurance, chiffrement, identité et accès, infrastructure, services mobiles, services externalisés / gérés, services de veille, Systems Recovery, formation et éducation.
- L'ensemble de données de cybersécurité utilisé dans cette recherche comprend 1 100 produits et services, regroupés (par activité d'approvisionnement ou de chaîne de valeur) en quatre niveaux de données, puis reliés aux 13 sous-secteurs de la cybersécurité.

Le marché mondial de la cybersécurité est décrit, y compris le volume du marché, le nombre de sociétés et la croissance pour différents sous-secteurs de la cybersécurité, en donnant des détails pour les régions (Europe, Asie, Amériques, etc.) et pour les principaux pays tels que les États-Unis, la Chine et le Japon. Ces statistiques permettent une comparaison avec le marché européen dans son ensemble et avec les principaux États membres européens. L'ampleur des estimations obtenues concernant les volumes de marché, le nombre de sociétés et les taux de croissance reflète la méthodologie propre utilisée CIMA, expliquée ci-dessus.

Les points clés sont:

- Sur la base de cette méthodologie, on peut affirmer que le marché de la cybersécurité est un marché mondial de 600 milliards d'euros, qui devrait croître en moyenne d'environ 17% au cours des cinq prochaines années, en termes de chiffre d'affaires, de nombre d'entreprises et d'emplois. Le marché le plus important est l'Amérique du Nord, suivie de l'Asie et de l'Europe. Les États-Unis et l'Union européenne représentent ensemble plus de la moitié (plus de 309 milliards d'euros) du marché mondial de la cybersécurité. Comme mentionné ci-dessus, ces valeurs sont plus élevées que dans la plupart des rapports de recherche (pas tous) car la recherche de preuves couvre une base particulièrement large.
- Du point de vue des ventes, de l'entreprise et de l'emploi, les services de veille représentent le plus grand marché de la cybersécurité, suivi par des dépenses consacrées à la sécurité des infrastructures et des applications. Le marché mondial de la cybersécurité a connu une croissance rapide dans tous les sous-secteurs au cours des 3 dernières années, allant de 5% pour la formation et l'éducation à 25% pour l'identité et l'accès et pour les services externalisés / gérés en 2015/16. Chaque sous-secteur de la cybersécurité devrait continuer à croître rapidement à un taux similaire (supérieur à 10% par an jusqu'en 2021), à l'exception de la formation et de l'éducation, qui devrait croître à un taux légèrement supérieur à 5%.
- En regardant les chiffres des ventes mondiales, les États-Unis sont le pays dominant (25,3% des ventes mondiales), suivis de la Chine (9%), du Japon (8,3%) et de l'Allemagne (5,7%). En termes de vente, l'UE (y compris le Royaume-Uni) représentait 26% du marché mondial en 2016, faisant de l'UE le plus grand marché de cybersécurité au monde, lorsqu'il est considéré comme un marché unique.
- Il existe de nombreuses opportunités de croissance au sein de l'UE (Allemagne, Royaume-Uni, Autriche, Belgique...) et dans toute l'Europe. Les entreprises européennes ont également la possibilité de rechercher d'autres opportunités sur les marchés mondiaux, à la fois d'un point de vue historique (Chili, UAE....) et du point de vue de la croissance prévisionnelle.

Le marché européen de la cybersécurité est décrit dans le rapport, y compris le volume du marché, le taux de croissance et les produits et services vendus dans l'ensemble de l'Europe et dans certains États membres. Les points clés sont:

- Sur la base de la méthodologie CIMA expliquée ci-dessus, on peut dire que le total des ventes de la cybersécurité dans l'UE en 2016 s'élevait à 157 973 millions d'EUR, soit une augmentation de 17% par rapport à 2015. L'Allemagne, le Royaume-Uni, la France et l'Italie ont des ventes nettement supérieures à celles des autres États membres. La croissance prévue des ventes pour l'UE entre 2016 et 2021, de 17,8% à 20,3%, est supérieure à la moyenne mondiale prévue de 16 à 18%. Ces taux de croissance anticipés sont principalement basés sur la croissance historique et ne tiennent pas encore compte des effets de réglementations supplémentaires telles que le GDPR, le NIS, le PSD2 ou d'autres cadres réglementaires.
- Le nombre total d'entreprises de cybersécurité dans l'UE en 2016 s'élève à 60 250 (c'est-à-dire des entreprises impliquées dans la chaîne logistique / valeur de la cybersécurité, comme expliqué ci-dessus), ce qui représente 27% du nombre total d'entreprises de cybersécurité dans le monde. En 2016, 909 600 personnes occupaient un emploi dans le secteur de la cybersécurité dans l'UE, soit 25% de l'emploi mondial dans le secteur en 2016. Les entreprises de cybersécurité de l'UE comptent 39% de micro, 35% de petites entreprises, 18% de moyennes et 8% de grandes entreprises. La répartition des tailles d'entreprise varie considérablement d'un État membre à l'autre (par exemple, les micro-entreprises représentent 32% des entreprises de cybersécurité au Danemark et 44% en Allemagne).
- Le marché de la cybersécurité dans l'UE a connu une croissance rapide dans tous les sous-secteurs au cours des trois dernières années, passant de 4% pour la formation et l'éducation à 26% pour le chiffrement en 2015-2016, le nombre d'entreprises et l'emploi dans l'UE augmentant à des taux

similaires. Chaque sous-secteur de la cybersécurité devrait continuer à croître rapidement à un taux similaire (supérieur à 10% par an jusqu'en 2021), à l'exception de la formation et de l'éducation, qui devrait croître à un taux légèrement supérieur à 5%. Les infrastructures (19%), la connaissance de la situation (17%) et la sécurité des applications (17%) sont les plus importants sous-secteurs de l'UE en termes de ventes.

- L'Europe est le siège social de 14% des 500 plus grands fournisseurs mondiaux de cybersécurité, contre 75% pour les Amériques (Nord et Sud), 7% pour Israël et 4% pour l'Asie.
- Les activités et les entreprises de cybersécurité ne sont pas uniquement issues du secteur des TIC, mais de toute une gamme de secteurs du marché. Sur les secteurs concernés par la fourniture de produits et services de cybersécurité pour l'UE en 2016, 31% de la valeur des ventes sont générés par des entreprises du secteur de la cybersécurité uniquement, 22% par des entreprises dont le cœur de métier est les TIC, 19% par dont les activités principales sont Défense / Aéronautique et 13% d'entre elles dont les activités principales sont la sécurité.
- L'analyse du marché de l'industrie de la cybersécurité définit 16 catégories d'utilisateurs finaux, basées sur les flux du marché de la cybersécurité. Les marchés des utilisateurs finaux de l'UE en termes de vente comprennent les utilisateurs privés (45% des ventes), les utilisateurs publics (31%) et les autres utilisateurs (25%). La catégorie «Autres» est large car elle inclut les activités de vente au détail (10%) et les activités non imputables (10%). Le marché de la cybersécurité dans le secteur public varie entre 24% (Allemagne) et 48% (au Royaume-Uni) et le marché de la cybersécurité dans le secteur privé entre 41% (Autriche) et 49% (République tchèque, France et Pologne).
- L'UE importe 8,5 milliards EUR de l'extérieur de l'UE, ce qui représente environ 5,3% du marché total de la cybersécurité dans l'UE en 2016. Le pourcentage d'importations dans chaque État membre de l'UE (par opposition à l'extérieur de l'UE) varie considérablement d'un pays à l'autre, de 17% pour le Royaume-Uni à 53% pour la France (chiffres 2016). Les États membres importent en moyenne 30% des produits / services en provenance d'autres pays de l'UE et 70% en dehors de l'UE: leurs importations dans l'UE vont de 20% pour le cryptage et des services externalisés / gérés à 32% pour les services de veille (Situational Awareness), la récupération du système (System Recovery) et le nettoyage des données (Data Cleaning).
- Bien que l'UE n'importe que 5,3% de sa demande intérieure (chiffres de 2016), la part de la demande de l'UE satisfaite par les entreprises internationales provenant des ventes des opérations établies dans l'UE se situe entre 21 et 25% (chiffres de 2016), en fonction de la part de marché. Si l'on associe des importations de cybersécurité provenant de l'extérieur de l'UE à des ventes de cybersécurité réalisées par des entreprises internationales à partir de bases opérationnelles établies dans l'UE, les importations «effectives» d'entreprises internationales ayant leur siège en dehors de l'UE représentent entre 26 et 30% de la demande en 2016.
- Les exportations de l'UE vers les pays tiers représentent 6,1 milliards d'euros, ce qui représente un déficit commercial formel de 2,4 milliards d'euros. Les États membres de l'UE présentant la plus forte intensité d'exportation (proportion des exportations par rapport aux ventes générées à l'intérieur de leurs frontières) sont la Croatie (14%), l'Estonie et l'Allemagne (10%), la Lettonie et la Bulgarie (9%), le Royaume-Uni, Chypre et l'Autriche et la Slovaquie (7%). Les pays ayant les plus faibles proportions d'exportations par rapport aux ventes sont la Roumanie, la Hongrie et la Suède (1%), le Danemark, les Pays-Bas, la Finlande, l'Espagne et la République tchèque (2%).
- Il convient de noter l'importance du Royaume-Uni dans cette analyse. En ce qui concerne les implications possibles du Brexit, la demande intérieure du Royaume-Uni de 30 522 millions d'euros (en 2016) est significative par rapport à la demande intérieure de l'UE-27 de 129 828 millions d'euros. À l'heure actuelle, le Royaume-Uni ne contribue pas beaucoup aux importations en provenance des marchés de l'UE-27 par rapport aux exportations, et le déficit commercial de l'industrie de la cybersécurité de l'UE-27 pourrait donc diminuer grâce au Brexit.

- Si l'on examine les exportations de l'UE-27 par rapport aux ventes (c'est-à-dire en prenant en compte les ventes et les exportations britanniques), l'intensité des exportations de l'UE-27 par rapport aux ventes chutera de 3,9% à 3,4% dans l'UE-28. L'activité d'exportation de l'UE-27 sans le Royaume-Uni est même inférieure à celle de ses concurrents par rapport aux activités de vente réalisées à partir de ses frontières.

La compétitivité de l'UE a été analysée, en analysant les flux commerciaux entre l'UE et les autres acteurs mondiaux et en comparant les importations, les exportations et les ventes, ainsi que les parts de marché relatives. Les points clés sont:

- Les exportations de l'UE ne représentent que 3,9% de ses activités commerciales, contre 6,3% pour les États-Unis, 10,1% pour l'Inde, 18,1% pour le Japon et 26,2% pour la Chine. Les activités d'exportation de l'UE sont nettement inférieures à celles de ses concurrents par rapport aux activités de vente réalisées à partir de ses frontières: l'UE ne réalise pas son potentiel d'exportation si on en juge par cette perspective économique. L'UE et ces concurrents se disputent fortement la part des exportations dans les domaines suivants: service de veille, récupération du système et nettoyage des données, puis infrastructure, identité, accès et sécurité des applications.
- De même, en comparant la demande intérieure régionale / nationale aux importations, il est possible d'analyser dans quelle mesure l'UE et d'autres régions / pays concurrents répondent à leurs besoins en matière de cybersécurité par des importations plutôt que par des fournisseurs internes. Comme mentionné ci-dessus, l'Union européenne importe 5,3% de sa demande intérieure, ce qui est supérieur à 4,2% pour les États-Unis, 4,5% pour l'Inde et 4,6% pour le Japon, mais inférieur à 6,1% pour la Chine. De plus, 21 à 25% de la demande de l'UE est satisfaite par des entreprises internationales opérant dans l'UE.
- Alors que les États-Unis continuent d'être le principal concurrent de l'UE sur les marchés mondiaux (suivis de près par la Chine), la Chine est le principal concurrent au sein des marchés de l'UE et plus particulièrement des plus petits pays de l'UE. Dans certains marchés en croissance, l'UE est un exportateur plus fort que les États-Unis et similaire à la Chine, comme la Corée du Sud, l'Indonésie, la Russie et l'Afrique du Sud, ce qui pourrait constituer une opportunité pour une campagne d'exportation plus coordonnée de l'UE dans les produits et services de cybersécurité.

L'intégration des résultats statistiques, une analyse des forces, des faiblesses, des opportunités et des menaces (SWOT) de l'industrie européenne de la cybersécurité a été réalisée, sur la base des résultats de l'étude et des remarques formulées tout au long du rapport. Les principales faiblesses et menaces à traiter incluent:

- Les exportations de l'UE ne représentent que 3,9% de ses activités commerciales, contre 6,3% pour les États-Unis et le Japon, 10,1% pour l'Inde, 18,1% pour le Japon et 26,2% pour la Chine. Les activités d'exportation de l'UE sont nettement inférieures à celles de ses concurrents par rapport aux activités de vente réalisées à partir de ses frontières: l'UE ne réalise pas son potentiel d'exportation.
- L'UE dans son ensemble importe 5,3% de ses produits et services de cybersécurité en provenance de sources non européennes. L'UE est un importateur net pour tous les sous-secteurs de la cybersécurité, à l'exception de la cyberassurance. Les principaux concurrents (États-Unis, Chine, Inde et Japon) sont des exportateurs nets dans tous les sous-secteurs.
- Toutefois, si l'on associe des importations de cybersécurité extra-européennes à des ventes de cybersécurité effectuées par des entreprises internationales basées sur des bases opérationnelles établies dans l'UE, les importations «effectives» d'entreprises internationales ayant leur siège en dehors de l'UE représentent entre 26 et 30% de la demande en 2016.

Les principales opportunités basées sur les forces de l'UE comprennent:

- Le marché mondial de la cybersécurité s'est développé rapidement au cours des trois dernières années (plus de 18%), le nombre d'entreprises européennes (et mondiales) et l'emploi

augmentant à un rythme similaire, et devrait continuer à croître rapidement à un taux similaire jusqu'en 2021. La croissance des ventes prévue pour l'UE entre 2016 et 2021 (17,8% à 20,3%) est supérieure à la moyenne mondiale prévue de 16 à 18% et est globalement conforme à la croissance historique de la cybersécurité dans l'UE.

- Les activités et les entreprises de cybersécurité ont émergé de plusieurs secteurs de marché où l'Europe est forte (TIC, défense / aérospatiale et sécurité) - cela offre des opportunités pour l'avenir.
- Le marché unique numérique favorisera la cybersécurité dans l'UE. La directive NIS incitera les secteurs d'infrastructures critiques de l'UE à s'attaquer à la cybersécurité, ce qui créera une opportunité pour l'industrie européenne.
- Les utilisateurs publics constituent une part significative du marché des utilisateurs finaux de l'UE en termes de ventes (au moins 31%) et les politiques en matière de marchés publics peuvent donc influencer de manière significative sur le marché de la cybersécurité.
- Alors que les États-Unis sont le principal concurrent de l'UE sur les marchés mondiaux (suivis de près par la Chine), la Chine, suivie des États-Unis, est le principal concurrent des fournisseurs de l'UE sur les marchés de l'UE et plus particulièrement dans les plus petits pays de l'UE.

Afin de soutenir l'objectif général de promotion de l'adoption et de la fourniture de solutions TIC sécurisées dans l'UE, une série d'ateliers a été organisée pour diffuser les premiers résultats et obtenir un retour d'information de la part de fournisseurs de services et des solutions de cybersécurité sélectionnés. Les points de vue et suggestions clés des participants à l'atelier et les recommandations de l'analyse peuvent être résumés comme suit:

1) Une politique industrielle européenne en matière de cybersécurité devrait être créée et promulguée pour soutenir l'industrie de la cybersécurité et réduire la dépendance vis-à-vis de marchés non européens tels que les États-Unis et la Chine. Cela soutiendrait le développement et l'existence d'importants opérateurs du marché européen de la cybersécurité. Exiger que toutes les offres comportant un contenu relatif à la cybersécurité contiennent une proportion définie pour les PME et interdire les normes nationales des États membres pour tous les marchés publics renforcerait également la capacité d'innovation de l'UE. Les marchés publics pourraient être scindés en deux: (1) marchés publics pour les achats de produits de base, (2) marchés publics stratégiques à des fins pour une politique industrielle.

2) L'activité d'exportation de l'UE est nettement inférieure à celle de ses concurrents par rapport aux activités de vente réalisées à partir de ses frontières: l'UE ne réalise pas son potentiel d'exportation si elle est jugée sous cet angle économique. Les principaux développeurs européens de technologies et les PME innovantes doivent être habilités à améliorer la croissance de leurs exportations. L'UE est forte sur certains marchés en croissance (tels que la Corée du Sud, l'Indonésie, la Russie et l'Afrique du Sud), ce qui pourrait constituer une opportunité pour une campagne d'exportation mieux coordonnée de l'UE dans les produits et services de cybersécurité. Il existe également des opportunités potentielles du point de vue de la croissance prévisionnelle (comme au Pakistan et à Taiwan). Un soutien coordonné aux exportations de l'UE dans les domaines où il existe une forte concurrence à l'exportation avec des concurrents internationaux (services de veille, récupération du système et nettoyage des données, suivi de l'infrastructure, de l'identité et de l'accès et de la sécurité des applications, etc.) doit être pris en compte.

3) Le développement des centres d'excellence de l'UE en matière de cybersécurité devrait être renforcé en développant et en renforçant le développement d'une organisation similaire à celle du NIST et en soutenant le développement et la croissance au niveau européen et par les États membres de centres d'excellence régionaux et locaux, tels que: Clusters de cybersécurité.

4) Les exigences de base pour les systèmes de certification et les normes pour les personnes, produits, services et autres composants doivent être définies. Ces systèmes devraient être auto-certifiés, mais fondés sur les normes établies par la CE.

5) Le marché du capital-risque doit être stimulé par la mise en place d'incitations fiscales importantes pour les investissements présentant un risque plus élevé. Le soutien financier de la CE à la création d'une plate-forme d'incubateur sur les 10 principaux marchés européens, ainsi que d'instruments financiers destinés aux investisseurs innovants dans le domaine de la cybersécurité devrait pouvoir bénéficier d'un soutien supplémentaire par le biais de co-investissements.

6) Des mesures pourraient être envisagées pour aider les petits pays de l'UE à accéder aux sources d'approvisionnement de l'UE, ce qui contribuera à améliorer la compétitivité globale de l'UE.

7) Une étude plus approfondie devrait être envisagée pour examiner les implications et l'impact de la forte dépendance de l'Union européenne vis-à-vis des fournisseurs internationaux sur le marché européen de la cybersécurité, par exemple les avantages et les inconvénients d'un tel investissement international en Europe dans la cybersécurité.

Background

The objective of this study is to provide the European Commission DG for Communications Networks, Content & Technology (DG CONNECT) with an independent and unbiased market analysis of the Cybersecurity industry within the European Union (EU). The study aims to promote the take-up and the supply of secure ICT solutions in the EU in order to improve the overall Cybersecurity in Europe.

The approach taken in this study is a market analysis on the basis of existing market data of over 900 different sources, based upon a methodology that has been scrutinized and used previously in the domain of Security, Cybersecurity and other industries.

The results presented in this final report are the first formal documentation of the 2016 data ever published. While the study was originally commissioned in 2013, work was done in a period spanning parts of 2015 and early 2016 and was partially reported internally to the European Commission in 2016. Additional components were studied in 2016, 2017 and 2018, taking into consideration developments happening in 2017.

This document describes the results of the 2017-18 study on the 2016 market data, a more accurate and recent study of the market by LSEC and PwC on 2016 market data, including global, EU, and Member State (MS) data on markets, products and services, companies, employment, trade flows, the methodology used, the taxonomy applied and detailed analysis.

The document presents a unique view of the European Digital Single Market as a dynamic, and economically very attractive high growth market, with multiple opportunities within the European market and beyond. It indicates a growing important domain for skilled Cybersecurity professionals and European entrepreneurs to be active in. It identifies some key markets and the significance of some European Member States both in terms of market size and their importance for economic trade beyond the European markets.

The report shows anticipated growth rates, based on historical perspectives only (not including some expected major drivers such as GDPR, the NIS directive, and other regulations) that already exceeds the average forecast number by various market analysts.

This study also provides an identification of the current European landscape, as well as providing further support for this strategically important economic activity, called Cybersecurity.

Context and Considerations

This report presents a stable but alternative view of the current Cybersecurity market, compared to standard market reports. In contrast to these, the methodology used here is innovative as the data and its analysis are based on actual trade flows related to an agreed stable taxonomy. The data collection focuses on the actual purchasing by organizations of Cybersecurity goods and services, sold by Cybersecurity providers in 2016 and is related to earlier years. The historical perspective indicates that the 2016 data are a continuation of earlier trends. There are no clear signs that these are very different from data collected in 2017 or expected in later years. Like all such reports, this report is a snapshot from a moment in time, but it will be distinguished for its factual analysis of trade flows, its historical perspective and its bottom-up taxonomy.

The report presents Europe as a stable and prosperous market for Cybersecurity services and products. With a continued growth perspective for the next five years, Cybersecurity should be considered further as an industry by itself, which needs to further mature.

While the report presents Cybersecurity as a significant multi-billion Euro market, indicating a large number of Cybersecurity providers, products and technologies, these contributors are not restricted to Europe. The context of these results should be seen in a market where much of the technology being used in Europe is provided by organizations originating from outside Europe. The report identifies them through their European trade representations. For example, turnover being generated on Cybersecurity by PwC will be accounted for in the country where the trade is generated and recorded. This could be any country in Europe where PwC has an office. The trade flows do not take into account ownership of PwC on an international basis, or monetary flows between the national trade offices and the non-European headquarters. Whether this is important or irrelevant is up to the reader to judge. Many of these companies employ a significant number of people in the industry, not much different from any other part of the world where people are contributing to the economic value of Cybersecurity. See also Chapter 0 for further relevant analysis.

An early 2018 report by CB Insights¹, has presented 2017 as a record year in terms of global deals and financing in Cybersecurity. Later in 2018² this trend is likely to be continued on the basis of continuous quarterly reporting in news coverage of “data security”. In 2017 over 7 billion EUR was disclosed as having been invested in Cybersecurity companies, almost twice the amount of the year before. A significant portion of this investment came through ten investment rounds of over 100 million EUR. But equally important in the perspective of this report, is that 69% of these disclosed deals took place in the USA. With an additional 7% in Israel, 6% in the UK, 3% in Canada and 2% reported in China, only 14% of that disclosed 7 billion EUR (which is still nearly a billion EUR) investment, is being invested elsewhere in the world (including Europe). These numbers are quite similar to the number of global mergers and acquisitions that have been disclosed: the majority being in the USA, Israel and UK. While these figures indicate that it is very likely that not all transactions are being disclosed (especially the smaller transactions, the investments and acquisitions not being reported as Cybersecurity, or not being reported for confidential reasons – for instance for private companies), it is likely that this represents a trend which has been valid for quite a number of years.

¹ Cybersecurity Trends to Watch in 2018. Industry opportunities and startups to watch, CB Insights, January 2018

² The Future of Data Security. Startups, emerging technologies, and Big Tech's innovations on the cutting edge of data security.

Other studies report on the sheer number of Cybersecurity companies throughout the globe being recognised for their innovation. Again, quite a large proportion of companies from USA, Israel and UK appear. This study does not reflect directly on the innovativeness of these companies, or their technologies. This study does report on the way these companies trade, either through their indirect local representation or directly through their international headquarters. The fact that Israel does not appear as a significant originating country for imports of Cybersecurity products and services into any of the European Member States, and that the USA is not always the largest exporter put a slightly different perspective on these facts. An important finding of this study is that in the UK, public spending is the largest single contributor to the Cybersecurity market. Relative to most other European Member States, the UK government contributes directly to the interest and significance of the investment community in the market. In other words, one can assume that the amount of public spending in Cybersecurity (or any other industry for that matter) will likely increase the appetite to entrepreneurship and innovation, will increase the interest of the investment community and will increase the appetite of the private markets to rely upon UK-originating products and services rather than other European ones.

The context of this study has to be seen in a market that is constantly evolving, but still maturing. Other studies such as the Global Cybersecurity Index (GCI)³ by the ITU, a survey that measures the commitment of Member States to Cybersecurity in order to raise awareness, presents a similar picture of maturity on the basis of legal, technical, organizational, capacity building and cooperation. The study shows the global and European market leaders (UK, France, Netherlands) from the Cybersecurity Industry Market Analysis as countries leading in the GCI or maturing (Germany, Belgium, Spain, Italy). Both studies present a different, but complementary perspective on the state of Cybersecurity in Europe.

While a lot of public funding has been provided for Research and Development in Europe, one phenomenon is that this European-funded intellectual property finds its way back into the European market, by being traded by a non-European entity. While this might be the case, it is the result of the fabric of interwoven relations of Cybersecurity experts trying to find their most effective route to market, rather than mitigating the originating funds into its originating market. The maturity of a somewhat more single market overseas than Europe, embraces European expertise and technology in encryption technology and defines a standard with it (the current AES encryption technology), which has been adopted by companies and institutions all over the world. Both US and non-US originating companies are utilising this technology, creating new innovative products and technologies and improving the overall Cybersecurity with it, which in itself is already a major accomplishment.

The European Cybersecurity Market is a complex fabric of different solution and technology providers, which according to this study clearly varies according to the European Member States. In some of the larger European Cybersecurity markets such as UK, Germany, France and Spain, there are a large number of Cybersecurity early stage innovative technology companies, that can find their route to market. These often work closely with system integrators and advisory companies, which provide additional guidance, technology and maintenance support to the enterprise market. In addition, there are various established channels for distribution, business networks and supporting organizations. In other European countries, these system integrators and advisory companies are the most important Cybersecurity market operators. They focus on reselling and integrating known and established (mainly non-European) brands, because of historical reasons, people skills and experience. In many cases Cybersecurity will be offered in addition, or alongside other traditional ICT-services such as

³ Global Cybersecurity Index (GCI), ITU 2017.

network installation, management and maintenance, software development and systems integration or overall managed services. In countries with a less advanced ICT-history, both people and companies are lacking interest to invest interest and resources to learn, be trained and further support innovative European developments, rather than utilizing international references and removing complexities and liabilities with small innovative technology vendors with less of track record. Cybersecurity buyers are looking for reference materials, following industry analysts, their peer and reference installations. Only to a lesser extent are they looking for the most innovative and disruptive Cybersecurity solution.

Contrary to many other traditional industries, the Cybersecurity Industry in Europe is mostly lacking this industrial fabric of European entrepreneurship, that allows for innovative companies to thrive, for both public and private organizations to test, evaluate, improve new European Cybersecurity technologies, products and services. These types of mechanisms do exist in traditional technologies, manufacturing industries, traditional security, automotive and general purpose ICT. However, the Cybersecurity Industry needs to be constantly supported with innovation coming from Research and Development, as many innovative companies are being created on the basis of these activities and existing technology companies are continuously looking for additional functionalities and markets to further enhance their current offerings. Increasingly many of these innovations need to be driven through external challenges – customer driven, on the basis of new technologies and fundamental differentiating factors.

These innovations from European engineering expertise added to the enhanced fabric of support and open minds to Cybersecurity innovations, will be integrated into the European Cybersecurity Market, ensuring the sustainability and further growth of the European technology providers and users.

About the Authors

Ulrich Seldeslachts, LSEC – Leaders In Security, Editor-in-Chief

Chief Editor in Charge, Managing Director of LSEC – Leaders in Security. Ulrich has been active in the Cybersecurity Industry for more than a decade as head of LSEC, with direct relations to professional end-users, research institutions and large and small Cybersecurity Industry market operators, with policy makers and other interest groups. Ulrich has been leading most of the in-country workshops and is related to ECSO, the Cybersecurity public private partnership (PPP) as Member with LSEC and as chair of the WG2 on market and investment developments.

Richard Chisnall, LSEC – Leaders In Security, Chief Editor

Richard has been leading the workshops and discussions with the industry in the two workshops in the UK. He has been instrumental in editing and reviewing the contents of the report. Richard has been in the Security and Defence Industry for more than 30 years, and has been involved in Cybersecurity for the last decade.

Neil Adams, LSEC – Leaders In Security, Chief Editor

Neil has been reviewing and providing inputs on the data analysis used, contributing the workshops in Belgium and in UK, ensuring consistency with high attention to detail in the study and the works. Neil has been involved as a Security expert for the last 20 years and in Cybersecurity for the last decade.

Chris Pickering, LSEC – Leaders In Security, Chief Editor

Chris has been leading the workshop and discussions in Italy and UK, with the industry. He has been providing significant contributions in the reporting and integration of the workshop results and perspectives in the report. Chris has been active in the domain of Security and Defence, and is an industry expert. Has been active in Cybersecurity in the last decade.

Wim Stoffelen, LSEC – Leaders In Security, Editor

Wim has been coordinating and reporting on the workshops, collecting feedback and interacting with the industry partners that made the organisation of the local workshops possible. He has been key in processing the workshop contents and inputs for this report. Wim has an extensive background in Cybersecurity during the last decade.

Martyn Poessinouw, LSEC – Leaders In Security , Editor

Martyn has been doing the data crunching and first level analysis from within kMatrix, a Competitive Market Intelligence company, active in Security for more than a decade and working on Cybersecurity for the last 3 years. Martyn has been dealing with the big data sets and ensuring data compliance. He has been a key contributor to this report.

Key workshop partners included : ECSO (the European Cybersecurity Organization), LSEC – Leaders In Security, HSD (The Hague Security Delta), Pôle SCS, ECO, INCIBE, Rhode Schwarz, Satways, Demokritos, Ericsson, Ciptor, Leonardo Group, Heliview, IBM, The UK Cybersecurity Forum and Cybersec.

Introduction to the CIMA report : scope, considerations, sources, structure, target audience

Scope of the study

The purpose of this study is to provide DG CONNECT with an independent and unbiased market analysis of the Cybersecurity industry within the European Union (EU). The study aims to promote the take-up and the supply of secure ICT solutions in the EU in order to improve the overall security of European ICT systems.

For this purpose, this study covers:

- The analysis of the current and future European Cybersecurity market trends;
- The analysis of other relevant countries from a global perspective (and including markets such as Asia, and North and South America);
- The study of current Cybersecurity products and services;
- The topology of the market, including market flows and barriers found by providers when selling their products and services;
- The strengths, weaknesses and opportunities of the European Cybersecurity market;
- The analysis of the role of the European Commission, European agencies and National Governments;
- Major European Cybersecurity industry players;
- A perspective on a way to differentiate the market and suggestions for specific policies to support the markets, based upon their maturity levels

The Quantitative Research methodology employed, the “CIMA methodology”, relies on a core analytical system called Profiling that is used to track technology and market change using “big data” techniques, analytical data grids, business case studies and industry-level research to provide probabilistic and measurable evidence about how companies/ economies adapt to and perform within changing market conditions. This approach is suited to providing multi-sourced "big data" solutions to define and quantify previously unobserved or "difficult-to-measure" markets where standard industrial classification systems are non-existent, restricted or rapidly out-dated. The methodology provides internally consistent global research, based upon market intelligence sources and rules rather than national statistics, that can be used to measure economic sectors that are not well represented by Standard Industrial Classification (SIC) codes or industry bodies and provides a flexible/ adaptable data structure with multiple levels of detail and multiple measures that are consistent across international boundaries. However, the process is able to report out through SIC code systems and the Nomenclature of Units for Territorial Statistics (NUTS) classification of administrative areas, where appropriate if so required. The multi-sourced approach can operate in areas where other approaches based on a National statistical approach or Trade/ industry approach (including survey techniques) either do not exist or are poorly aligned with the sector/ market under investigation, but has the limitation therefore of not being directly comparable with traditional statistics.

As introduced in Chapter 0 and described in detail in Chapter 0, the adopted model is based upon a bottom-up identification, analysis, measurement and quantification of traded Cybersecurity activities, that would be understood by practitioners in the field, and that are then organised into a hierarchical structure that is used to aggregate and then report the results. In doing so, the research has included the widest range of (measurable) activities that fit the definition, including activities by companies that are specialists in Cybersecurity sector and by companies that may be non- specialist but operate within the Cybersecurity supply/ value chain. One of the reasons that the value for the Cybersecurity sector in this report is higher than in most (not all) other research reports is that the search for evidence is conducted on a very broad base. This is a deliberate feature for a global reporting system

that must be able to accommodate national variations in definition without losing the ability to compare results across multiple continents or countries. This has allowed the analysis to for example show how Cybersecurity activities and companies have emerged from a wide range of market sectors, in particular from companies whose core businesses are Defence/ Aerospace and Security, and not primarily from the ICT sector.

The main conclusions and recommendations were found during the development of the report. These were debated with industry representatives from various Member States during workshops held between June and October 2017. During these workshops, the presented outcomes were validated as fit for their purpose, additional questions were raised by participants on the meaning and structures of the presented data, suggestions were made to restructure (Identity Management, Situational Awareness, and other categories – Training category was added), a small number of additional observations were made and are part of this report. The workshops were additionally used to evaluate assumptions and conclusions made during the analysis. Discussions were held on the qualitative level and additional analysis that needed to be undertaken (for instance looking at the country reports in comparison to GDP or population). The study has been structured in 6 phases, including an inception phase, a stakeholder engagement process, a first progress report, a second progress report (with a market analysis and an industrial Cybersecurity landscape analysis), a final report with a SWOT analysis and main findings. The phases are shown in the following figure:

Figure 1 : Phases of the study



In order to collect information about the current status of the Cybersecurity market in Europe, the consortium LSEC-PwC investigated the current market situation on the basis of market intelligence from over 900 different sources of data. The collected data from the years prior to 2016 showed that the approach of a wide industry market study on a voluntary basis would not provide any significant result and insight over the European Cybersecurity Industry Market.

The assumption that the European Cybersecurity Market could be investigated by a web survey across different member states, was countered by the fact that already in 2015 over 40,000 companies were active in the domain of Cybersecurity in Europe. Within the timescales provided and the requirements listed, organizing a representative survey would not have been feasible.

In order to answer all relevant questions (not all of them could be fully answered from the collected datasets) and to better understand some of the market dynamics, the consortium proposed to organize a series of workshops in different Member States. Participants were invited from different Cybersecurity solutions and services providers, with different backgrounds, market focus areas and levels of maturity. These company representatives were presented with the preliminary outcomes and results of the study, and invited to participate in a discussion and debate on the presented facts and figures, asked to comment on some of the qualitative questions from the Industry study.

This document covers the following:

- The analysis of the industrial Cybersecurity market regarding all Member States (with an assessment of the market size, existing sectors, trends, products and topology);
- The analysis of the current situation of the European industrial Cybersecurity market, and the evolution it will undergo in the upcoming years;
- A comparison between the European Cybersecurity market and other relevant regions;

- The analysis of the current situation of the European business landscape (studying providers, competitors, the market fragmentation, the gap between European necessities and European products and services, exports, imports, investment and main barriers);
- A SWOT analysis of the European Cybersecurity market; and
- The main findings and conclusions drawn during the development of the study.

Main considerations

This document is the final report of the project and contains **all results of the study, both the parts developed in 2016 and the updated components in 2017/18**. This study was done independently, and gathered data directly from European companies and organisations during face to face interviews, surveys and through workshops and conferences, and from different independent data sources and other market intelligence. From prior studies, the reliability of the results of the latter will be averaging over 85%.

The document contains two major parts : the first part contains the independent study done in 2017/18. This was executed by PwC together with LSEC. The second part of the document contains components done during the study in 2016, done by PwC together with Everis.

Jointly the document combines the various components requested by the official tender, and gradually adds more detail and information in the process.

Sources

The sources of the data used in the study are:

- **Desktop research and previous studies:** Over 900 different sources were used for the collection of data for the quantitative research and analysis of the underlying results. In addition, several previous studies were analysed and taken into consideration for the elaboration of the analysis. The sources used to develop the study are included in

Appendix I : Data Sources.

- **Workshops:** workshops were held from June 2017 until September 2017 with representatives of the European Cybersecurity Industry. During these workshops some of the quantitative data were presented and debates and discussions were held on the factual results, questioning the results and outcomes and considering some rationale for some of the results. These discussions led to further in-depth study of some of the components during additional quantitative data research. Some of the quantitative discussions were focused on improving the current situation for the European Cybersecurity Industry as a whole, and some specific markets. New areas of interest from the demand side were identified during the workshop.
- **The Global State of Information Security® Survey (GSIS Survey):** this survey of experts from different sectors is conducted every year by PwC.
- **Cybersecurity Market Survey (CM Survey):** for this study several ad-hoc on-line surveys, addressed at both consumers and providers of IT security solutions were held in 2015 - 2016. The CM Survey had received 388 answers from 43 different countries and served as a consideration for the further quantitative analysis and qualitative debate in 2017.
- **Contact with national associations and Cybersecurity authorities:** for the quantitative analysis of each of the 28 European Union Member States (EU-28), 20 different trade associations provided quantitative data regarding national Cybersecurity markets in 2015 - 2016, allowing a comparison with quantitative data in 2017.

Document structure

The information offered in this document is structured as follows:

- Document guidance comprising: **Glossaries; Index; Table of Figures and Table of Tables**
- **Chapter 0 :Executive Summary**
- **Chapter 0 : Background**
- **Chapter 0 : Context and Considerations**
- **Chapter 0 : About the Authors : Brief biographical details of the principal authors**
- **Chapter 0 : Introduction** to the CIMA report : scope, considerations, sources, structure, target audience
- **Chapter 0 : Quantitative Cybersecurity Research** : describes the definition for Cybersecurity used as part of the study, relating to its historical perspective, its data sources and identifying the various sub-categories containing the hundreds of products and different underlying levels of categorization. This chapter also elaborates on the used methodology and outlines its underlying analysis and scrutinizing the various data sources.
- **Chapter 0 : Global Cybersecurity Market** : this chapter describes the Global Cybersecurity market, including the market volume, number of companies, growth at worldwide level, indicating details from different continents and major countries such as US and Japan. These statistics allow for a comparison with the European market as a whole, and with some of the leading European Member States, appearing in the top 20 on a global scale.
- **Chapter 0 : EU Cybersecurity Market** : this chapter describes the European Cybersecurity market, including the market volume, growth rate and the products and services available in Europe as a whole and in Appendix A on specific country levels. Chapter 0 also includes some of the key measures, identifies the sub-sectors and indicates the number of companies, including the way some of the main providers have been identified. The chapter also clarifies the main types of sectors on the buy side, where most organizations acquiring sold products and services can be categorized under. Finally, the chapter identifies the import and exports on a global basis and within the EU.
- **Chapter 0 : EU Competitiveness** : an analysis of the key trade flows between the EU and other nation States, export vs import perspectives.
- **Chapter 0 : Workshops** : Overview of the workshops held, location
- **Chapter 0 : Analysis related to the pre-defined study requirements** : Interpretation of the study requirements, methodology and findings.
- **Chapter 0 : SWOT Analysis of the European Cybersecurity Industry**
- **Chapter 0 : Conclusions and Recommendations on the Cybersecurity Industry Market Analysis of the European Market : Analysis of the findings and key observations**
- **0 : Appendix A : EU Country Level Data** : A characterisation for each of the 28 Member States analysing the same parameters individually, mainly today on sub category level of sales activities, to allow for a more granular comparison between EU Member States, in terms of levels of maturity and potentially focus areas.
- **0 : Appendix B : EU Sales by Sub-sector and Purchaser Industry** : an attempt to identify the key End- User markets, by Industry and Sub-level 2 Categories
- **0 : Appendix C : Imports by Country of Origin per EU Member State**
- **0 : Appendix D : Exports by Country of Origin per EU Member State**
- **0 : Appendix E : Competitive Dashboards** : Trade flow data for EU, competitors and each of the 28 Member States
- **0 : Appendix F : Trade Flows by Sub-sector** : Trade flow by sub-sector for EU and competitors

- **0 : Appendix G : Research Methodology Confidence Levels** : this chapter clarifies the used methodology and provides some additional levels of confidence and clarification on the levels of confidence, on its reliability of the project numbers and statistics. The factual support to the data analysis.
- **0 : Appendix H : Taxonomy – Cybersecurity Data Level 2 – 4 Definitions**: provides further detail on the use of the definition of Cybersecurity market, its subcomponents on Level 2, and how it breaks down into various underlying levels, which in the end are connected to actual product and services.
- **0 : Appendix I : Data Sources**: a list of over 900 data sources used to collect the big data driving the analysis and the factual market results.
- **0 : Appendix J : List of Acronyms**: used to identify the Member States and other important acronyms.
- **0 : Appendix K : Top 500 Global Cybersecurity Companies**: part of the study results, a list of companies to identify European companies active on a global basis, a listing on the basis of the high growth ranking (and on the basis of their headquarter)
- **0 : Appendix L : Participant organisations in the CIMA workshops**
- **0 : Appendix M : Results from workshops**
- **0 : Appendix N : Cybersecurity Research Methodology 2017**

Intended audience for this document

The intended audience for this document is:

- European Commission – DG CONNECT – Unit Trust & Security and other units dealing with Cybersecurity.
- European Member States’ representatives, MEPs and their respective administrations
- Selected European Cybersecurity Industry Market representatives
- Selected European Cybersecurity Catalysts, Clusters, Associations and industry collective representations

Its main purpose is to stimulate further discussion and debate, in order for further analyse the European Cybersecurity Industry and to allow further debate for the European and Member State Cybersecurity Industry policies and Cybersecurity strategies.

Quantitative Cybersecurity Research

This report includes quantitative analysis of the global Cybersecurity market, with specific reference to the performance of the 28 countries of the European Union.

Defining the Cybersecurity Market, Taxonomy and Scope

The current Cybersecurity research is based upon a research programme that started in the UK in 2006 and has reported to national government on the global Security market for 10 years and on Cybersecurity for five years.

An initial Cybersecurity definition was created in 2010, updated in 2013 and in 2014 to reflect significant changes in the content and reporting of Cyber activities. This history reflects the constantly changing nature of an emerging sector. Cybersecurity is defined as an industry that responds to the escalating challenges of maintaining the confidentiality, integrity, availability and resilience of Cyberspace and to counter "deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or network or the information and/ or programmes resident in or transiting these systems or networks. "

The 2014 definition was "road- tested" as part of a programmes of workshops conducted across 10 EU countries. It was also closely reviewed by the European Cybersecurity Organisation (ECISO) at both the beginning and end of the research programme. As a result, a few Cybersecurity activities within the 2014 definition have been re-allocated between the 13 sub-sectors of Cybersecurity and, it is important to note, no gaps were identified in the definition.

Key points about the Cybersecurity definition used for this report are:

- The data set for this report, therefore, includes recent data (2015/16) and historical data to 2014 and earlier. The current definition has evolved since its first introduction in 2010 and will continue to evolve i.e. at any point, the definition is a "freeze- frame" on what is happening in the industry.
- Any proposed changes to the definition are investigated to ensure that they are quantifiable and additions to the definition are "run backwards" to ensure that data history and trend analysis is maintained
- Data is structured to enable multiple coding, filtering and reporting of the data without changing the underlying data structure. In this way, definitions can be "dynamic" without losing content and context.

The data set for this report, therefore, includes current year data (2016) and historical data to 2014 and earlier.

The slightly revised definition for this research includes 13 sub-sectors of Cybersecurity. These are:

• Anti- Malware	• Infrastructure
• Application Security	• Mobile
• Business Continuity	• Outsourced/ Managed Services
• Cyber Consultancy	• Situational Awareness
• Cyber Insurance	• Systems Recovery
• Encryption	• Training & Education.
• Identity and Access	

These sub-sectors are described in more detail in the Glossary and in Appendix H.

The **Cybersecurity data set used for this research includes 1,100 products and services**, aggregated (by supply or value chain activity) into four data levels and then reported for the 13 sub-sectors. All products and services are also coded, so that they can be reported according to different definitions or different needs. The current sector definition includes the widest possible range of cyber- related activities on the principle that it is easier to filter- out activities for any specific analysis than it is to add them to the data set at a later point⁴.

To identify Cybersecurity activities to be included as part of the definition, the research approach included several stages:

- Scoping the broader economic sectors of ICT, Logistics, R&D, Manufacturing, Services, Electronics, Defence, Telecommunications, Security etc. within which Cybersecurity activities reside
- Isolating and then validating those activities from the broader sectors that fit with the proposed definition of Cybersecurity
- Examining the data and sources within those sectors to construct an evidence base of sources that can be used to measure Cybersecurity across multiple metrics
- Examining the data and sources further, to ensure that the Cybersecurity activities can be clearly differentiated from economic activities that are generated due to other reasons.

Further information about sector definition and boundaries and the challenges of quantifying an emerging sector will be included in the forthcoming quantitative research methodology.

Methodology

The full quantitative research methodology is documented in detail separately to this draft report, but a brief description is included below. Key points about the methodology are:

- It employs a big data approach to curating economic and markets values from multiple data sources
- The data can be sourced from all economic sectors- not just Cybersecurity sources
- Data sources are global and so is the data set. Use of common descriptions for products and services means that Cybersecurity can be measured across national boundaries and classification systems to capture inter- trading between all the major economies
- The methodology has been “in play” for over 10- years across multiple difficult-to-measure sectors- including Security since 2006 and Cybersecurity since 2010.

Standard Industrial Classification Systems (SIC) or European NACE codes are currently poorly equipped to measure Cybersecurity activities and industry survey approaches have achieved limited results, so

⁴ While the definition of Cybersecurity is consistent with earlier works in Cybersecurity Industry Market assessments, the final taxonomy of Cybersecurity sub sectors will be different. A detailed and rigorous mapping exercise conducted across the earlier definitions confirmed that all previously defined categories of Cybersecurity products and services are included within the current definition and taxonomy, but that the current use is much broader and including domains and sources not earlier identified.

the adopted multi- source approach creates new and robust economic values from other sources of data.

With no definitive sources of data available, the key task is to identify meaningful and multiple sources of transactional (and other) data and use this to populate a detailed and segmented model of Cybersecurity that transforms the available evidence from singular and fragmented insights into structured observations. Much of this data is already in the public domain, but needs the corroboration of multiple sources (using Big Data analytics) before it can be validated and made fit-for-purpose.

The research creates and applies a wide range of domestic and international metrics. Domestic metrics include sales, employment, company count, historical/ forecast growth and innovation and are used to establish the economic baseline for Cybersecurity at the national level. International metrics include imports, exports, trade flow and market share and provide a competitive context for performance benchmarking and market opportunity analysis.

All values (data points), as per the above metrics, are generated from multiple sources of evidence, collected and managed as part of a source information system. All data sources are tracked over time and routinely tested for reliability, robustness and accuracy before being selected to calculate a specific data point. Each calculation includes between 10-200 sources and the reported value is based upon the “mean” derived from these sources.

Market forecasts are calculated in a similar way to other metrics, i.e. from multiple sources, but with one exception. Forecast sources are also assessed for their “hit rate” or historical level of accuracy and this factor introduces a “weighting” element into the calculation that is not included for other metrics. Historical growth may be used to “smooth” the forecast results, depending on the level of uncertainty (spread of forecast values) in the selected sources.

Confidence in data values is a key feature of the quality assurance (QA) process and is applied to all key metrics. A data confidence level is calculated based upon the difference between the “mean” value and the upper and lower values in the list of sources selected for that data point. Typically, 85% is the target confidence level i.e. the differences in the sources fall between +/- 15%. Other QA techniques include multiple check points between countries and across different sectors, “deep dives” into specific data points and time series analysis.

The research includes activities by companies that are specialists in Cybersecurity sector and by companies that may be non- specialist but operate within the Cybersecurity supply/ value chain. The source data, therefore, includes following categories:

1. Companies that solely provide Cybersecurity products and services
2. Companies that (amongst other activities) provide Cybersecurity products and services
3. Companies that provide products and services that form part of the Cybersecurity supply/ value chain.

Category 2 includes Defence, Security, ICT, Research and Professional Service organisations that provide Cybersecurity as part of a wider portfolio of activities or that provide Cybersecurity as part of a wider ICT/ Security solution.

Over 900 sources have been used for the research. These include Cybersecurity sources, other industry sources, financial, investor, academic, insurance, legal, procurement sources as well as

company sources. Data sources are tracked over time, with a history based upon source name, source value, year it relates to, the number of times used, "hit rate" (a measure of reliability) and whether it is to be accepted for a specific research purpose or applied to a specific metric.

Cybersecurity Industry Models

This research has adopted a single model of the Cybersecurity industry. This includes a definition and a taxonomy of Cybersecurity activities that fit within that definition. As described in the accompanying methodology document, the adopted model is based upon a bottom-up identification, analysis, measurement and quantification of traded Cybersecurity activities that are then organised into a hierarchical structure that is used to aggregate and then report the results. This model has the advantage of being:

- Pragmatic- only activities that can be robustly measured are included, and
- Practical- lower level activities can be added to and reorganised, (the result of the underlying study, following discussions with ECSO-members and during in-country workshop from June 2017 through October 2017), without losing data integrity, reporting integrity or data history
- Flexible- Cybersecurity data captured in this way can be adapted to different models of the industry.

One such exercise was conducted at the very beginning of this research process, to demonstrate that the adopted research definition and taxonomy captured the widest possible range of Cybersecurity activities. But also, during the conduct of this research, other national taxonomy models of Cybersecurity have been taken into consideration to come up with the underlying taxonomy model:

- UK, thematic approach to Security, including Cybersecurity, for exports (Frost & Sullivan)- July 2017
- Spain, catalogue of Cybersecurity solutions (Spanish National Cybersecurity Institute)- April 2016
- France, Cybersecurity & Digital Trust (Hexatrust)- 2017
- EU, Cyberwatching.eu, (Wallom)- 2017

Each approach has different strengths and provides theoretical, quantitative or practical insights (but not all three) into what Cybersecurity means, what it contains and who provides it. Given the emergent nature of the sector it is unsurprising that different approaches and definitions co-exist and that no standard approach has yet been adopted. It is likely, based upon our experience of other emerging sectors, that this will continue for some time.

The approach taken in this research and report is to focus on the process of measurement, quantification and comparability/ trend analysis by developing and maintaining a global data set that is unconstrained by national preferences or definitions, but reflects national differences in Cybersecurity activities and performance. This data set is detailed, updatable and flexible in that the data can be re-coded to fit with other conceptual models of the sector and with existing national definitions. In the simplest terms if the data at the bottom of the hierarchy (Level 5) is detailed, robust and varied, then all the intermediate reporting levels (Level 4 to 2) can be flexible in how the data is aggregated and "labelled." So, the focus has been on developing a detailed evidence base of Cybersecurity activities that provides a "best fit" but evolving sector definition and taxonomy of products and services that can be redesigned to reflect future changes.

In doing so, the research has included the widest range of (measurable) activities that fit the definition, from the widest range of providers, whether they be Cybersecurity companies or companies in other industries that provide Cybersecurity solutions. One of the reasons that the value for the Cybersecurity sector in this report is higher than in most (not all) other research reports is that the search for evidence is conducted on a very broad base. This is a deliberate feature for a global reporting system that must be able to accommodate national variations in definition without losing the ability to compare results across multiple continents or countries.

Global Cybersecurity Market

Introduction

This chapter of the report focuses on global sales, companies, employment and growth for the Cybersecurity sector. The analysis in this section relates to the size of the Cybersecurity sector, its geographical distribution, sub-sector performance historical and forecast growth and the relative economic performance of the larger global economies.

The size of the global Cybersecurity market has been calculated using a very wide range of sources (listed at Appendix I) and is measured by global sales across 226 countries or independent economies. Confidence levels for the global data are included in **Appendix G : Research Methodology Confidence Levels** (as per the methodology statement). The value for the Cybersecurity sector in this report is higher than in most (not all) other research reports because the search for evidence covers a very broad base which allows the accommodation of national variations in definition without losing the ability to compare results across multiple continents or countries.

Global Cybersecurity Key Metrics

This section of the report focuses on four key metrics:

- **Sales** is a measure of economic activity by identified companies and their supply chain within a defined country, based upon where the economic activity is delivered from rather than where it is reported.
- **Companies** is a measure of the total number of companies in a country that are either core to the delivery of sector products & services or form an integral part of the supply chain.
- **Employment** is a measure of the level of employment, in Whole Time Equivalents (WTEs), across core and supply chain companies involved in delivering sector products/ services.
- **Growth** is an historical and forecast measure of the annual percentage rate of change in sales. Currently, historical growth trends are recorded for many metrics (Sales, Imports, Exports, Employment) but **forecast** growth is only applied to Sales and Exports.

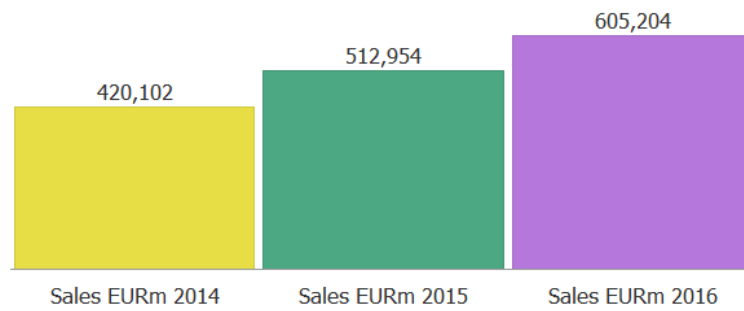
1.1.1 Key Learnings

The Cybersecurity market is globally a EUR 600 billion market, and is expected to grow in the next five years on average by approximately 17% both in terms of sales, number of companies and employment. The largest market is North America, followed by Asia and Europe. Africa is significantly lagging behind. This report splits the Cybersecurity market into 13 major sub categories, indicating a balanced spread on global basis between activities in Situational Awareness (21%), Infrastructure (18%) and Application Security (16%). However, these results are mainly driven by the top global contributing markets and countries to the total market. The USA and the EU combined for instance contribute more than half (over EUR 309 billion) to the global Cybersecurity market.

1.1.2 Analysis

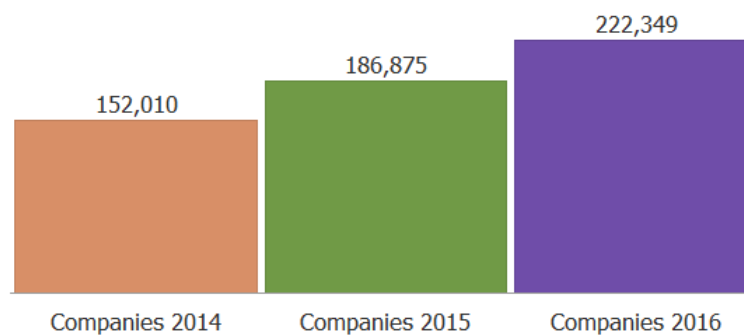
The total for Cybersecurity sales in 2016 was EUR 605,204 million (see Figure 2). This was an increase of **18%** on 2015 sales of EUR 514,954 million. This compares with an increase of **22%** between 2014-2015.

Figure 2 : Global Cybersecurity Sales 2014 to 2016 (m EUR)



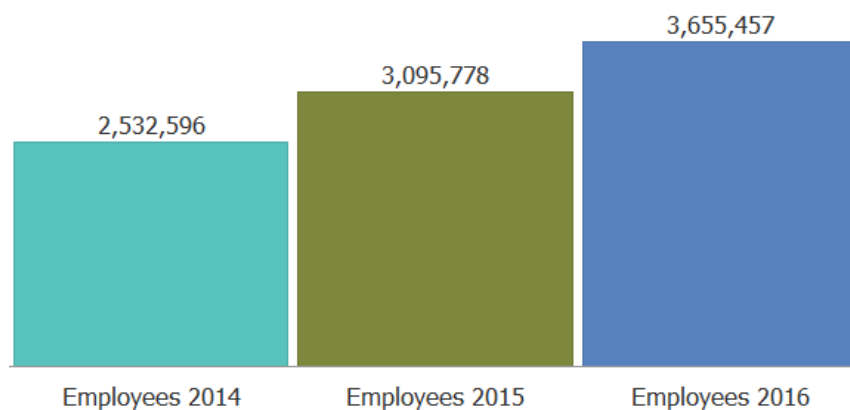
The total for number of Cybersecurity companies in 2016 was 222,350 (see Figure 3). This was an increase of **19%** on the 2015 company count of 186,875. This compares with an increase of **23%** between 2014- 2015.

Figure 3 : Global Total Number of Cybersecurity Companies 2014 to 2016



The total for Cybersecurity employment in 2016 was 3.7m (see Figure 4). This was an increase of **18%** on the 2015 employment count of 3.1m. This compares with an increase of **22%** between 2014- 2015.

Figure 4 : Global Cybersecurity Employment 2014 to 2016

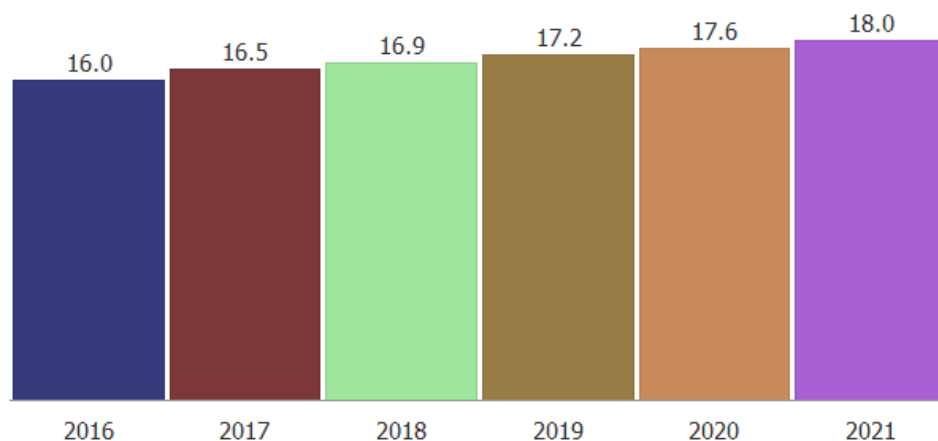


Historical growth for the past two years was 22% (2014-15) and 18% (2015-16). Global forecast growth is 16% for 2016, increasing to 18% by 2021. Growth forecasts for this research are based upon analysis of multiple forecasts and are calculated as a weighted mean based upon the 2016 level of sales.

1.1.3 Forecasts

The forecast growth rates are significantly lower than recent historical growth and this has been a feature of growth forecasts over the past 5 years, which have typically understated future growth by 4-5%. Therefore, the growth rates at Figure 5 should not be read as a significant fall-off in Cybersecurity growth, but reflect a lag between market forecasts and actual industry performance. This phenomenon is not restricted to Cybersecurity and has been observed across several emerging sectors.

Figure 5 : Global Cybersecurity Forecast Sales Growth 2016 to 2021



1.1.4 Conclusions and Recommendations

The global Cybersecurity market has grown rapidly over the last 3 years (above 18%) with the number of global companies and employment growing at the same rate, and is forecast to continue growing rapidly at a similar rate out to 2021.

The EU Cybersecurity companies should be encouraged and supported to reap the potential benefits of the anticipated further global growth of Cybersecurity products and services. The EU should continue actively and proactively to take actions to support the development of an EU Digital Single Cybersecurity market, including utilising that strategy in international collaboration, to prevent risks and dangers from cybercriminal activities happening from and within the EU.

Global Cybersecurity by Sub-sector

Cybersecurity has been divided into 13 sub-sectors, each of which is described briefly in the Glossary and in more detail (including a description of the types of products and services which are included in these subcategories) in Appendix H. These sub-sectors show different levels of historical growth.

1.1.5 Key Learnings

The Cybersecurity market has been divided into 13 sub-sectors (categories), collected through different layers (five detailed in this report), representing over 1100 different product categories. From both sales, company and employment perspective, Situational Awareness was the largest market, followed by Infrastructure and Application Security spending. It is worrisome that only EUR 513 million is being spent in Training and Education. Unfortunately, this is a global trend, that can partially be explained by the fact that it is likely that training and education will be linked directly to products and services. Slight differences appear when comparing global Cybersecurity markets to Europe, and there are further variations in the Member State analysis, so additional indicators for different levels of maturity for these Member States have been used.

1.1.6 Analysis

Table 1 compares sub-sector sales for the period 2014 to 2016. Growth rates between 2014 and 2015 are uniformly higher than for 2015 to 2016. The highest growth sub-sectors across both periods are: Outsourced/ Managed Services, Encryption, Identity & Access, Infrastructure and Cyber Consultancy. Faster

Table 1 : Global Cybersecurity Sales (m EUR) 2014 to 2016

Level 2	2014	Growth %	2015	Growth %	2016
Situational Awareness	92.901	20	111.081	17	129.586
Infrastructure	74.316	26	93.317	17	109.594
Application Security	68.100	19	80.779	21	97.734
System Recovery & Data Cleansing	61.683	22	75.346	18	88.840
Business Continuity	32.870	23	40.456	13	45.591
Identity & Access	21.666	32	28.699	25	35.825
Anti Malware	24.733	18	29.285	21	35.548
Cyber Security Insurance	15.985	16	18.502	10	20.384
Mobile	8.994	17	10.528	12	11.802
Encryption	5.982	37	8.195	22	9.981
Cyber Consultancy	6.722	25	8.420	18	9.952
Outsourced/Managed Services	5.803	35	7.858	25	9.852
Training & Education	449	9	488	5	513
Total	420.205	22	512.954	18	605.204

Figure 6 : Global Cybersecurity Sub Level 2 Category Spread for 2016 in %

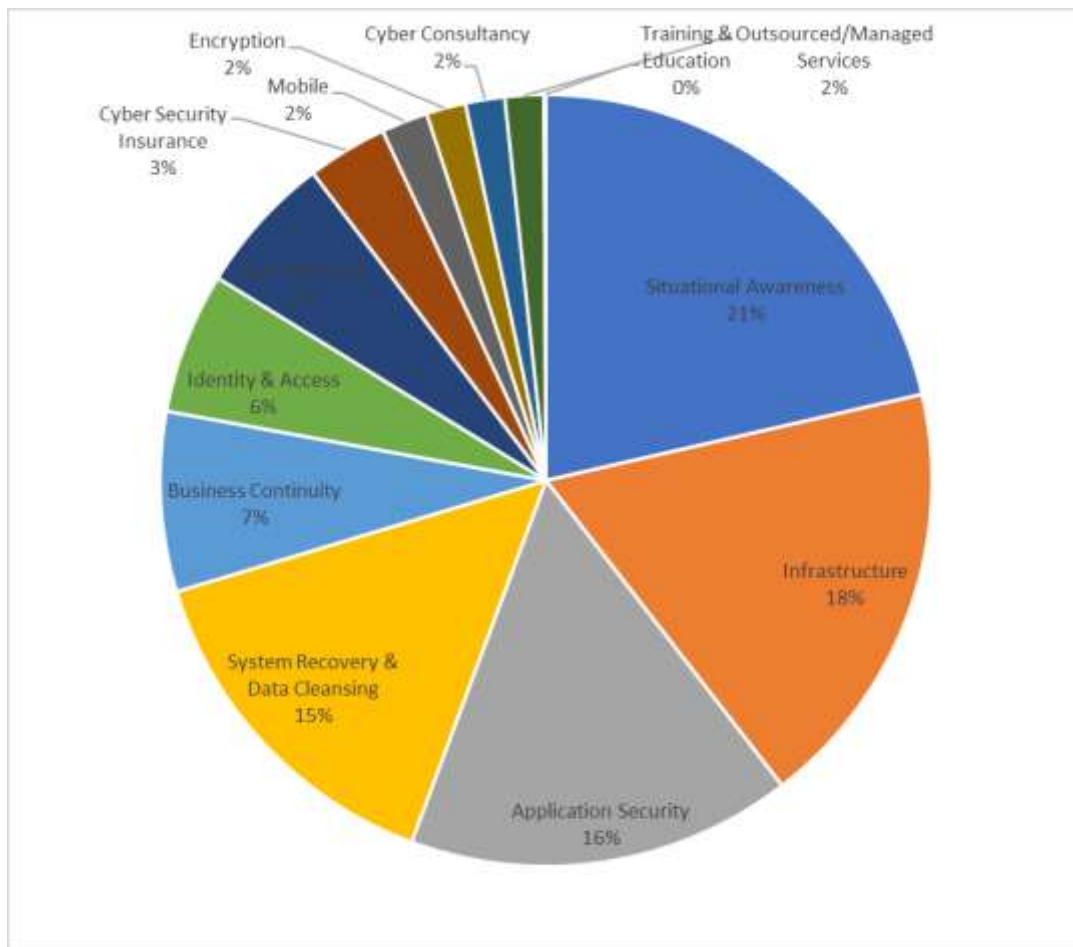


Table 2 compares sub-sector company count for the period 2014 to 2016. The highest growth sub-sectors across both periods are, once again: Outsourced/ Managed Services, Encryption, Identity & Access, Infrastructure and Cyber Consultancy.

Table 2 : Global Number of Cybersecurity Companies 2014 to 2016

Level 2	2014	Growth %	2015	Growth %	2016
Situational Awareness	30.939	20	37.107	17	43.246
Infrastructure	28.717	24	35.667	17	41.903
Application Security	20.831	21	25.111	23	30.984
System Recovery & Data Cleansing	21.058	23	25.913	17	30.225
Identity & Access	10.382	35	13.980	29	17.966
Business Continuity	11.089	23	13.645	14	15.546
Anti Malware	7.998	17	9.325	21	11.241
Cyber Security Insurance	8.049	12	9.039	11	9.991
Encryption	3.150	40	4.404	29	5.692
Outsourced/Managed Services	2.975	40	4.168	30	5.410
Cyber Consultancy	3.400	29	4.389	21	5.305
Mobile	2.898	23	3.553	19	4.230
Training & Education	524	10	575	6	609
Total	152.010	23	186.875	19	222.349

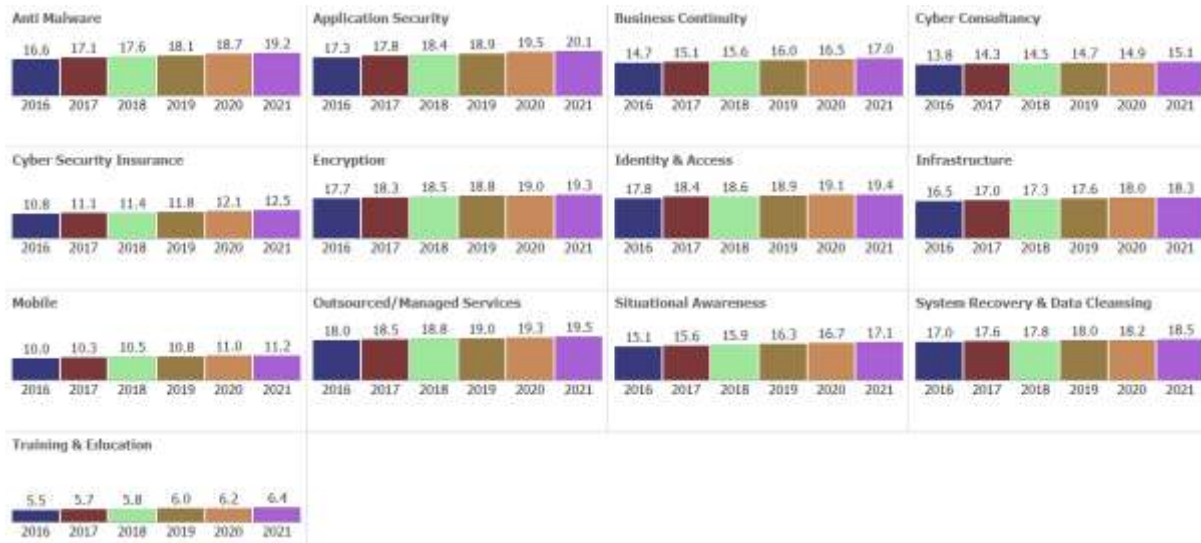
Table 3 compares sub-sector employment for the period 2014 to 2016. The highest growth sub-sectors across both periods are, once again: Outsourced/ Managed Services, Encryption, Identity & Access, Infrastructure and Cyber Consultancy..

Table 3 : Global Cybersecurity Employment, number of people active in Cybersecurity from 2014 to 2016

Level 2	2014	Growth %	2015	Growth %	2016
Situational Awareness	534.869	20	640.860	17	747.030
Infrastructure	445.605	23	547.026	17	640.694
Application Security	395.975	19	471.301	21	569.374
System Recovery & Data Cleansing	344.632	23	423.967	17	496.461
Identity & Access	156.962	38	216.943	32	286.051
Business Continuity	188.951	23	232.378	14	265.379
Anti Malware	151.636	17	177.275	19	210.389
Cyber Security Insurance	111.473	14	127.179	13	143.473
Mobile	67.000	17	78.087	12	87.102
Encryption	43.977	37	60.404	22	73.660
Cyber Consultancy	47.465	27	60.152	19	71.484
Outsourced/Managed Services	41.279	38	57.118	24	71.003
Training & Education	2.773	11	3.089	9	3.359
Total	2.532.596	22	3.095.778	18	3.665.457

Forecast growth for the 13 sub-sectors also varies for global Cybersecurity. Figure 5 demonstrates a wide variation in growth between Training & Education (single digit growth) and Outsourced/ Managed Services (18% growth). Once again, there is a mismatch between historical and forecast growth rates, so the forecast rates in Figure 5 are indicative of continued future growth but probably understate that growth by 4-5% (at least for the next 2-3 years).

Figure 7 : Global Cybersecurity Forecast Growth 2016 to 2021 by Sub-sector



Tables 1-3 and Figure 5 demonstrate that Cybersecurity growth is consistently high across all sub-sectors, that high growth is set to continue, with the suggestion (to be proven over the next 1- 2 years) that global sector growth rates may have plateaued.

The drivers for growth (evidence drawn from the source materials used to compile the forecasts) have been, and remain:

- Increasing levels of cyber- crime and reported costs of cyber- crime
- The widening range of targets for cyber- crime i.e. public, private and individual
- Increasing levels of awareness and responsiveness to cyber- crime
- Increased exposure to cyber- crime as more business and private activity goes online
- Increased levels of compliance requirements and reporting in relation to Cybersecurity
- Increase in national and international Cybersecurity initiatives relating to critical infrastructure protection
- Better industry sources leading to greater value/ activity capture, specifically for Cybersecurity
- Shift within the IT industry itself to reclassify some existing activities as Cybersecurity.

While levels of cyber- crime are predicted to continue increasing, the research data suggests that the reclassification of Cyber activities is probably approaching completion, ending the “artificial” element of growth arising from the re-labelling of market activities. It is also likely that the major “catch-up” element of investment in Cybersecurity has mostly passed and that future market demand will be driven from a more predictable and consistent “invested” baseline with budgets for further and future procurements.

1.1.7 Conclusions and Recommendations

The global Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, varying from 5% for Training and Education to 25% for Identity and Access and for Outsourced/ Managed Services in 2015/16, with the number of global companies and employment growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per

annum out to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%.

Most investment has gone into Situational Awareness – related activities: systems, technologies, services and people supporting a better understanding of the information related to Cybersecurity incidents. Overall mostly investment has been going in technologies and supporting advisory services, such as integration, whilst training and education was clearly not in balance with this investment in overall architecture. This has been a trend for over the last 3 years, and is set to continue. On a global basis, it is clear that with less than 1 percent of spending in training and education, and in combination with consultancy and managed services, Cybersecurity has mainly been a technology market.

During the workshops (see also Chapter 0), participants from the various European Member States recommended a stronger activity from the European market players in other global markets. Participants suggested for some larger European groups to have a stronger European presence that could be identified as European on a global level.

Global Cybersecurity Sales by Geography

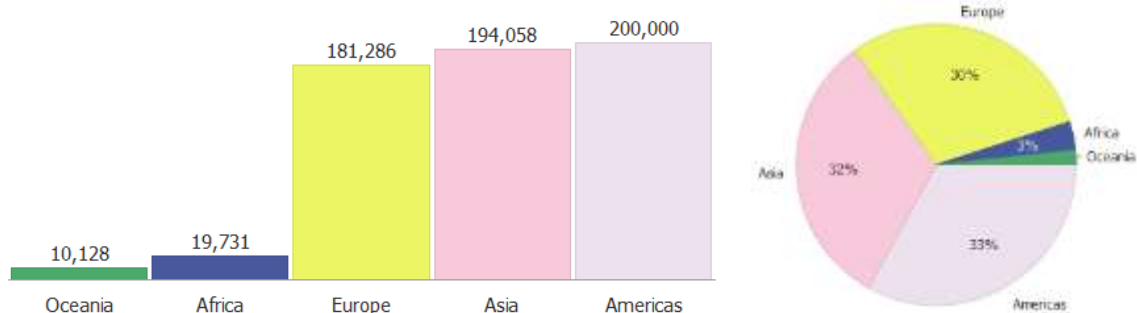
1.1.8 Key Learnings

Europe as a geographical entity is positioned in third place in terms of global Cybersecurity market sales following the US and Asia. In the top 20 leading Cybersecurity countries from a sales perspective and also from a growth perspective, there are 6 top European countries (Germany, UK, France, Spain, Italy and the Netherlands). The top 10 countries represent 69% of the total global Cybersecurity market in sales terms. Of the top 500 high growth companies in Cybersecurity in the world, only 14% originate from the EU.

1.1.9 Analysis

Cybersecurity sales in 2016 were evenly split between the Americas (33%), Asia (32%) and Europe (30%) as shown in Figure 8 : Cybersecurity Sales by Global Region 2016 (m EUR) and %. This split has not changed since 2014. The global split for companies and employment is broadly similar to sales.

Figure 8 : Cybersecurity Sales by Global Region 2016 (m EUR) and %



The breakdown of global sales is shown in more detail in Table 4, where the Top 20 countries are ranked for 2014, 2015 and 2016 showing columns for sale value in (m EUR), country ranking and country sales as a % of the global total.

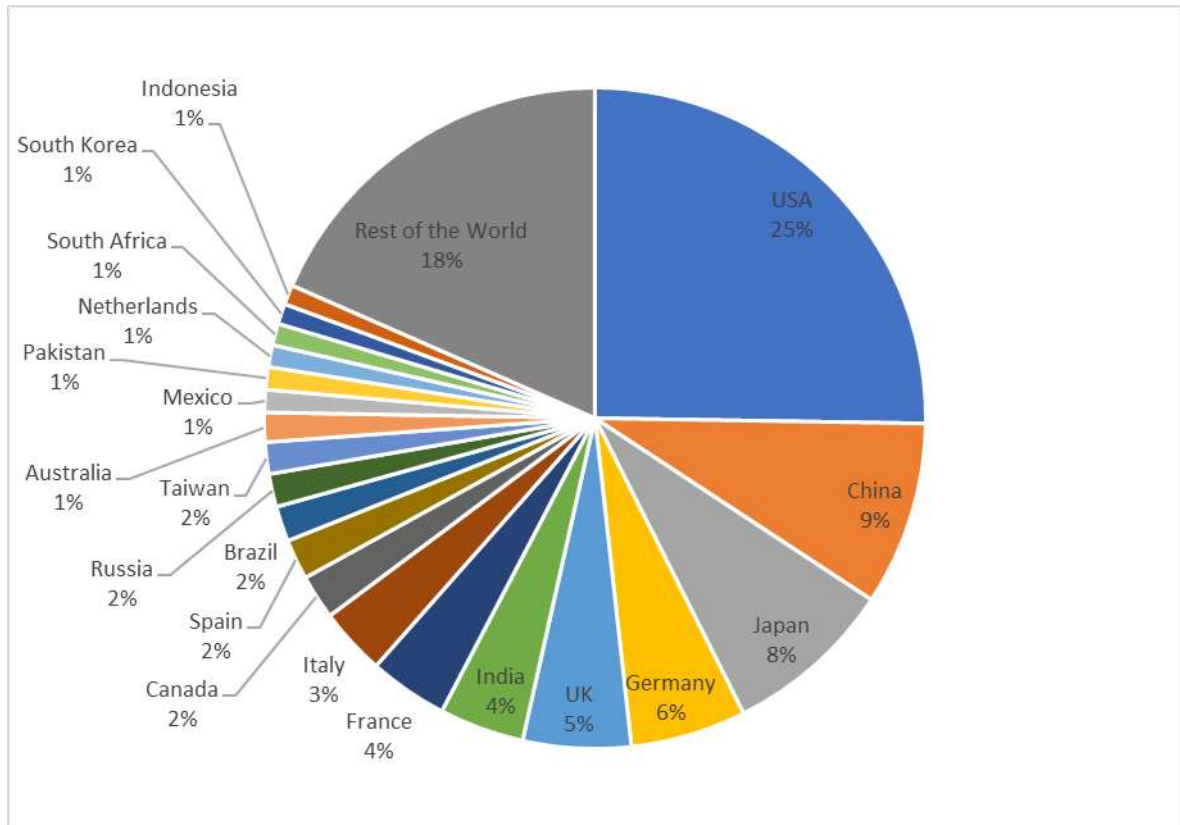
Table 4 shows that the USA accounted for 25% of global sales in all three years, followed by China (9%) and Japan (8%). The USA market share for Cybersecurity is higher than the average USA share of global GDP at 22%. The highest-ranking EU countries in sales terms are Germany (4th with 6%), UK (5th with 5%) and France (7th with 4%).

In general, global market share has not changed significantly in the short term from 2014 to 2016, as evidenced by the figures for the top 20 countries in Table 4. The exceptions are UK (increase from 5.1-5.3%), Taiwan (increase from 1.3-1.5%) and Pakistan (increase from 0.6-1.1%). The only country in the top 20 that has consistently lost market share is China (9.2-9.0%).

Table 4 : Cybersecurity Country Ranking and Market Share by Sales (m EUR) 2014-2016

Country	Ranking	2014	Market Share %	2015	Market Share %	2016	Market Share %
USA	1	106.082.6	25.3	129.394.2	25.2	152.841.0	25.3
China	2	38.621.3	9.2	46.770.4	9.1	54.464.2	9.0
Japan	3	35.278.5	8.4	43.014.3	8.4	50.386.0	8.3
Germany	4	23.431.9	5.6	28.965.4	5.6	34.260.9	5.7
UK	5	21.597.6	5.1	26.698.1	5.2	31.949.7	5.3
India	6	17.849.5	4.2	21.513.6	4.2	25.070.2	4.1
France	7	16.449.4	3.9	19.888.7	3.9	23.302.2	3.9
Italy	8	14.127.6	3.4	17.291.4	3.4	19.909.7	3.3
Canada	9	9.295.1	2.2	11.248.1	2.2	13.189.8	2.2
Spain	10	8.557.7	2.0	10.251.9	2.0	11.943.0	2.0
Brazil	11	7.527.9	1.8	9.055.3	1.8	10.436.2	1.7
Russia	12	7.092.9	1.7	8.474.9	1.7	9.783.3	1.6
Taiwan	13	5.606.2	1.3	7.301.7	1.4	9.360.3	1.5
Australia	14	6.105.3	1.5	7.423.5	1.4	8.698.0	1.4
Mexico	15	4.899.5	1.2	5.832.8	1.1	6.722.0	1.1
Pakistan	16	2.512.6	0.6	4.191.3	0.8	6.673.3	1.1
Netherlands	17	4.536.2	1.1	5.520.3	1.1	6.485.1	1.1
South Africa	18	4.596.6	1.1	5.561.3	1.1	6.415.2	1.1
South Korea	19	4.451.4	1.1	5.282.5	1.0	6.026.4	1.0
Indonesia	20	4.226.6	1.0	5.056.7	1.0	5.816.6	1.0

Figure 9 : Cybersecurity Sales market share on a global basis, top 20 countries



Overall, the top 10 countries accounted for 69% of Cybersecurity sales in all three years and the top 20 countries accounted for 82%. Six European countries (Germany, UK, France, Italy, Spain and the Netherlands) are in the top 20 countries in terms of Cybersecurity sales in 2016. Considering the EU as a Digital Single Market, it would be the single largest Cybersecurity trader on a global basis when compared to countries as opposed to regions.

Table 5 provides a similar year-on-year analysis, but this time by country annual growth rather than by market share for the top 20 countries. Table 5 records the sales value for 2014, 2015 and 2016 and historical growth is expressed in percentage terms between 2014-2015 and 2015-2016.

Table 5 : Cybersecurity Country Sales Growth (m EUR) 2014-2016

Country	Ranking	2014	Growth %	2015	Growth %	2016
Pakistan	16	2.512.6	66.8	4.191.3	59.2	6.673.3
Taiwan	13	5.606.2	30.2	7.301.7	28.2	9.360.3
UK	5	21.597.6	23.6	26.698.1	19.7	31.949.7
Germany	4	23.431.9	23.6	28.965.4	18.3	34.260.9
USA	1	106.082.6	22.0	129.394.2	18.1	152.841.0
Netherlands	17	4.536.2	21.7	5.520.3	17.5	6.485.1
Canada	9	9.295.1	21.0	11.248.1	17.3	13.189.8
Australia	14	6.105.3	21.6	7.423.5	17.2	8.698.0
France	7	16.449.4	20.9	19.888.7	17.2	23.302.2
Japan	3	35.278.5	21.9	43.014.3	17.1	50.386.0
India	6	17.849.5	20.5	21.513.6	16.5	25.070.2
Spain	10	8.557.7	19.8	10.251.9	16.5	11.943.0
China	2	38.621.3	21.1	46.770.4	16.5	54.464.2
Russia	12	7.092.9	19.5	8.474.9	15.4	9.783.3
South Africa	18	4.596.6	21.0	5.561.3	15.4	6.415.2
Brazil	11	7.527.9	20.3	9.055.3	15.2	10.436.2
Mexico	15	4.899.5	19.0	5.832.8	15.2	6.722.0
Italy	8	14.127.6	22.4	17.291.4	15.1	19.909.7
Indonesia	20	4.226.6	19.6	5.056.7	15.0	5.816.6
South Korea	19	4.451.4	18.7	5.282.5	14.1	6.026.4

Table 5 also demonstrates consistent growth across the three year period for all top 20 countries in sales terms, with lower growth between 2015-2016. The exceptions (noted above with increased market share) are Pakistan with annual growth of 60% and Taiwan with annual growth of 28%. Outside of the top 20, the highest growth countries for Cybersecurity sales were Vietnam (72%), Venezuela (68%), UAE (57%) and Chile (31%) (see Table 6) but these represent high growth from a comparatively low sales baseline.

Table 6 : Cybersecurity Global – Top Growth Countries (Sales Growth) (m EUR) 2014-2016

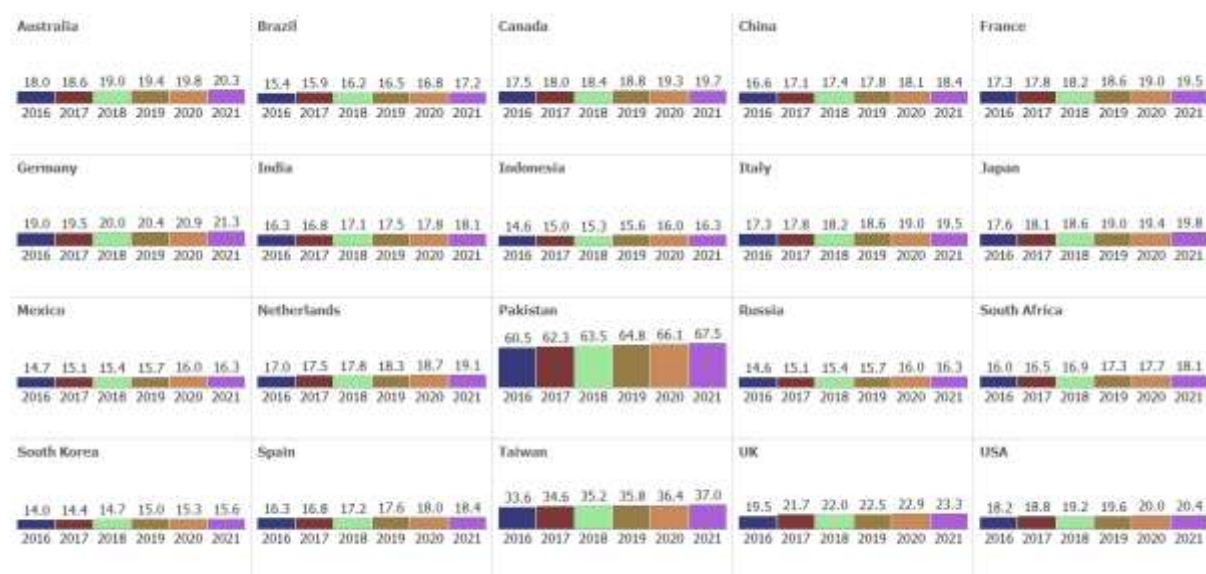
Country	Ranking	2014	Growth %	2015	Growth %	2016
Vietnam	23	1.359.8	63.6	2.224.9	72.1	3.829.1
Venezuela	33	890.8	60.0	1.425.2	68.0	2.395.0
Pakistan	16	2.512.6	66.8	4.191.3	59.2	6.673.3
United Arab Em	45	713.1	49.7	1.067.6	56.8	1.674.2
Chile	43	955.9	37.0	1.309.8	30.6	1.710.9
Taiwan	13	5.606.2	30.2	7.301.7	28.2	9.360.3
UK	5	21.597.6	23.6	26.698.1	19.7	31.949.7
Germany	4	23.431.9	23.6	28.965.4	18.3	34.260.9
Bahrain	107	129.0	21.0	156.1	18.3	184.6
USA	1	106.082.6	22.0	129.394.2	18.1	152.841.0
Malta	131	67.8	22.1	82.7	18.0	97.6
Qatar	94	213.8	21.1	258.9	17.9	305.1
Austria	30	2.276.4	21.6	2.768.0	17.8	3.261.4
Bahamas	137	54.6	21.1	66.2	17.6	77.9
Iceland	116	95.0	22.2	116.1	17.6	136.5
Netherlands	17	4.536.2	21.7	5.520.3	17.5	6.485.1
Luxembourg	88	244.1	21.9	297.6	17.4	349.4
Belgium	21	3.159.6	22.5	3.869.8	17.4	4.541.9
Canada	9	9.295.1	21.0	11.248.1	17.3	13.189.8
Turkey	24	2.613.9	21.9	3.186.7	17.3	3.736.4

Table 6 presents the top growth countries on a global basis, which differs from Table 5, in that other growth markets become apparent, indicating further export potential and dynamics – even for some of the smaller EU countries such as Austria, Belgium, Luxembourg, Iceland and Malta.

Historical growth rates varied across the top 20 countries and the same is true for forecast sales growth rates. Figure 10 presents growth rates for the period 2016-2020 for each country.

The highest forecast growth rates are for Pakistan and Taiwan (reflecting historical growth performance) and then for Germany, UK and the USA. Previous reservations about global forecast growth rates also apply to the country growth rates i.e. that future country growth is probably understated by 4-5% at least for the next 1-2 years.

Figure 10 : Cybersecurity Forecast Sales Growth % by Top 20 Country



To underpin this growth analysis, further research was conducted into global high growth companies and their country of origin. This research identified the top 500 global companies based upon highest level of growth in sales between 2015 and 2016. This list provides data that is limited to company name, broad area of Cybersecurity expertise and country of origin. The list is provided at

Appendix K : Top 500 Global Cybersecurity Companies, with EU- based companies shown in Red.

The majority of companies in this list originate from the USA, reflecting its dominant market position and access to growth capital. The EU accounts for 69 out of the 500 companies- 14% of the total.

1.1.10 Conclusions and Recommendations

Looking at global sales figures the USA is the dominant country in terms of sales (25.3% of global sales) followed by China (9%), Japan (8.3%) and Germany (5.7%). Forecast growth rates for the top 20 countries in sales terms out to 2020 are all above 10% per annum, varying between 10-11% for South

Korea through to 19.6-21.2% for Taiwan and 35-38.5% for Pakistan. The USA and Germany are forecast to grow faster (13.2-14.5%) than all of the other Top 20 countries apart from Taiwan and Pakistan.

The EU as a single market would be the largest global Cybersecurity market, in sales terms, when compared to countries rather than regions, higher than the US market. A European Digital Single Market for Cybersecurity could, therefore, be considered as a powerful trade entity. Considering the differences in growth rates, there are multiple growth opportunities within the EU (Germany, UK, Austria, Belgium, ...) and other parts of Europe. **There are also opportunities for European companies to seek out global market opportunities from a historical and future forecast growth perspective (such as Pakistan and Taiwan).**

If the European Digital Single Market for Cybersecurity is consolidated, and reinforced by additional measures in the EU to strengthen European Cybersecurity companies in Europe, it would be conceivable that this spills over on a global level and that the representation of European companies on a global level will increase.

EU Cybersecurity Market

Introduction

Chapter 0 focuses upon the EU and the 28 Member States within it. The same key measures from the global research (Sales, Number of Companies, Employment) are included in the analysis, with the addition of further measures relating to imports, exports, share of GDP, Cybersecurity providers, size of companies and end- users for Cybersecurity products and services. In the second draft further sections will be added on competitiveness and market opportunity. The value for the Cybersecurity sector in this report is higher than in most (not all) other research reports because the search for evidence covers a very broad base which allows the accommodation of national variations in definition without losing the ability to compare results across multiple continents or countries.

This part of the study focuses on the EU 28 Member States and therefore does not take into account other European countries, such as Switzerland and Norway. However, as a result of discussions during the workshops, they have been added for further information and analysis.

EU Cybersecurity Key Metrics

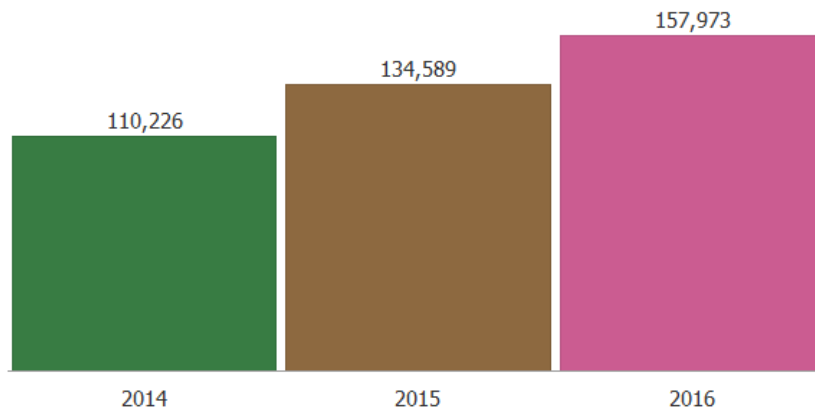
1.1.11 Key Learnings

The EU Cybersecurity market continues to grow in line with global markets and will have grown beyond EUR 160 billion in 2017, with over 60,000 companies providing products and services. The EU Cybersecurity market provides employment to nearly 1 million people. As a single market, the EU (28 Member States) would be the largest Cybersecurity market on the globe. The EU continues to be an interesting market opportunity, with an individual growth rate as a consolidated single market of 20% by 2021. This is mainly represented by some significant large markets such as Germany and UK. These anticipated growth rates are mainly based upon historical growth and do reflect potential effects of additional regulations such as GDPR, NIS, PSD2 or other regulatory frameworks.

1.1.12 Analysis

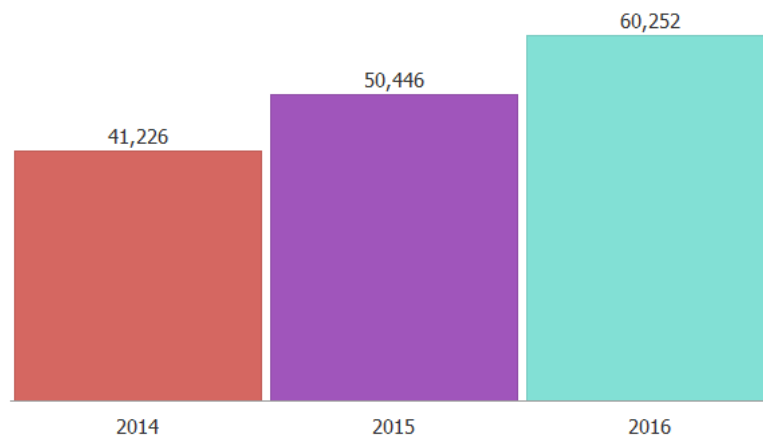
The total for EU Cybersecurity sales in 2016 was EUR 157,973 million (see Figure 11). This was an increase of **17%** on 2015 sales of EUR 134,589 million. This compares with an increase of **22%** between 2014- 2015. The EU accounted for 26% of the global market in 2016, just ahead of the 25% for the USA. With the UK included in the EU, Europe as a whole is the single largest Cybersecurity market in the world.

Figure 11 : EU Cybersecurity Sales 2014 to 2016 (m EUR)



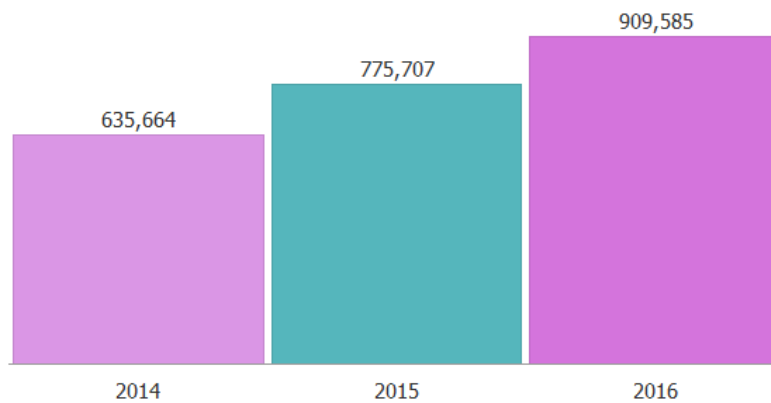
The total number of Cybersecurity companies in 2016 was 60,250 (see Figure 12). This was an increase of **19%** on the 2015 company count of 50,446. This compares with an increase of **22%** between 2014-2015. The EU accounted for 27% of the global total number of companies for 2016.

Figure 12 : Number of Cybersecurity Companies in EU (28) 2014 to 2016



The total for Cybersecurity employment in 2016 was 909,600 (see Figure 13). This was an increase of **17%** on the 2015 employment count of 775,700. This compares with an increase of **22%** between 2014-2015. The EU accounted for 25% of the global employment for 2016.

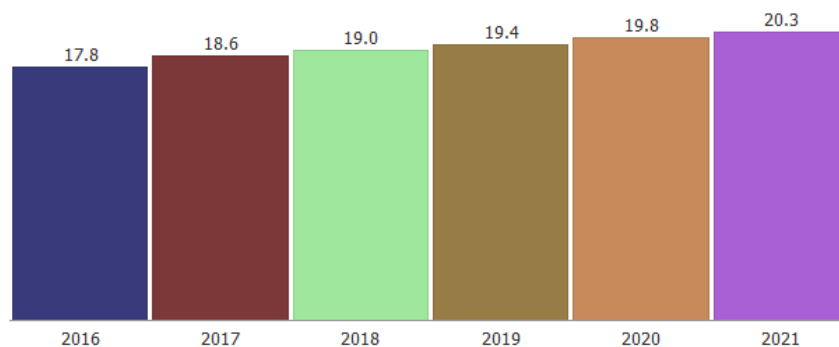
Figure 13 : EU Cybersecurity Employment (nr of people) 2014 to 2016



1.1.13 EU Cybersecurity Forecasts

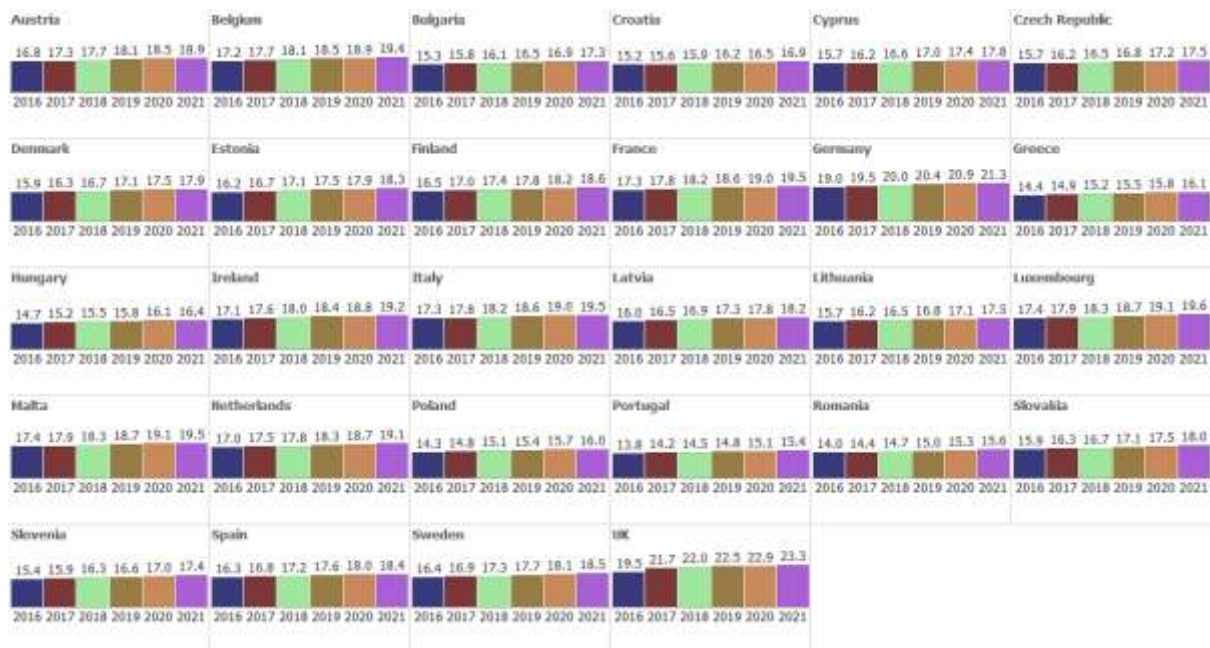
Forecast sales growth for the EU between 2016- 2021 is shown in Figure 14. This forecast growth of 17.8%- 20.3% is above the forecast global average of 16-18% (Figure 4) and, unlike the global forecast for growth, is broadly in line with historical EU growth in Cybersecurity.

Figure 14 : EU Cybersecurity Forecast Growth 2016 to 2021



What is perhaps of more interest is the forecast growth rates by EU country (Figure 15). As with the analysis of the global top 20 countries, the growth rates for Germany and the UK stand out and are mostly responsible for the EU growing at a faster rate than the global average. In all cases the forecast growth rates seem very promising. The expected growth rates for Ireland and Luxembourg are , both of which are also above the average for the EU. These forecast numbers are not directly taking into consideration expected impact in 2017–2020 from regulations such as GDPR, NIS, PSD2 and other sectorial and Member State Cybersecurity regulations and policies.

Figure 15 : EU Cybersecurity Forecast Growth 2016 to 2021 by Country



1.1.14 Conclusions and Recommendations

In Sales terms the EU (including the UK) represented 26% of the global market in 2016, above the USA at 25%, making the EU the single largest Cybersecurity market in the world when integrated effectively into a single market.

The EU Cybersecurity market has grown rapidly over the last 3 years (above 17%) with the number of EU companies and EU employment growing at the same rate, and is forecasted to continue growing rapidly at a similar rate out to 2021. The forecast growth rates out to 2021 are significantly higher (above 19%) for Germany and the UK than other Member States. Since these Member States (Germany, UK, France, Italy, Spain, The Netherlands and Belgium) are contributing most to the EU Cybersecurity market, the gap between these countries and the other European countries will continue to exist and grow further.

During the workshops it was confirmed that in terms of the number of companies and local expertise, innovation and market acceptance, many Eastern European countries are lagging behind in terms of Cybersecurity maturity. While in Western European markets, many companies and governments have developed Cybersecurity policies and deployed Cybersecurity products and services, supporting the development of the local markets, this activity is still ongoing in many other parts of Europe. These Member States can likely learn from best practices from the leading European Member States, and should be stimulated to work more closely with market leaders and innovators from the more mature Member States, while adopting actions at Member State level.

EU Cybersecurity by Sub-sector

1.1.15 Key Learnings

Infrastructure is the largest Cybersecurity sub-sector for the European market, followed by Situational Awareness and Applications Security. However, there are major differences between the various Member States as shown in the Member States reports in Chapter 0. Similar to the rest of the world,

Training and Education are only a minor portion of the total spent into Cybersecurity, just over EUR 111 million in 2016, on the total of nearly EUR 160 billion. The subcategories Identity and Access, Encryption and Outsourced / Managed Services have been the fastest growing domains for the last two consecutive years.

1.1.16 Analysis

Following the earlier analysis of the global Cybersecurity market, the EU Cybersecurity market has been divided into 13 sub-sectors.

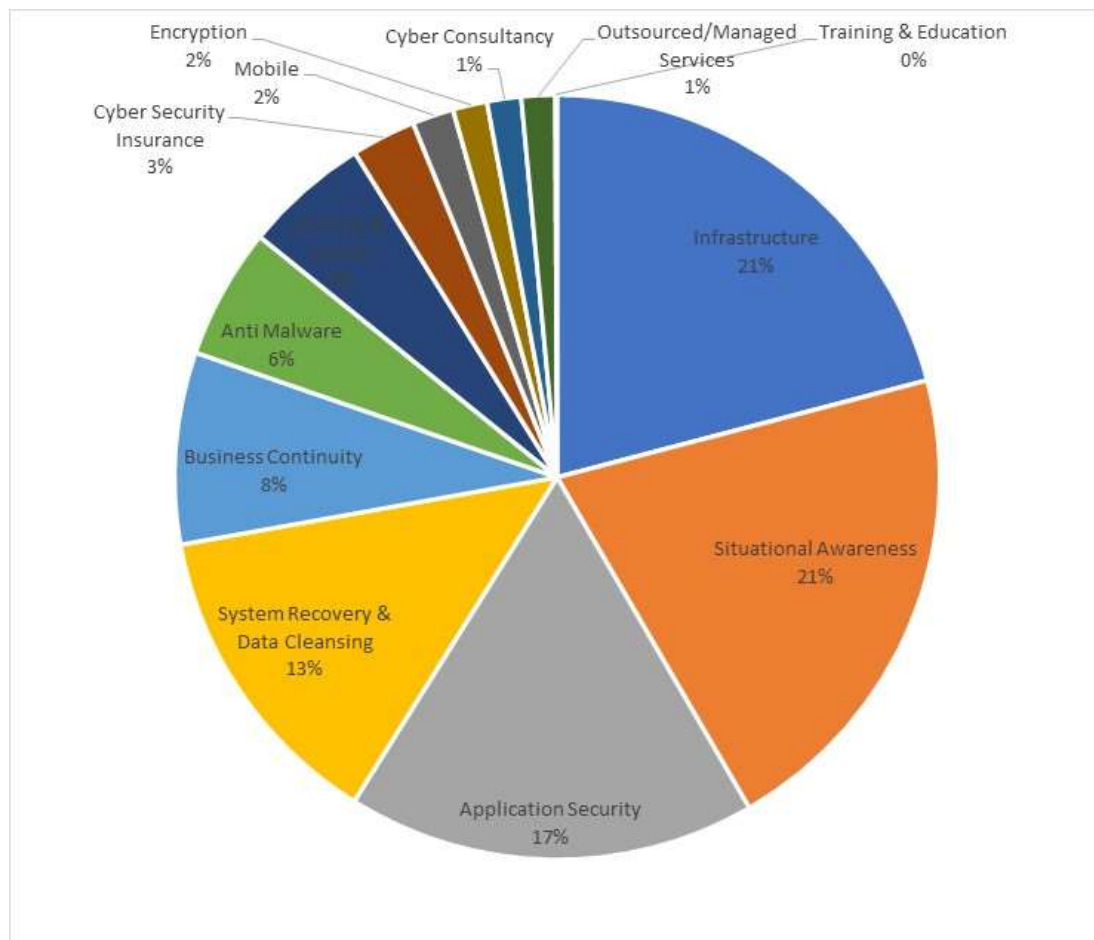
Table 7 compares EU sub-sector sales for the period 2014 to 2016. Growth rates between 2014 and 2015 are uniformly higher than for 2015 to 2016. The highest growth sub-sectors across both periods for the EU are: Outsourced/ Managed Services, Encryption, Identity & Access, Cyber Consultancy and Infrastructure, which is overall in line with the global perspective, but obviously driven mainly by the top 10 European Member States (Germany, UK, France, Italy, Spain, Netherlands, Belgium, Sweden) in terms of Sales.

Table 7 : EU Cybersecurity Sales (m EUR) 2014 to 2016, by sub-sector

Level 2	2014	Growth %	2015	Growth %	2016
Infrastructure	22.477	24	27.859	19	33.040
Situational Awareness	23.509	19	28.071	17	32.717
Application Security	18.916	23	23.241	17	27.296
System Recovery & Data Cleansing	14.578	22	17.824	18	20.971
Business Continuity	9.316	20	11.202	14	12.813
Anti Malware	6.272	22	7.632	15	8.756
Identity & Access	5.277	29	6.809	23	8.376
Cyber Security Insurance	3.364	15	3.873	11	4.301
Mobile	2.131	15	2.460	12	2.763
Encryption	1.396	31	1.826	26	2.296
Cyber Consultancy	1.553	23	1.914	19	2.272
Outsourced/Managed Services	1.369	32	1.804	25	2.261
Training & Education	96	10	106	4	111
Total	110.226	22	134.589	17	157.973

Table 7 shows the revision of the categories at Level 2 after reassigning hierarchy membership for members of the taxonomy at Level 3 and below (the sub-categories). This was initiated as a result of the qualitative workshops held with Cybersecurity Industry representatives and further analysis.

Figure 16 : EU Cybersecurity Sub-level 2 Category Spread for 2016 in %



The historical growth rates in sales between 2014-2015 range between 32% (Outsourced/ Managed Services) and 10% (Training & Education). The range between 2015- 2016 is between 26% (Encryption) and 4% (Training & Education). When compared with the historical global growth (Table 1) the growth rates between 2014-2015 are broadly consistent.

Table 8 compares EU sub-sector number of Cybersecurity products and services trading companies for the period 2014 to 2016. Growth rates between 2014 and 2015 are uniformly higher than for 2015 to 2016. The highest growth sub-sectors between 2014 and 2015 for the EU (and also at the global level) are: Outsourced/ Managed Services, Encryption, Identity & Access, Cyber Consultancy, Business Continuity and Infrastructure. The qualitative assessment of this increase was part of the debates during the qualitative workshops, and resulted in further analysis of the data in subcategories 3 to 5 and resulted in a re-categorisation of subcategory 2. These results have been integrated, and clearly showed the lack of spending on training and education performed in the sector.

Table 8 : EU Cybersecurity Number of Companies 2014 to 2016

Level 2	2014	Growth %	2015	Growth %	2016
Anti Malware	2,162	20.0	2,594	29.7	3,365
Application Security	5,919	22.8	7,267	19.1	8,655
Business Continuity	3,142	19.6	3,759	25.5	4,719
Cyber Consultancy Services	642	29.3	830	41.0	1,169
Cyber Insurance	3,845	12.1	4,310	-18.7	3,505
Encryption	2,856	34.4	3,838	41.5	5,429
Identity & Access Based Services	7,506	24.1	9,314	19.7	11,153
Infrastructure	860	31.8	1,133	28.9	1,461
Mobile	726	19.2	865	63.9	1,417
Outsourced/Managed Services	926	34.9	1,249	30.0	1,624
Situational Awareness	7,585	20.0	9,103	15.8	10,546
System Recovery & Data Cleansing	5,059	22.2	6,183	16.6	7,208

(the result after the re-organisation of the sub-level categories)

Level 2	2014	Growth %	2015	Growth %	2016
Anti Malware	2,042	21	2,461	15	2,834
Application Security	5,911	23	7,259	14	8,261
Business Continuity	3,137	20	3,754	21	4,543
Cyber Consultancy	684	28	876	20	1,051
Cyber Security Insurance	1,745	15	2,010	10	2,205
Encryption	749	33	996	26	1,256
Identity & Access	2,511	33	3,330	31	4,358
Infrastructure	8,281	25	10,368	18	12,227
Mobile	722	19	861	15	992
Outsourced/Managed Services	697	33	930	18	1,100
Situational Awareness	7,585	20	9,103	16	10,546
System Recovery & Data Cleansing	5,059	22	6,183	17	7,208
Training & Education	40	8	43	5	45
Total	41,226	22	50,446	19	60,252

The historical growth rates in the number of companies between 2014-2015 range between 33% (Encryption, Identity & Access and Outsourced/ Managed Services) and 8% (Training & Education). The range between 2015- 2016 is between 31% (Identity & Access) and 5% (Training & Education). When compared with the historical global growth (Table 2) the growth rates between 2014-2015 are broadly consistent.

Table 9 compares EU sub-sector employment for the period 2014 to 2016. Growth rates between 2014 and 2015 are, once again, uniformly higher than for 2015 to 2016. The highest growth sub-sectors across both periods for the EU (and also at the global level) are: Outsourced/ Managed Services, Encryption and Infrastructure- followed closely by Cyber Consultancy.

Table 9 : EU Cybersecurity Employment 2014 to 2016

Level 2	2014	Growth %	2015	Growth %	2016
Anti Malware	41,748	19.7	49,976	13.4	56,688
Application Security	108,772	21.6	132,292	18.2	156,332
Business Continuity	51,146	20.0	61,370	16.1	71,223
Cyber Consultancy Services	7,983	29.9	10,368	21.5	12,599
Cyber Insurance	23,500	14.6	26,920	13.0	30,422
Encryption	39,027	32.7	51,801	23.1	63,778
Identity & Access Based Services	122,799	22.6	150,610	17.9	177,531
Infrastructure	11,215	30.3	14,610	22.3	17,873
Mobile	17,357	14.5	19,875	12.0	22,263
Outsourced/Managed Services	11,950	34.2	16,037	23.9	19,864
Situational Awareness	124,617	20.1	149,648	15.5	172,803
System Recovery & Data Cleansing	75,551	22.0	92,199	17.4	108,210

(the result after the re-organisation of the sub-level categories :)

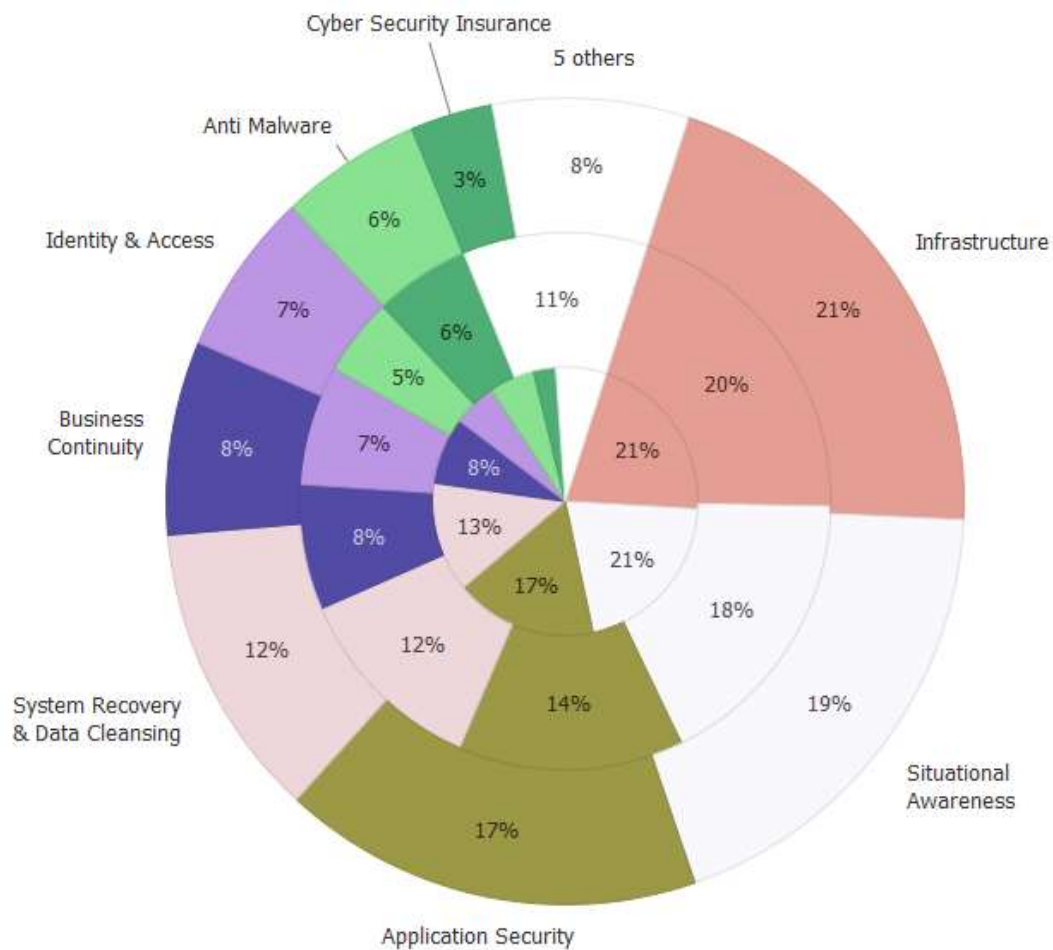
Level 2	2014	Growth %	2015	Growth %	2016
Anti Malware	38,082	21	45,978	13	52,034
Application Security	107,982	22	131,422	18	154,961
Business Continuity	50,818	20	61,014	16	70,642
Cyber Consultancy	10,937	24	13,609	23	16,699
Cyber Security Insurance	23,500	15	26,920	13	30,422
Encryption	10,285	31	13,511	24	16,719
Identity & Access	38,806	28	49,855	20	59,789
Infrastructure	128,312	24	159,099	19	188,570
Mobile	16,614	15	19,066	10	21,051
Outsourced/Managed Services	9,752	33	12,942	28	16,530
Situational Awareness	124,617	20	149,648	15	172,803
System Recovery & Data Cleansing	75,551	22	92,199	17	108,210
Training & Education	408	9	446	12	500
Total	635,664	22	775,707	17	909,585

The historical growth rates in employment between 2014-2015 range between 34% and 15% (Cyber Insurance and Mobile). The range between 2015-2016 is between 24% and 12% (Mobile).

When compared with the historical global growth (Table 3) the growth rates between 2014- 2015 are broadly consistent, but between 2015-2016 EU growth in Anti Malware, Cyber Consultancy, Encryption, Infrastructure and Outsourced/ Managed Services are all lower than the global average.

The differences across the three key measures are illustrated in Figure 17, where the three measures are shown as concentric circles on a pie chart, split by sub-sector for 2016. The **inner circle** is **sales**, the **middle circle** is **companies** and the **outer circle** is **employment**. For ease of presentation, the smallest four sub-sectors have been grouped as "Other". Figure 17 demonstrates that the largest sub-sector by sales is Situational Awareness, but the largest sub-sector by employment is Identity & Access Based Services. Generally, the largest five sub-sectors account for approximately 80% of total sales, companies and employment. The largest variations across measures occur in the smaller Cybersecurity activities like Encryption and Cyber Insurance.

Figure 17 : EU Cybersecurity Key Measures by Sub-sector 2016



The final analysis of Cybersecurity sub-sectors is to compare the mix of sub-sector activities by EU country. For this a 100% stacked bar chart is used at Figure 18 to visualise the key differences by country. The data relates to 2016 sales and the percentage for each sub-sector is shown within each stacked bar. Visually, the graphic is not perfect as all the data is not completely visible, but the chart clearly illustrates that the Cybersecurity business mix differs by country.

For example, Figure 18 shows Situational Awareness as 21% of sales across the EU, but at the country level the range is 16% (Netherlands and Latvia) to 27-28% (Croatia, Poland and Portugal). Similarly:

- Identity & Access Based Control is 20% of EU sales, with a range of 11% (various countries) to 26-27% (Belgium and Denmark)
- Application Security is 17% of EU sales, with a range of 8% (Croatia, Czech Republic and Hungary) to 23-24% (Sweden and Ireland)
- System Recovery & Data Cleansing is 13% of sales, with a range of 10% (Germany) to 25% (Hungary).

Similar patterns are evident from analysis of data for 2014 and 2015 and for other measures-companies and employment- suggesting that each country is developing different specialisms in Cybersecurity or responding to different challenges. A possible explanation for this, is the level of maturity of Cybersecurity in the specific Member states.

Figure 18 : EU Cybersecurity sales per country, per sub category in % as proportion of total Sales per country



1.1.17 Conclusions and Recommendations

The EU Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, varying from 4% for Training and Education to 26% for Encryption in 2015/16, with the number of EU companies and EU employment growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum out to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%. Infrastructure (19%), Situational Awareness (17%) and Application Security (17%) are the largest EU sub-sectors in sales terms.

While it is likely that additional Training and Education will be included in many cases with products and services, it is clear that there is a significant underspend in comparison. **The apparently low EU investment in Cybersecurity Training and Education, and slow growth in the Training and Education market compared to other sub-sectors, highlights the need for EU investment including structural measures to improve overall EU skills and capabilities.**

It appears that more Cybersecurity mature Member States (in terms of the Cybersecurity market size, number of companies and employment, and on a per capita basis as per description in the next paragraphs), tend to have a slightly different spending pattern which is indicating that less is being spent in preventive measures (Situational Awareness, Identity and Access, Encryption) rather than in mitigation and remediation measures (System Recovery / Data Cleansing).

EU Cybersecurity by Country

In the previous section, the differences in the mix of Cybersecurity activities were briefly explored from Sales, Number of Companies, Employees and Domain perspectives at global and EU-level. In this section, at EU-level a first further breakdown towards Member States will be reported. Following this section, additional Member States details will be reported and documented. On the Country level, further detail can be found on Switzerland, Norway and Israel, within Europe.

1.1.18 Key Learnings

Germany and UK are by far the largest Cybersecurity markets in Europe. Together with the other 5 leading countries, they contribute to nearly 80% of the total European Cybersecurity market. While Germany is the single largest European Cybersecurity market (EUR 34,261 billion), there are significantly more companies in the UK (18,025 companies) than in Germany (12,755 companies), whereas total employment in Germany (215,523) is significantly larger than in the UK (150,255 employees). When comparing Cybersecurity spending as a percentage of GDP, countries like Estonia, Bulgaria, Latvia, Slovakia and Italy (between 1.6 and 1.2% of GDP) are significantly bigger spenders in Cybersecurity, closely followed by Germany, UK, Belgium and Sweden (1.1% of GDP).

1.1.19 Analysis

Table 10 compares Cybersecurity sales by EU country for 2014 to 2016, ranked by size. The table demonstrates:

- Sales in 2016 varies between EUR 93 million (Malta) and EUR 34,261 million (Germany)
- Sales by EU country show consistently strong growth for the past two years
- Growth 2015- 2016 ranges between 14% (Bulgaria) -20% (UK)
- Growth 2014- 2015 ranges between 19% (Croatia and Hungary) -24% (Germany and UK).

Table 10 : EU Cybersecurity Sales (m EUR) 2014 to 2016 by Country

Country	2014	Growth %	2015	Growth %	2016
Germany	23,432	23.6	28,965	18.3	34,261
UK	21,598	23.6	26,698	19.7	31,950
France	16,449	20.9	19,889	17.2	23,302
Italy	14,128	22.4	17,291	15.1	19,910
Spain	8,558	19.8	10,252	16.5	11,943
Netherlands	4,536	21.7	5,520	17.5	6,485
Belgium	3,160	22.5	3,870	17.4	4,542
Sweden	2,310	21.8	2,813	16.7	3,283
Austria	2,276	21.6	2,768	17.8	3,261
Poland	2,227	19.4	2,658	14.4	3,040
Denmark	1,501	20.0	1,801	15.3	2,076
Finland	1,323	21.3	1,605	16.1	1,864
Ireland	1,201	21.9	1,463	15.9	1,696
Greece	1,135	18.6	1,346	14.9	1,546
Czech Republic	854	21.0	1,034	15.9	1,198
Portugal	879	17.6	1,034	14.2	1,180
Romania	844	18.7	1,002	13.7	1,140
Slovakia	793	20.0	952	16.4	1,109
Hungary	745	19.1	887	15.2	1,022
Bulgaria	549	20.7	663	13.6	753
Slovenia	345	19.3	412	15.6	476
Latvia	275	20.7	332	15.7	384
Luxembourg	244	21.9	298	17.4	349
Croatia	244	19.1	291	15.7	337
Lithuania	227	19.6	272	16.2	316
Estonia	187	20.6	226	16.3	263
Cyprus	137	19.3	163	15.5	188
Malta	68	22.1	83	18.0	98

Table 11 compares the number of Cybersecurity companies per EU country for 2014 to 2016, ranked by size. The table demonstrates:

- Number of Cybersecurity companies in 2016 varies between 7 (Malta) and 18,000 (UK)
- Company count by EU country show consistently strong growth for the past two years
- Growth 2015-2016 ranges between 14% (Latvia) -23% (UK), with high growth for Luxembourg and Malta from a low company base
- Growth 2014-2015 ranges between 17% (various countries) -25% (Germany).

Table 11 : EU Cybersecurity Number of Companies 2014 to 2016 by Country

Country	2014	Growth %	2015	Growth %	2016
UK	12,031	21.6	14,625	23.3	18,025
Germany	8,494	25.1	10,626	20.0	12,755
France	5,903	22.5	7,230	17.2	8,476
Italy	4,842	22.2	5,919	16.8	6,914
Spain	2,958	20.8	3,572	17.1	4,181
Netherlands	1,553	22.4	1,902	17.7	2,239
Belgium	1,152	22.2	1,407	17.5	1,653
Poland	684	18.6	812	13.6	922
Austria	604	22.5	740	19.0	880
Sweden	471	23.0	579	18.6	687
Denmark	473	19.8	567	17.1	664
Finland	249	23.5	308	18.5	365
Greece	261	18.5	309	14.4	354
Portugal	253	17.3	297	13.1	336
Romania	239	16.5	278	13.4	315
Hungary	205	18.9	244	14.6	280
Czech Republic	184	20.5	221	16.0	257
Ireland	168	24.8	210	19.7	251
Slovakia	166	18.6	197	16.3	229
Lithuania	78	20.7	94	15.9	109
Bulgaria	69	17.4	80	14.4	92
Slovenia	62	19.5	75	14.4	85
Croatia	47	21.4	57	15.9	65
Luxembourg	26	27.2	33	23.9	41
Latvia	22	18.2	26	12.7	30
Estonia	16	22.4	20	16.4	23
Cyprus	11	18.6	13	14.4	15
Malta	4	30.4	6	26.3	7

Table 12 compares Cybersecurity employment by EU country for 2014 to 2016, ranked by size.

Table 12 : EU Cybersecurity Employment 2014 to 2016 by Country

Country	2014	Growth %	2015	Growth %	2016
Germany	147,501	22.9	181,241	18.9	215,523
UK	101,420	24.8	126,557	18.7	150,255
France	102,603	21.7	124,821	17.0	146,086
Italy	87,631	21.6	106,542	16.9	124,546
Spain	52,700	20.4	63,457	15.6	73,371
Netherlands	27,615	21.6	33,583	15.7	38,864
Belgium	14,411	21.3	17,482	16.8	20,417
Poland	14,072	19.0	16,742	13.4	18,985
Sweden	13,138	21.1	15,915	15.2	18,340
Austria	9,260	20.9	11,192	16.4	13,033
Ireland	8,778	21.8	10,690	17.4	12,554
Denmark	8,724	19.2	10,396	14.7	11,923
Finland	6,961	21.2	8,435	16.5	9,826
Greece	6,685	19.0	7,953	13.9	9,056
Portugal	5,380	17.4	6,316	13.1	7,147
Czech Republic	4,883	20.0	5,861	15.5	6,772
Romania	4,980	17.8	5,865	13.6	6,663
Hungary	4,455	19.4	5,319	14.6	6,098
Bulgaria	3,650	19.4	4,358	16.7	5,087
Slovakia	3,155	19.0	3,753	15.6	4,337
Luxembourg	1,635	22.0	1,994	18.1	2,355
Slovenia	1,431	19.2	1,706	13.9	1,943
Latvia	1,103	20.1	1,325	15.4	1,529
Lithuania	1,029	20.6	1,241	16.1	1,442
Croatia	1,041	19.9	1,248	15.2	1,437
Estonia	731	20.3	879	16.1	1,020
Cyprus	470	19.7	563	15.2	649
Malta	221	24.1	274	19.1	327

The table demonstrates:

- Employment in 2016 varies between 330 (Malta) and 215,500 (Germany)
- Employment by EU country show consistently strong growth for the past two years
- Growth 2015- 2016 ranges between 13% (Portugal and Poland) -19% (Germany and UK)
- Growth 2014- 2015 ranges between 17% (Portugal and Romania) -25% (UK).

If one analyses the average size of EU Cybersecurity companies in EU MS the results are as follows:

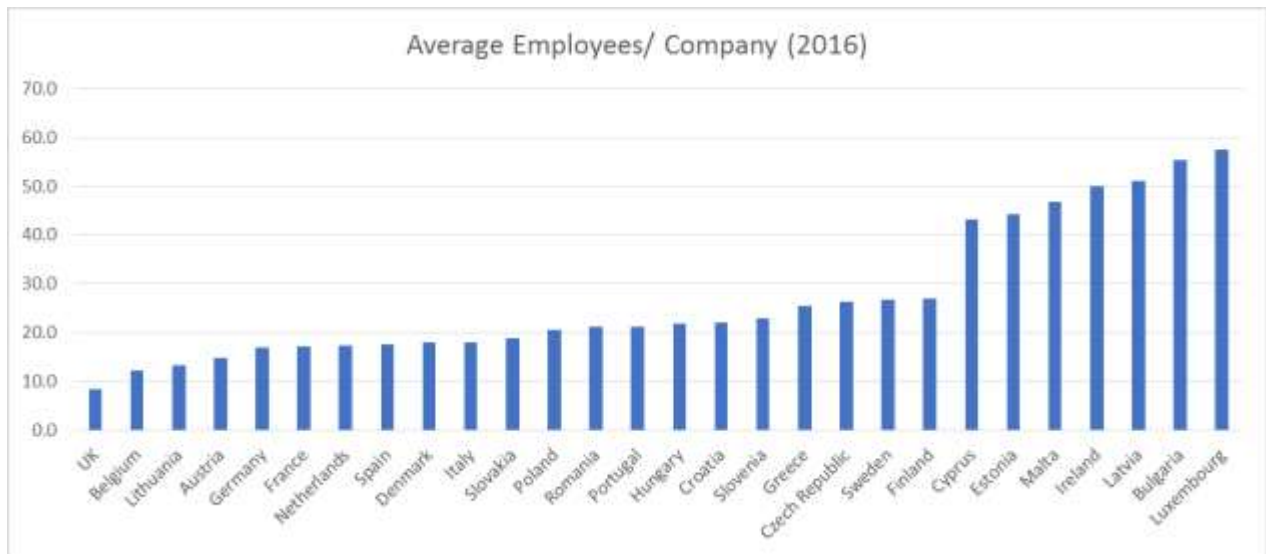
Table 13 : Average employees per company for EU Member States (ordered by size)

Member State	Average Employees/ Company (2016)	Companies 2016 (1)	Employees 2016 (2)
UK	8.3	18025	150255
Belgium	12.4	1653	20417
Lithuania	13.2	109	1442
Austria	14.8	880	13033
Germany	16.9	12755	215523
France	17.2	8476	146086
Netherlands	17.4	2239	38864
Spain	17.5	4181	73371
Denmark	18.0	664	11923
Italy	18.0	6914	124546
Slovakia	18.9	229	4337
Poland	20.6	922	18985
Romania	21.2	315	6663
Portugal	21.3	336	7147
Hungary	21.8	280	6098
Croatia	22.1	65	1437
Slovenia	22.9	85	1943
Greece	25.6	354	9056
Czech Republic	26.4	257	6772
Sweden	26.7	687	18340
Finland	26.9	365	9826
Cyprus	43.3	15	649
Estonia	44.3	23	1020
Malta	46.7	7	327
Ireland	50.0	251	12554
Latvia	51.0	30	1529
Bulgaria	55.3	92	5087
Luxembourg	57.4	41	2355
EU TOTAL	15.1	60250	909585

1) Table 10 - EU Cybersecurity Companies 2014 to 2016 by Country

2) Table 11 - EU Cybersecurity Employment 2014 to 2016 by Country

Figure 19 : Average employees per company for EU Member States (ordered by size)



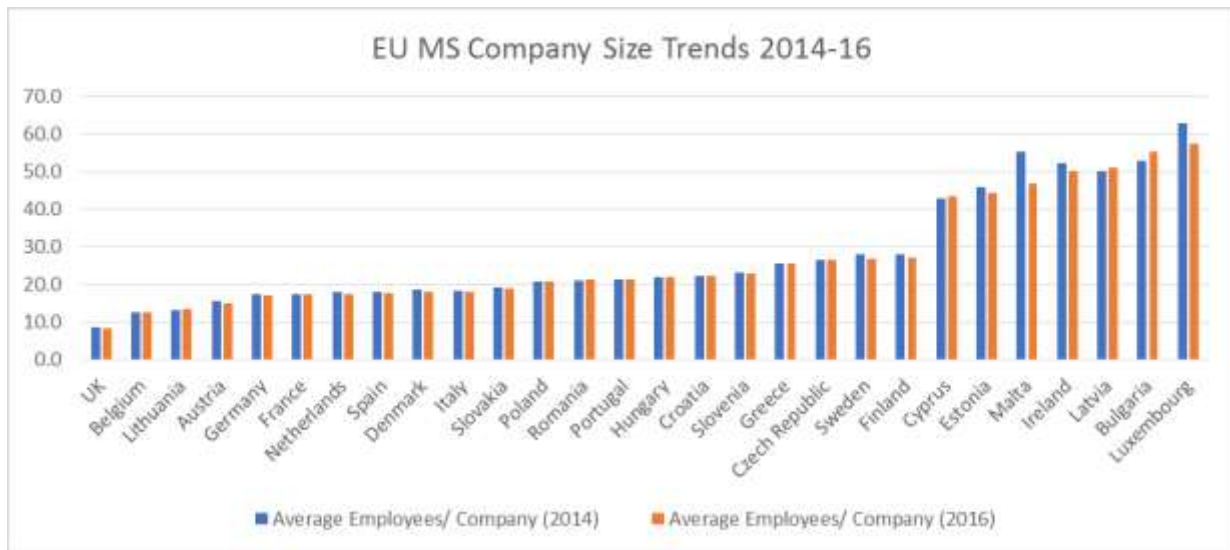
The average number of employees in EU Cybersecurity companies is 15, but this varies across the EU from 8 in the UK to over 40 in Estonia, Ireland, Latvia, Bulgaria and Luxembourg.

If one then looks at the trends in company size from 2014 to 2016, one sees that as the EU security market has developed and sales have grown the average size of Cybersecurity company across the EU has fallen, though not substantially (15.4 in 2014 to 15.1 in 2016), with small falls in most Member States. See Table 12, Table 13, Table 14, Figure 19 and Figure 20.

Table 14 : Average employees per company for EU Member States between 2014 and 2016

MS	Average Employees/ Company (2014)	Average Employees/ Company (2016)
UK	8.4	8.3
Belgium	12.5	12.4
Lithuania	13.2	13.2
Austria	15.3	14.8
Germany	17.4	16.9
France	17.4	17.2
Netherlands	17.8	17.4
Spain	17.8	17.5
Denmark	18.4	18.0
Italy	18.1	18.0
Slovakia	19.0	18.9
Poland	20.6	20.6
Romania	20.8	21.2
Portugal	21.3	21.3
Hungary	21.7	21.8
Croatia	22.1	22.1
Slovenia	23.1	22.9
Greece	25.6	25.6
Czech Republic	26.5	26.4
Sweden	27.9	26.7
Finland	28.0	26.9
Cyprus	42.7	43.3
Estonia	45.7	44.3
Malta	55.3	46.7
Ireland	52.3	50.0
Latvia	50.1	51.0
Bulgaria	52.9	55.3
Luxembourg	62.9	57.4
EU TOTAL	15.4	15.1
1) Table 10 - EU Cybersecurity Companies 2014 to 2016 by Country		
2) Table 11 - EU Cybersecurity Employment 2014 to 2016 by Country		

Figure 20 : Average employees per company for EU Member States between 2014 and 2016



If one looks at how average company size varies with the sales made by companies in Member States (shown for 2016), the largest economies tend to have lowest average company size, as they have more extensive ecosystems with a higher proportion of small companies. See Table 15 and Figure 21.

Table 15 : Average Company Size mapped against Member State Sales in 2016.

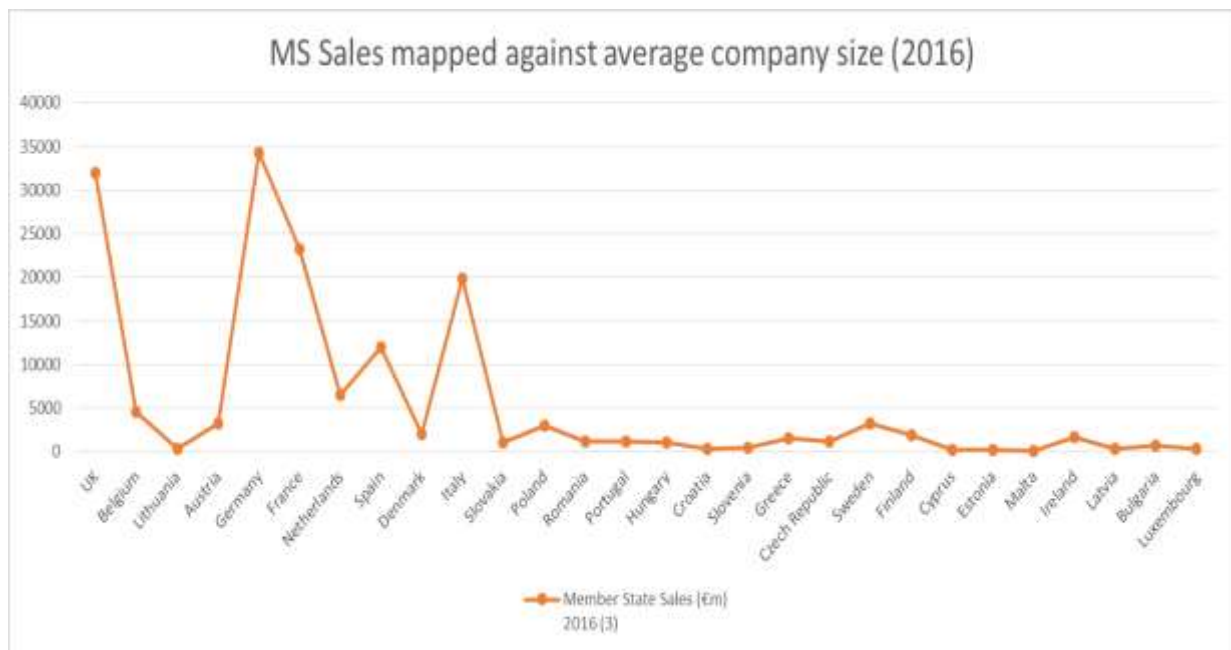
MS	Average Employees/ Company 2016 (1,2)	Member State Sales (€m) 2016 (3)
UK	8.3	31950
Belgium	12.4	4542
Lithuania	13.2	316
Austria	14.8	3261
Germany	16.9	34261
France	17.2	23302
Netherlands	17.4	6485
Spain	17.5	11943
Denmark	18.0	2076
Italy	18.0	19910
Slovakia	18.9	1109
Poland	20.6	3040
Romania	21.2	1140
Portugal	21.3	1180
Hungary	21.8	1022
Croatia	22.1	337
Slovenia	22.9	476
Greece	25.6	1546
Czech Republic	26.4	1198
Sweden	26.7	3283
Finland	26.9	1864
Cyprus	43.3	188
Estonia	44.3	263
Malta	46.7	98
Ireland	50.0	1696
Latvia	51.0	384
Bulgaria	55.3	753
Luxembourg	57.4	349

1) Table 10 - EU Cybersecurity Companies 2014 to 2016 by Country

2) Table 11 - EU Cybersecurity Employment 2014 to 2016 by Country

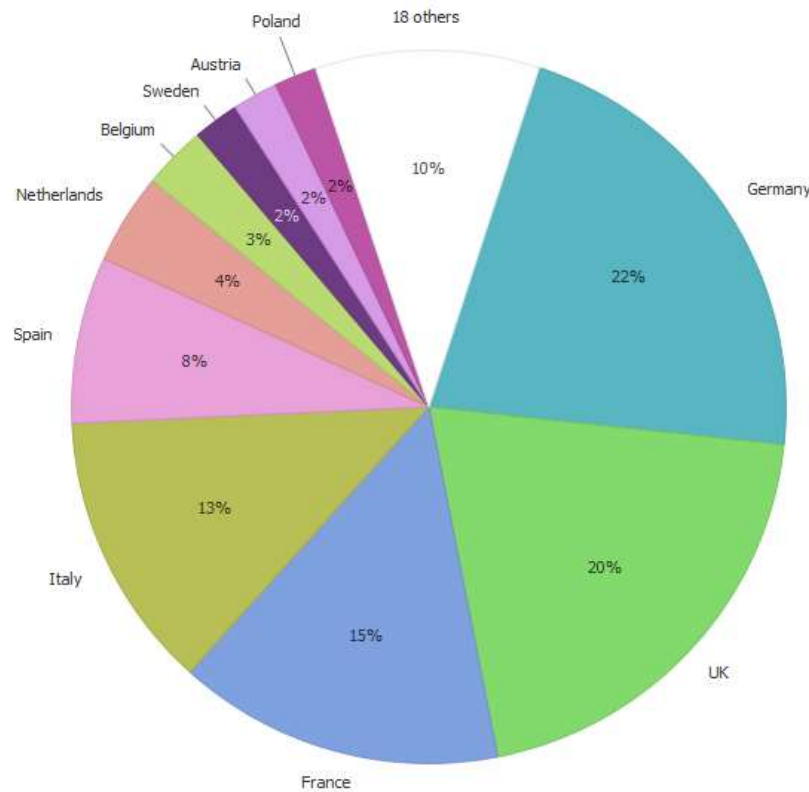
3) Table 12 - EU Cybersecurity Sales compared with GDP (EUR m) 2016

Figure 21 : Average Company Size mapped against Member State Sales in 2016.



Overall, the ranking of EU countries is demonstrated by Figure 22, representing Cybersecurity product and service sales by country for 2016. The country percentages are the same in 2014 and 2015. The top country ranking- Germany, UK, France and Italy- can be partially attributed to the relative size of their national economies.

Figure 22 : EU Sales % by EU Country 2016



These rankings change if Cybersecurity sales are considered as a percentage of national GDP. Table 16 compares Cybersecurity sales with GDP for 2016, by EU country. The table compares each country by share of EU sales, share of EU GDP and sales as a percentage of GDP⁵.

As an example, Germany represents a consistent set of values - 21% of EU GDP, 22% of EU Cybersecurity sales and sales as a percentage of GDP equals 1.1% (the average for the EU). Germany is ranked first by sales, first by GDP but 8th by sales as a share of GDP. In comparison:

- Bulgaria, Latvia, Slovakia, UK, Estonia, Slovenia and Italy rank highest for Cybersecurity sales as a percentage of GDP i.e. percentage is greater than average of 1.1%
- Ireland, Portugal and Luxembourg rank the lowest i.e. percentage is 0.6%, compared with EU average of 1.1%
- UK, Italy, Germany, Belgium and Spain all show a higher percentage of EU Cybersecurity sales compared with EU GDP.

⁵ GDP is based upon Eurostat 2016 GDP published 2017

Table 16 : EU Cybersecurity Sales compared with GDP (m EUR) 2016

Country	GDP EURm	% of EU GDP	Cyber Sales EURm	% of Cyber Sales	Cyber Sales as % of GDP
Austria	349,344	2.4	3,261	2.1	0.9
Belgium	421,611	2.8	4,542	2.9	1.1
Bulgaria	47,364	0.8	753	0.5	1.6
Croatia	45,819	0.3	337	0.2	0.7
Cyprus	17,901	0.1	188	0.1	1.1
Czech Republic	176,564	1.2	1,199	0.8	0.7
Denmark	277,339	1.9	2,076	1.3	0.7
Estonia	20,916	0.1	263	0.2	1.3
Finland	214,062	1.4	1,864	1.2	0.9
France	2,228,857	15.0	23,302	14.8	1.0
Germany	3,134,070	21.1	34,261	21.7	1.1
Greece	175,888	1.2	1,547	1.0	0.9
Hungary	112,399	0.8	1,023	0.6	0.9
Ireland	265,835	1.8	1,696	1.1	0.6
Italy	1,672,438	11.3	19,910	12.6	1.2
Latvia	25,021	0.2	384	0.2	1.5
Lithuania	38,637	0.3	316	0.2	0.8
Luxembourg	54,195	0.4	349	0.2	0.6
Malta	9,896	0.1	98	0.1	1.0
Netherlands	702,641	4.7	6,485	4.1	0.9
Poland	424,269	2.9	3,040	1.9	0.7
Portugal	184,934	1.2	1,180	0.7	0.6
Romania	169,578	1.1	1,140	0.7	0.7
Slovakia	80,958	0.5	1,109	0.7	1.4
Slovenia	39,769	0.3	476	0.3	1.2
Spain	1,113,851	7.5	11,943	7.6	1.1
Sweden	462,058	3.1	3,283	2.1	0.7
UK	2,366,911	16.0	31,950	20.2	1.3
Total	14,833,126	100.0	157,973	100.0	1.1

1.1.20 Conclusions and Recommendations

Looking at EU sales figures Germany, the UK, France and Italy have significantly larger sales than other Member States. The average number of employees in EU Cybersecurity companies is 15, but this varies across the EU from 8 in the UK to over 40 in Estonia, Ireland, Latvia, Bulgaria and Luxembourg. If one then looks at the trends in company size from 2014 to 2016, one sees that as the EU Cybersecurity market has developed and sales have grown the average size of a Cybersecurity company across the EU has fallen, though not substantially, with small falls in most Member States. If one looks at how average company size varies with the sales made by companies in Member States, the largest economies tend to have lowest average company size, as they have more extensive and likely more mature ecosystems with a higher proportion of small companies. This may offer larger economies a greater opportunity for innovation.

The level of supply chain fragmentation of Member State markets appears to be related to the size and level of maturity of these markets, but this is hard to prove from the analysis.

During the different workshops, a recurring theme for discussion was the recognition of the high number of companies throughout Europe and the high level of employment in comparison to the expectations of the participants. One important consideration was the high level of fragmentation of the market, especially in the larger and more mature markets. The overall recommendation from all the workshops was to identify and support companies that could be considered European Cybersecurity market leaders, that might need to become larger and stronger to participate on a global scale. This general appreciation for more consolidation rather than more fragmentation was apparent throughout the workshops.

Focus group participants noted that Cybersecurity is still an immature market so fragmentation is not surprising. There are a lot of innovative small companies and a growing M&A activity, which can be both good and bad. For example, it appears difficult to develop and grow EU companies in fields such as Encryption: acquisitions of SMEs by, for example, US companies is an ongoing issue, just as it is in other fast developing sectors such as Electric Vehicles. Differences in culture which drive investment (e.g. US venture capital funding associated with a strong risk-taking culture, Government-driven innovation funding programmes in Asia) give international competitors a competitive advantage compared to Europe, but this applies more widely than Cybersecurity.

There are also major barriers to the growth of start-ups in Europe. Failure by start-ups is culturally acceptable in the US but not in the EU, where entrepreneurs find it difficult to get financial backing if previous business ventures have been unsuccessful. Selling is difficult for start-ups and immature SMEs as users are very risk averse. Other barriers for start-ups include a need for lawyers (IP, employment, etc) which is very time consuming and distracts from the core growth aims of the business.

There may also be fragmentation in research projects and activities, with similar research happening in Spain, Germany and other parts of Europe. If this was combined or better coordinated a larger impact could be created, e.g. such as for the US Joint Strike Fighter in the defence research field.

It is recognised that it is very difficult for large companies to link to innovative SMEs, particularly as timescales for projects and funding budgets are very different. It is also difficult for large companies and SMEs to cooperate effectively across new developing value chains. For example, in Industry 4.0 connecting elements together to form a new value chain has security implications and requires large and small companies to cooperate across sectors, which is very challenging.

Cybersecurity clusters exist in a number of Member States and represent the views of and support small and large business and academia. These provide brokerage for collaborative projects and links as well as access to professional services (see EC Framework 7 'Facilitate Industry and Research in Europe' (FIRE) project reports, <http://www.trustworthyictonfire.com>). Many of the EU clusters have been stimulated by national or regional financial support and some have become self-sustaining through subscription models, etc. It was noted by participants that the US ecosystem is more sustainable as DARPA, DHS etc publish longer-lasting innovation pipelines/roadmaps.

The high density of strong academic institutions working in Cybersecurity located near Industry companies requiring access to this expertise is an EU strength (e.g. compared to Asia), as is the quality and low cost of education in the EU (e.g. compared to the US).

EU Cybersecurity Supply

In this section, the focus is on EU providers of Cybersecurity. Previous analysis identified approximately 60,000 companies involved in the delivery of Cybersecurity products and services.

1.1.21 Key Learnings

Only 14% of EU based Cybersecurity companies are part of the global top 500 market leading Cybersecurity highest growth companies. While many of the high growth companies have their representative offices in EU, the large majority of these companies are headquartered in the US. In the EU, the large majority of Cybersecurity companies are micro and small sized enterprises (approximately 74%). Should micro-enterprises be disregarded, the total number of companies would drop to 36,750 (from the 60,250), but the total Cybersecurity market size would drop less than 10%. EU Cybersecurity products and services are supplied by companies that originated from Cybersecurity, ICT, Security, Defence, Insurance and Academic sectors. The largest contribution is coming from the Cybersecurity sector itself (34%), but the originating domains of ICT (24%) and Defence/ Aerospace (20%), next to Security (14%) are also significant. The level of contribution from these originating sectors differs significantly on a country basis. In Denmark and Latvia (45%) or Greece (34%) for instance, the companies that developed in the Cybersecurity domain contribute far more to the Cybersecurity market than for instance in Belgium, where most products and services are being delivered by traditional ICT companies (30%).

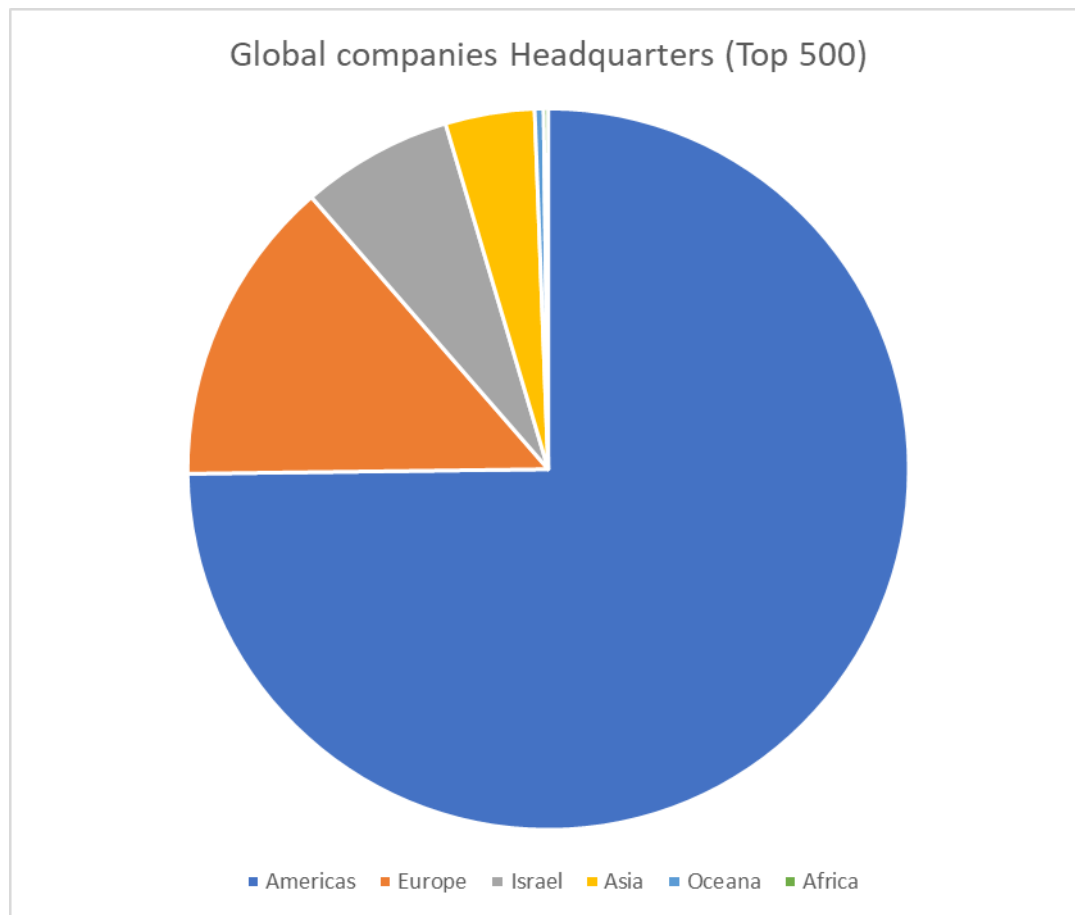
1.1.22 Analysis

From the global Cybersecurity sales data we identify the top 500 global Cybersecurity companies by sales volume, and where their corporate headquarters are based. The following Table and Figure shows where these top 500 global companies are based, comparing Europe to international competitors.

Table 17 : Global locations (corporate headquarters) of top 500 Cybersecurity providers

	Americas	Europe	Israel	Asia	Oceania	Africa
Global companies Headquarters (Top 500)	374	69	34	20	2	1
Proportion	74.8%	13.8%	6.8%	4.0%	0.4%	0.2%

Figure 23 : Global locations (corporate headquarters) of top 500 Cybersecurity providers



Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia.

In Figure 24, the Cybersecurity companies have been split into Micro (<10 employees), Small (10-49 employees), Medium (50- 249 employees) and Large (> 250 employees). The research estimates Micro companies at 23,280 (39%), Small companies as 21,240 (35%), Medium sized companies as 10,970 (18%) and Large companies (8%). These percentages are almost identical at the global level.

Figure 24 : EU Company Size Ranges

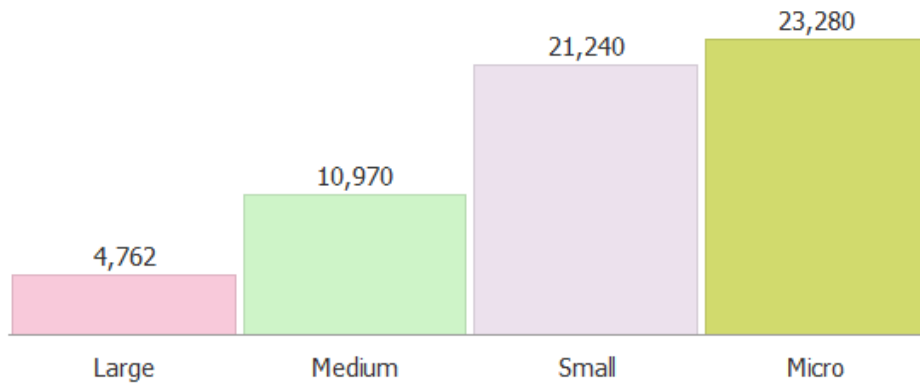


Figure 25 : EU Cybersecurity Providers Company Size Ranges by Country 2016



In Figure 25 the company size analysis is extended to each EU country. For all 28 countries, the ranges are:

- Micro- 32% (Denmark) - 44% (Germany)
- Small- 31% (Slovakia) – 40% (Denmark)
- Medium- 15% (Germany) – 22% (Belgium, Ireland and Slovenia)
- Large- 6% (Croatia, Germany and Slovakia) – 11% (Denmark).

Figure 25 demonstrates that the most significant difference across EU countries relates to the number of Micro businesses involved in delivering Cybersecurity. This is intuitively correct for an emerging sector and reflects the trend for skilled individuals and entrepreneurs to set up new and boutique

businesses. It is a reasonable assumption that the future health of the Cybersecurity sector will depend upon a) new micro businesses entering the market and b) current micro businesses becoming medium- sized enterprises. That said, if micro businesses were to be filtered out of the analysis, the company count would reduce by 39% to 36,750 but the sales value for the sector would decrease by less than 10%.

Cybersecurity is also something of a hybrid sector, in that its roots extend into companies in sectors like ICT, Defence and Security. Everyone involved in the sector can name Defence or ICT companies that are also involved in Cybersecurity but, as yet, the inter- relations between these sectors have not been mapped. The perception is that Cybersecurity activities have primarily emerged from the ICT sector. Research was, therefore conducted into the company base for delivering Cybersecurity products and services, identifying the core sector for that company and the proportion of its business that relates to Cybersecurity.

An example of this is shown in Table 18 : Example for Constructing the Typology of Cybersecurity Providers, using six corporates as examples to illustrate their core business activity and then, what proportion of their activities relate to other activities- including Cybersecurity. These proportions are then converted into sales values, aggregated and then used to calculate the proportion of Cybersecurity sales generated by companies falling within the seven sectors of Cyber, ICT, Defence, Security, Academia, Insurance and “Other”. For example, BAE Systems is an Aerospace/ Marine company, aligned closely with the Defence sector that also happens to provide Cybersecurity activities that are NOT related to Cyber defence.

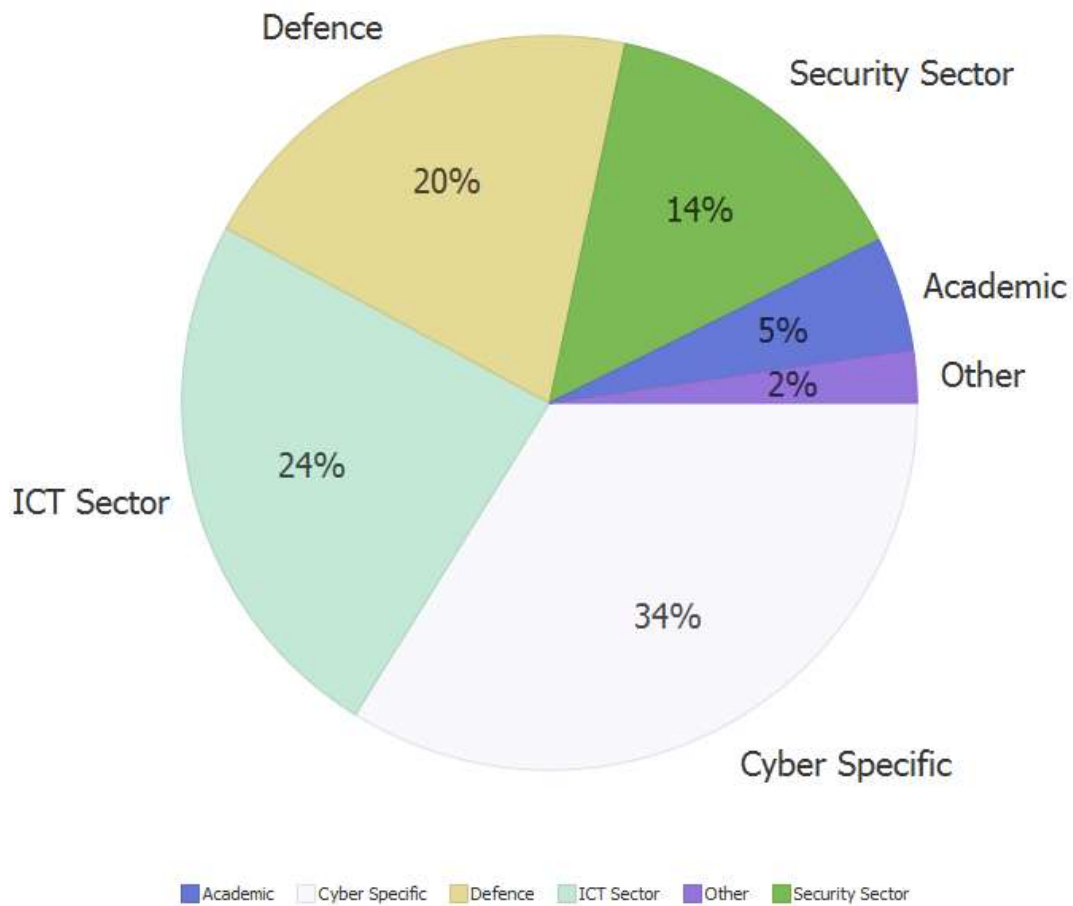
Table 18 : Example for Constructing the Typology of Cybersecurity Providers

Company	Approximation of total business activity % outside main stream business					
	Main Stream Business	ICT	Defence	Security	Cyber	Other
BAE Systems	Aerospace, Marine	2.3	4.6	7.2	6.3	1.3
Airbus	Commercial Aerospace	1.4	3.3	2.6	2.4	2.4
BT Group plc	Telecoms		1.1	1.4	3.5	0.92
QinetiQ	Defence	4.6		8.4	11.3	1.6
Thales Group	Marine, Aerospace	1.2	3.4	14.3	4.5	2.5
Rockwell Collins	Rail, Air, Infrastructure	3	2.2	11.3	3.5	1.8

Further information about the methodology employed, the definitions of each “sector” and how allocations are made to each category is part of the Research Methodology description in Chapter 0.

Figure 26 summarizes the sectors involved in delivering Cybersecurity products and services for the EU. It shows that 34% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 24% originates from companies whose core business is ICT, 20% originates from companies whose core business is Defence/ Aerospace and 14% from companies whose core business is Security. Cyber Insurance is only delivered by Insurance companies and Academia (through spin-out, research partnership or consultancy accounts for 5%. “Other” includes the 2% that cannot be allocated elsewhere.

Figure 26 : Contribution into Cybersecurity by Sector in EU



While these results rely on some subjective assessments of company core activities and estimates of the proportion of revenues relating to Cybersecurity, they do reveal that the roots of Cybersecurity reach beyond the ICT sector.

When the research results are disaggregated by sub-sector of Cybersecurity (see Figure 27) then Cybersecurity contributions range between 21-44%, Defence 14-25%, ICT 15-29%, Security 10-18% and Academia 4-6%.

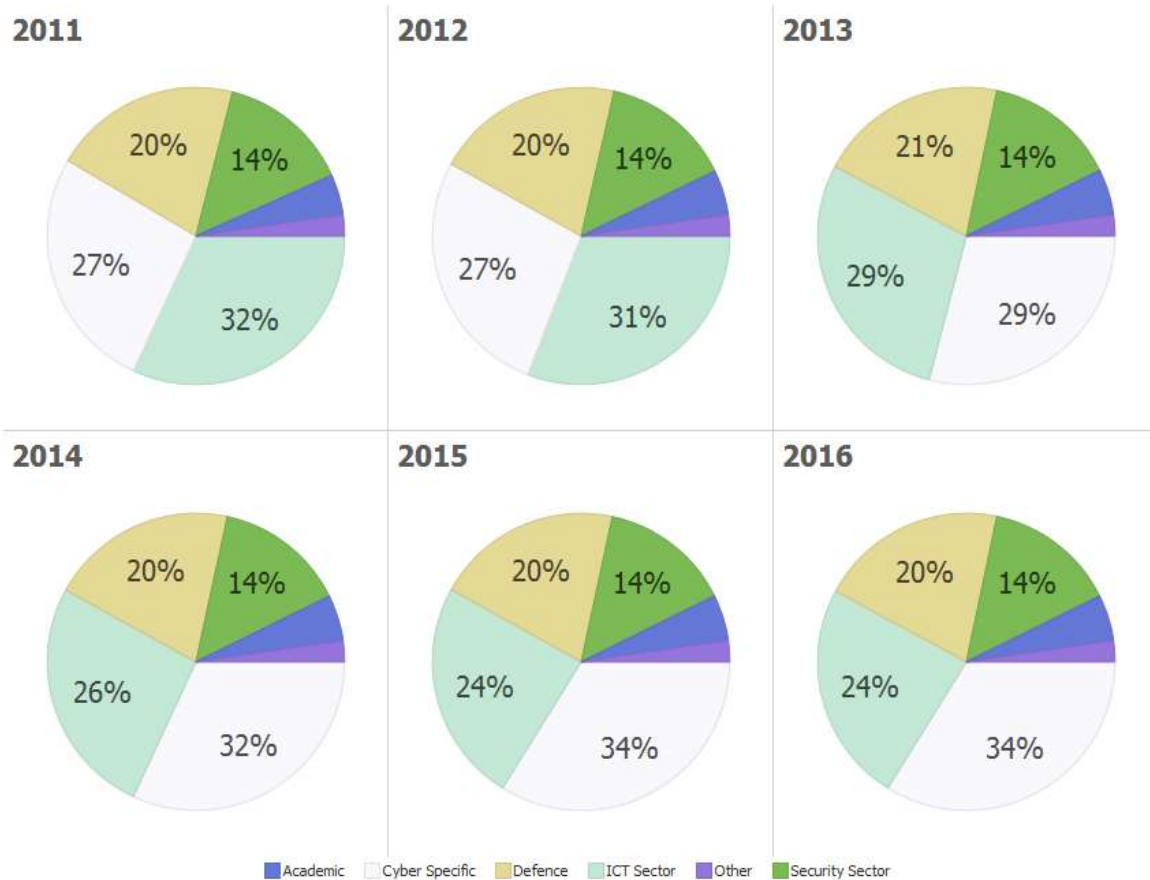
Figure 27 : Contribution in Cybersecurity Sales by Sector, related to by Sub-sector



Cyber Insurance and Training & Education were omitted from this graphic as they are delivered by a single sector.

In Figure 28, the sectoral base of EU Cybersecurity was analysed from a historical perspective, traced back to 2011. This analysis showed that the contribution of Cybersecurity specific companies increased annually, from 27% to 34% of the total.

Figure 28 : Relative Contribution in Cybersecurity Sales by Sector – historical perspective (from 2011 to 2016)



In comparison, the ICT sector as a contributor to the overall Cybersecurity market decreased from 32% to 24% over the last five years, with all other sectors remaining consistent as a percentage of the total for all five years. This analysis suggests that a) some ICT companies have specialised in Cybersecurity over this period and have re-branded themselves and b) an increasing number of new entrants into the marketplace are Cyber specific companies.

Historical analysis for 2011- 2016 reveals also the following:

- Anti Malware Cyber specific percentage increased from 29-41%, with a corresponding reduction for ICT from 35-22%
- Application Security Cyber specific percentage increased from 19-33%, with a corresponding reduction for ICT from 43-27%
- Business Continuity Cyber specific percentage increased from a low 11% to 25%, with a corresponding reduction for ICT from 44-29%
- Encryption Cyber specific percentage increased from a high of 38% to 41%, with a corresponding reduction for ICT from 20-15%
- Outsourcing/ Managed Services Cyber specific percentage started at 44% and has remained static over the period.

This analysis confirms that Cybersecurity specific companies have become more important for the development of some sub-sectors of Cybersecurity than others, but that overall delivery from Cybersecurity specific companies represents an increasing proportion of sector value and growth.

The final analysis is by sector and by country, summarised in Figure 29.

Figure 29 : Contribution of Cybersecurity by Sector and per Country



Figure 29 shows the proportion of Cybersecurity activities per country contributed per sector. It shows that the average of 34% of activities being contributed by dedicated Cybersecurity companies ranges between 15% and 45% (Latvia and Denmark). In comparison:

- Defence (average 20%) ranges between 13% (Denmark) and 24% (Germany)
- ICT (average 24%) ranges between 17% (Greece and Latvia) and 30% (Belgium)
- Security (average 14%) ranges between 9% (Cyprus) and 20% (Spain).

Analysis per country and by sector raises the question whether existing strong sectors (Defence in Germany) influence how Cybersecurity products and services are delivered at the national level, and even further, how the Defence sector influences Cybersecurity and conversely.

1.1.23 Conclusions and Recommendations

Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia. This reinforces the workshop recommendation of the need to identify and support companies that could be considered European Cybersecurity market leaders, that might need to become larger and stronger to participate on a global scale.

Looking at the sizes of EU Cybersecurity companies they comprise 39% micro, 35% small, 18% medium and 8% large companies: these proportions are almost identical at the global level. The distribution of company sizes varies significantly across Member States e.g. micro-companies are 32% of companies in Denmark through to 44% in Germany.

Cybersecurity activities and companies have not emerged solely from the ICT sector, but from across a range of market sectors. Looking at the sectors involved in delivering Cybersecurity products and services for the EU in 2016, 34% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 24% originates from companies whose core business is ICT, 20% originates from companies whose core business is Defence/ Aerospace and 14% from companies whose core business is Security. There are also significant variations in these figures between Member States, with a significantly higher contribution from Cybersecurity originating companies in Denmark, Latvia, and Greece while in other countries such as Belgium, Sweden, and Germany other industries are contributing more significantly to the Cybersecurity market and benefitting these Member State Cybersecurity industries. **Further study of the impact of Cybersecurity technologies in the Defence domain and their relationship to Cybersecurity activities for other applications, to investigate measures that would help the EU and individual Member States obtain the full benefits of dual use, should be considered.**

EU Cybersecurity End- Users

In this section, the focus is on EU end-users of Cybersecurity, the purchasing companies/ organisations. This part of the research started in 2014 and has been further developed here. The research aims to divide end- users of Cybersecurity products and services into categories:

- Public- includes any national, regional or local department, organisation or agency that includes Cybersecurity as part of its remit and is funded by government.
- Private- includes a range of industries- Utilities, Transport etc.- based upon Critical Infrastructure definitions from the different Member States
- “Other”- relates to Private sector activities and includes most retail activity, transactions that are too small to identify or that (for commercial or other reasons) are not traceable to any of the other Private end- user markets.

1.1.24 Key Learnings

The Cybersecurity Industry Market Analysis defines 16 end user categories, based upon the Cybersecurity market flows, orienting towards identifying critical infrastructures, as they were defined by the European Member states. The private sector is by far the largest consumer, accounting for nearly 45% of the total EU Cybersecurity Market. A large portion of the market cannot be identified, as the data sources do not allow it to be categorized reliably under either public or private. For example, some of it includes retail, but it is not identifiable as a significant contributor as such. From the private sector, the Defence Industries are the single largest individual sector also purchasing Cybersecurity products and services. Utilities such as Water and Energy industries, follow Information Technology industries as the next other large Cybersecurity consumers. The 13 subcategories of products differ somewhat per sector. For instance, relatively more Infrastructure and Cyber Consultancy Services are purchased by Private sector, whereas an almost equal spend is going to System Recovery and Data Cleansing for Public and Private, relatively speaking only a little is being spent by the Other domain on this service. There are significant differences between EU countries in the relative contribution by the public sector: in countries like UK, Poland, Greece, Lithuania, Croatia and Czech Republic public spending is significantly higher (over 40%) than in other countries in Europe (around 26%).

1.1.25 Analysis

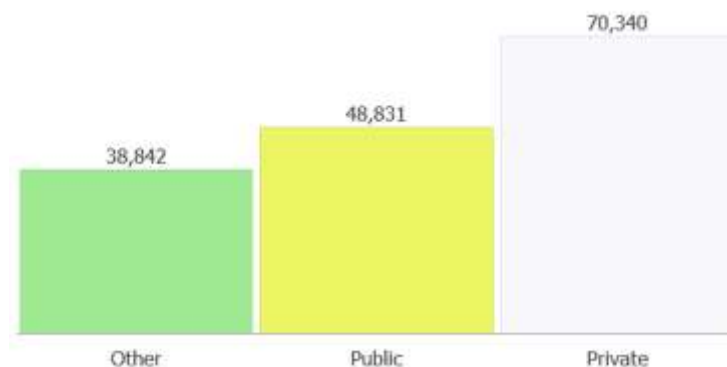
For the Private Sector, the 16 categories used for analysis of end- users are:

- Chemical & Pharma Processing
- Commercial Facilities
- Communications
- Manufacture & Assembly
- Emergency Services
- Defence Industries
- Financial Services
- Construction
- Food & Agriculture
- Energy
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Education Sector
- Transport & Logistics
- Water & Wastewater Utilities

The content related to each heading is defined in **Chapter 0, Section 1.1.127 End- User Types and Markets**

Figure 30 presents the three main categories of End- users for the EU-Private equals EUR 70,340 million (45%), Public EUR 48,831 million (31%) and “Other” EUR 38,842 million (25%). The “Other” category is so large because it includes retail activities (10%), un-attributable activities (10%) and activities relating to sectors other than the 16 listed (5%). Efforts to reduce the “Other” category are ongoing, but require better sources of data and reporting from end- users before more accurate allocations of the 25% can be achieved.

Figure 30 : EU Cybersecurity End-User Distribution according to Private, Public and other markets



In Figure 31, the Private category is broken down into the 16 sub categories. This shows that: Defence accounts for 7% of the Cybersecurity total with Information technology, Water Utilities and Government Facilities each accounting for 4%. Financial Services is suspiciously low at 2% of the total and it is suspected (but not yet proven due to a lack of transparency in the source data) that much of the unattributed portion of “Other” may relate to Financial Services.

Figure 31 : EU Cybersecurity End- Users- Full Break Down

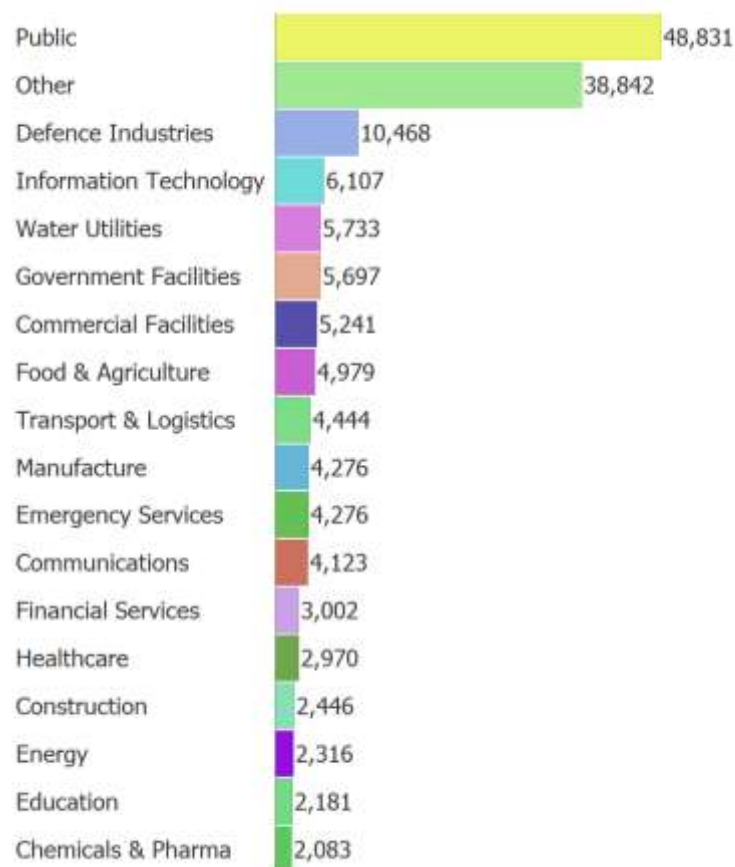


Figure 32 segments each Cybersecurity sub-sector by Private, Public and “Other”. The “Other” category ranges between 2% for Cyber Insurance (high data transparency) to 34% for Application Security. The Public category ranges between 22% for Identity & Access Based Services to 53% for Cyber Insurance.

Figure 32 : EU Cybersecurity End-Users Distribution by Sub-sector



Figure 33 : EU Cybersecurity End-Users Distribution by Country



This analysis is extended in **Appendix E : Competitive Dashboards**, where tables are included for each EU country. This research stream suggests that there is still much that is unknown about the end-users of Cybersecurity (due to high level of granularity in End-User types to reduce the level of un-

attributable activity – Other category), but what is known shows different patterns of procurement in each EU country- by sub-sector and by End- User market.

Figure 33 segments each EU country by Private, Public and “Other”. The “Other” category ranges between 8% (Poland) to 34% (Germany). The Public category ranges between 24% (Germany) to 48% (UK) and the Private category ranges between 41% (Austria) to 49% (Czech Republic, France and Poland).

Measuring sales by Cybersecurity sub-sector and by End-User market is presented in sales for the whole of the EU, with End-Users Markets as rows and Cybersecurity sub-sectors as columns (Table 19 : EU Sales by Level 2 Sub Categories and Distributed over End-User Markets). The table shows that the Public Sector and “Other” categories combined account for between 55-56% of each sub-sector, with Defence Industries accounting for 7% of all sub-sectors, followed by Government Facilities and Water Utilities with 4% of all sub-sectors.

Table 19 : EU Sales by Level 2 Sub Categories and Distributed over End-User Markets

End- User Market	Anti Malware	Application Security	Business Continuity	Cyber Consultancy	Cyber Security Insurance	Encryption	Identity & Access	Infrastructure	Mobile	Outsourced/ Managed Services	Situational Awareness	System Recovery & Data Cleansing	Training & Education	Total	% of Total
Chemicals & Pharma	76	351	177	30	56	30	119	443	35	30	453	283	1	2,083	1.32
Commercial Facilities	287	883	408	74	145	75	276	1,154	95	78	1,089	673	4	5,241	3.32
Communications	217	735	339	59	114	61	220	778	77	59	912	550	3	4,123	2.61
Manufacturing	252	751	341	58	119	62	222	895	77	61	874	562	3	4,277	2.71
Defence Industries	606	1,728	846	148	291	154	563	2,245	176	155	2,130	1,419	7	10,468	6.63
Public	4,501	14,339	6,751	1,188	2,215	1,195	4,384	17,175	1,437	1,172	17,080	10,870	59	82,367	55.50
Construction	143	385	189	35	64	35	121	565	42	38	512	316	2	2,446	1.55
Financial Services	182	557	223	52	87	52	150	549	56	47	620	425	2	3,002	1.90
Food & Agriculture	287	836	425	73	141	70	262	1,056	86	67	1,010	662	3	4,979	3.15
Energy	129	435	183	32	66	34	126	438	41	38	470	323	1	2,316	1.47
Government Facilities	305	958	459	81	158	84	306	1,159	100	84	1,227	772	4	5,697	3.61
Healthcare	153	507	230	42	82	43	150	673	51	42	599	399	2	2,971	1.88
Information Technology	368	1,053	507	85	167	86	318	1,276	113	81	1,239	810	4	6,107	3.87
Education	156	399	167	29	58	33	109	469	33	28	415	284	1	2,181	1.38
Transport & Logistics	257	787	356	63	125	63	237	912	79	63	908	591	3	4,444	2.81
Water Utilities	313	963	453	85	160	86	317	1,173	100	87	1,211	781	4	5,733	3.63
Emergency Services	252	751	341	58	119	62	222	895	77	61	874	562	3	4,277	2.71
Total	8,756	27,296	12,813	2,272	4,301	2,296	8,376	33,040	2,763	2,261	32,717	20,971	111	157,973	100.00
% of Total	5.5	17.3	8.1	1.4	2.7	1.5	5.3	20.9	1.7	1.4	20.7	13.3	0.1	100	

This analysis is extended in **Appendix A : EU Country Level Data**, , where tables are included for each EU country. There is still much that is unknown about the end- users of Cybersecurity (with research ongoing to reduce the level of unattributable activity), but what is known shows different patterns of procurement in each EU country- by sub-sector and by End-User market.

1.1.26 Conclusions and Recommendations

The EU End User markets in sales terms comprises Private users (45% of sales), Public users (31%) and “Other” users (25%). The “Other” category is large because it includes retail activities (10%) and un-attributable activities (10%). The Public sector Cybersecurity market ranges between 24% (Germany) to 48% (UK) and the Private sector Cybersecurity market ranges between 41% (Austria) to 49% (Czech Republic, France and Poland).

Given the large expenditure by the EU public sector in Cybersecurity (EUR 48,831 million or 31% of the market), a more strategic approach to public sector expenditure on Cybersecurity could have a significant impact on the European Cybersecurity market and strengthen the positioning of EU Cybersecurity companies globally.

In the workshops, participants were clear on the need for national governments and the EU to lead by example. The US built up its leading ICT market position through military funding. Cybersecurity is not seen as a strategic defence capability in the EU unlike in the US. Industry needs to be supported with a strategic view at EU level.

While governments are policy makers and supporters of the competitiveness of national companies, products are also bought from outside their region and Europe. Current EU Public Procurement policies which focus on the best price are not conducive to building up national champions and markets, e.g. Thales and Leonardo tried to develop firewalls but stopped as it was not commercially beneficial. **Public Procurement could be split into two: (1) for commodity purchasing, (2) strategic with an industrial policy. The use of Defence funds could also be considered.**

PCP instruments were largely unknown to the Cybersecurity focus group participants. Innovative procurement could be considered in order to stimulate faster acceptance of technology.

EU Cybersecurity Imports⁶

Cybersecurity imports are a measure of the products and services that enter the EU from outside of its geographic borders. In this section imports are analysed by: EU and Non- EU country; Cybersecurity product and service and Originating market (within and without the EU).

1.1.27 Key Learnings

The EU imports EUR 8.5 billion in Cybersecurity Products and Services from outside of the EU, which is approximately 5.4% of the total EU Cybersecurity market in 2016 and accounts for approximately 18% of the global Cybersecurity imports. In absolute terms, Germany and Italy are the largest importers outside of the UK. However, there is a large variation in terms of EU countries importing from outside EU compared to within the EU. Denmark, Czech Republic, UK and Bulgaria – but actually 11 of the 28 Member States import most (over 80%) of their total imports from outside of the EU. Only France is importing more than half of its imports from within the EU. However, France is only importing 4.7% from its total Cybersecurity market. Taking the perspective of imports in relation to the total Cybersecurity market per country further, most Eastern-European countries (Hungary, Estonia, Latvia, Czech Republic, Romania and Bulgaria), next to Portugal are importing most. UK has been importing only 3% in comparison to the total UK Cybersecurity market (EUR 31,950 million), in 2016. Other significant Cybersecurity markets in Europe such as Germany (5.1%), Italy (5.3%), Spain (5.1%) are in the same category. Subcategories representing Encryption (79.4%) and Outsourced / Managed Services (79.7%) appeared to be relatively the highest in imported products and services into the EU Cybersecurity market from outside of the EU. In absolute terms both Situational Awareness and System Recovery & Data Cleansing subcategories, represent both over EUR 2 billion in imports from outside of the EU.

⁶ The Cybersecurity Industry Market Analysis (CIMA) is the presentation of the results from the analysis of the actual Cybersecurity products and services trade activities. Numbers presented are the result of the combined and concluded sales of these actual products and services during the period of 2016.

1.1.28 Analysis

Global imports for 2016 are estimated at EUR 48,000 million, of which EUR 12,100 million or 25% arrived in the EU. Table 20 shows EU imports divided into imports from within the EU and from outside of the EU. The overall value of Non- EU imports is EUR 8,504 million or 70%, with 30% of imports from within EU countries. The highest volume importers are Germany, France, Italy and the UK.

*Table 20 : Total Imports and EU Imports by EU Country in (m EUR),
alphabetical order and ordered by Non-EU % imports*

Country	Imports	Imports EU	EU %	Imports Non- EU	Non- EU %	Country	Imports	Imports EU	EU %	Imports Non- EU	Non- EU %
Austria	622.5	208.2	33.4	414.3	66.6	Denmark	479.1	74.7	15.6	404.4	84.4
Belgium	529.8	175.6	33.1	354.2	66.9	Czech Republic	424.3	68.3	16.1	355.9	83.9
Bulgaria	236.1	42.1	17.8	194.0	82.2	UK	949.5	163.6	17.2	785.9	82.8
Croatia	28.1	5.6	19.7	22.6	80.3	Bulgaria	236.1	42.1	17.8	194.0	82.2
Cyprus	8.9	1.8	19.7	7.1	80.3	Poland	503.0	91.6	18.2	411.4	81.8
Czech Republic	424.3	68.3	16.1	355.9	83.9	Hungary	472.7	86.2	18.2	386.5	81.8
Denmark	479.1	74.7	15.6	404.4	84.4	Malta	4.0	0.8	19.3	3.2	80.7
Estonia	108.8	24.8	22.8	84.0	77.2	Croatia	28.1	5.6	19.7	22.6	80.3
Finland	395.7	86.5	21.9	309.2	78.1	Cyprus	8.9	1.8	19.7	7.1	80.3
France	1,102.9	587.9	53.3	515.0	46.7	Greece	454.2	90.2	19.9	364.0	80.1
Germany	1,753.9	554.5	31.6	1,199.4	68.4	Slovakia	44.9	8.9	19.9	36.0	80.1
Greece	454.2	90.2	19.9	364.0	80.1	Slovenia	22.4	4.6	20.5	17.8	79.5
Hungary	472.7	86.2	18.2	386.5	81.8	Ireland	72.0	14.8	20.6	57.2	79.4
Ireland	72.0	14.8	20.6	57.2	79.4	Luxembourg	15.7	3.2	20.6	12.4	79.4
Italy	1,051.4	443.5	42.2	607.9	57.8	Latvia	141.2	29.1	20.6	112.2	79.4
Latvia	141.2	29.1	20.6	112.2	79.4	Finland	395.7	86.5	21.9	309.2	78.1
Lithuania	93.9	25.2	26.9	68.7	73.1	Sweden	396.6	88.6	22.3	308.0	77.7
Luxembourg	15.7	3.2	20.6	12.4	79.4	Romania	392.8	88.1	22.4	304.8	77.6
Malta	4.0	0.8	19.3	3.2	80.7	Estonia	108.8	24.8	22.8	84.0	77.2
Netherlands	774.1	278.5	36.0	495.5	64.0	Lithuania	93.9	25.2	26.9	68.7	73.1
Poland	503.0	91.6	18.2	411.4	81.8	Portugal	413.4	112.1	27.1	301.3	72.9
Portugal	413.4	112.1	27.1	301.3	72.9	Germany	1,753.9	554.5	31.6	1,199.4	68.4
Romania	392.8	88.1	22.4	304.8	77.6	Belgium	529.8	175.6	33.1	354.2	66.9
Slovakia	44.9	8.9	19.9	36.0	80.1	Austria	622.5	208.2	33.4	414.3	66.6
Slovenia	22.4	4.6	20.5	17.8	79.5	Netherlands	774.1	278.5	36.0	495.5	64.0
Spain	603.8	232.4	38.5	371.4	61.5	Spain	603.8	232.4	38.5	371.4	61.5
Sweden	396.6	88.6	22.3	308.0	77.7	Italy	1,051.4	443.5	42.2	607.9	57.8
UK	949.5	163.6	17.2	785.9	82.8	France	1,102.9	587.9	53.3	515.0	46.7
Total	12,095.6	3,591.4	29.7	8,504.2	70.3	Total	12,095.6	3,591.4	29.7	8,504.2	70.3

The percentage of imports from within the EU varies by country (see Figure 34). For the UK it is as low as 17%, while for France it is as high as 53%. The strongest inter-trading relations within the EU for Cybersecurity include France, Italy, Spain, Netherlands, Austria, Belgium and Germany.

At the individual country level the analysis breaks down imports in more detail. In Figure 34 two examples - France and the UK- are compared using the originating countries for imports. For the UK 25% of imports were from the USA (compared with 17% for France), while 30% of French imports came from Germany (compared to 4% for the UK). The top countries for UK imports were USA, China, India, Japan and Germany compared with France- Germany, USA, China, Italy and UK. This analysis suggests that very different trading patterns exist within the EU. As a result a similar analysis for each EU country has been applied using the charts at **Appendix C : Imports by Country of Origin per EU Member State**. At the EU- country level the percentage of imports from China ranges between 10-43%, the USA range is between 7-32%, Germany between 4-30%, UK between 3-14% and Japan between 3-8%.

Figure 34 : EU and Non- EU Imports for UK and France

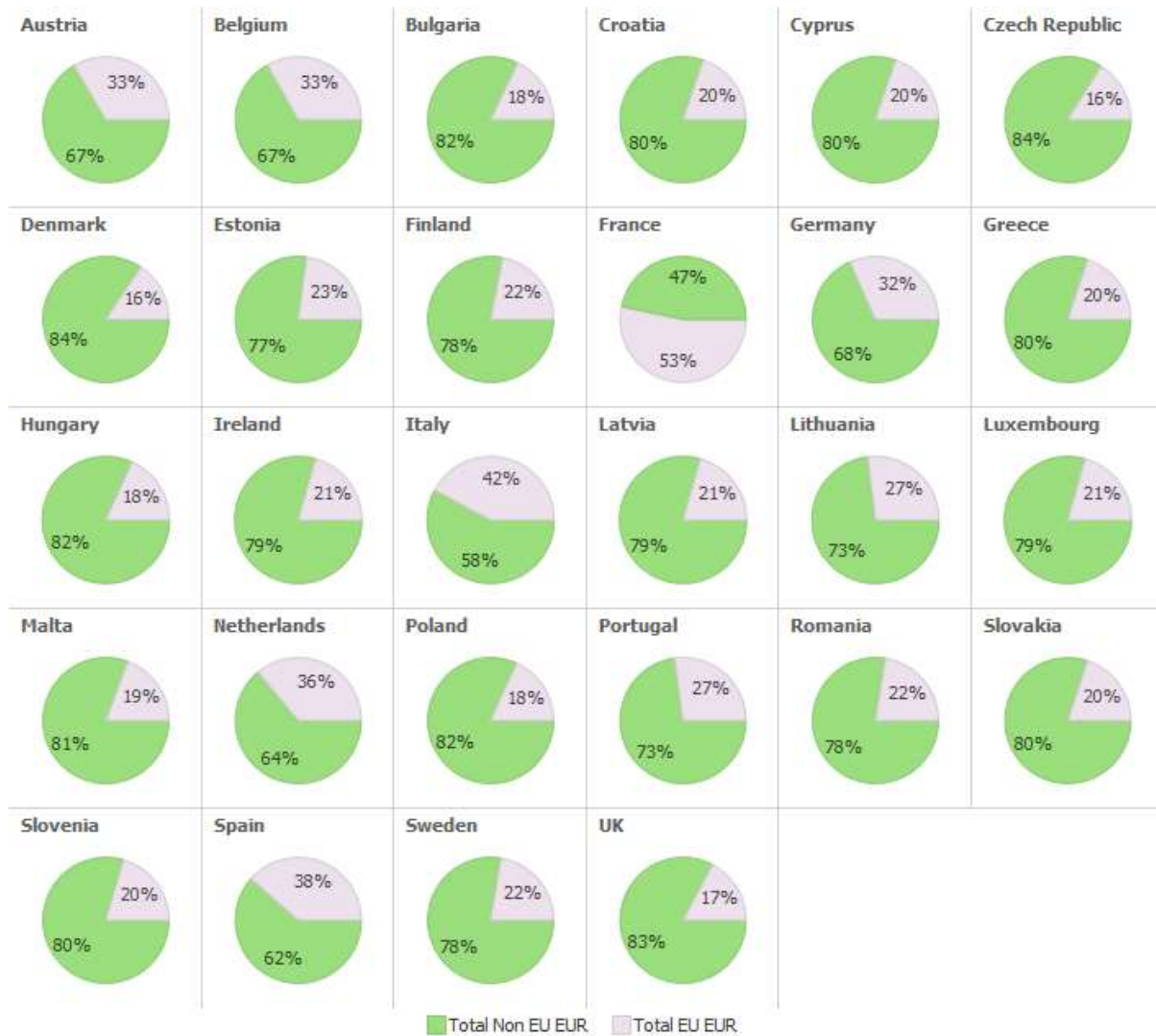
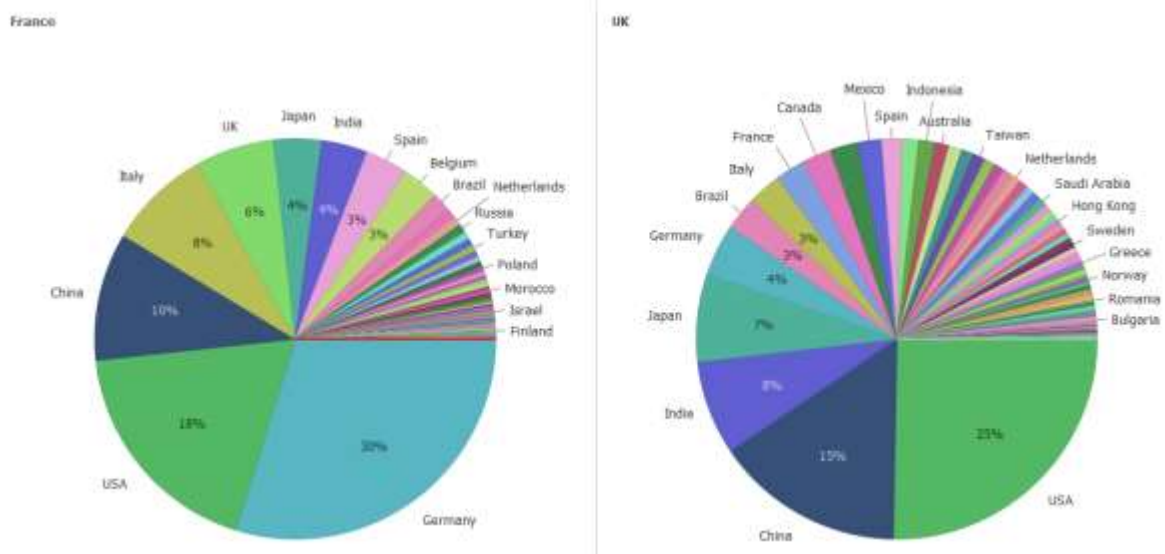


Figure 35 : EU and Non- EU Imports for UK and France- % by Country



Imports have been analysed by sub-sector in Table 21 which demonstrates that EU imports (average 30%) vary between 20% for Encryption and Outsourced/ Managed Services and 32% for Situational Awareness and System Recovery & Data Cleansing

Table 21 : EU Imports by Sub-sector 2016 (m EUR) – alphabetical and top down non-EU % imports

Sub Sector	All Imports EURM	EU Imports EURM	EU % of Imports EURM	Non- EU Imports EURM	Non- EU % of Imports EURM
Anti Malware	487	135	27.7	352	72.3
Application Security	997	300	30.0	698	70.0
Business Continuity	605	164	27.2	441	72.8
Cyber Consultancy	379	90	23.7	289	76.3
Cyber Security Insurance	397	117	29.4	281	70.6
Encryption	245	51	20.6	194	79.4
Identity & Access	864	193	22.3	671	77.7
Infrastructure	1,085	308	28.4	777	71.6
Mobile	378	115	30.4	263	69.6
Outsourced/Managed Services	253	51	20.3	202	79.7
Situational Awareness	3,340	1,084	32.5	2,256	67.5
System Recovery & Data Cleansing	3,020	972	32.2	2,049	67.8
Training & Education	44	12	27.2	32	72.8
Total	12,096	3,591	29.7	8,504	70.3

Upon assessment of the intensity of imports by EU Member State by calculating a simple proxy measure- imports as a percentage of country sales, Table 22 : Imports in EU by Country in Import as % of Sales – alphabetically and top down % - compares sales and imports for each country. The ratio of imports to sales on average is 7.7% for all of the EU, but ranges between 3-46% for individual countries.

Table 22 : Imports in EU by Country in Import as % of Sales – alphabetically and top down %

Country	Sales (m EUR)	Imports (m EUR)	Imports as % of Sales
Hungary	1.022	473	46.2
Estonia	263	109	41.4
Latvia	384	141	36.7
Czech Republic	1.198	424	35.4
Portugal	1.180	413	35.0
Romania	1.140	393	34.5
Bulgaria	753	236	31.4
Lithuania	316	94	29.7
Greece	1.546	454	29.4
Denmark	2.076	479	23.1
Finland	1.864	396	21.2
Austria	3.261	622	19.1
Poland	3.040	503	16.5
Sweden	3.283	397	12.1
Netherlands	6.485	774	11.9
Belgium	4.542	530	11.7
Croatia	337	28	8.3
Italy	19.910	1.051	5.3
Germany	34.261	1.754	5.1
Spain	11.943	604	5.1
France	23.302	1.103	4.7
Cyprus	188	9	4.7
Slovenia	476	22	4.7
Luxembourg	349	16	4.5
Ireland	1.696	72	4.2
Malta	98	4	4.1
Slovakia	1.109	45	4.1
UK	31.950	950	3.0
Total	157.973	12.096	7.7

The countries with the lowest intensity of imports are:

- UK 3%
- Slovakia and Malta 4.1%
- Ireland 4.2%

- Luxembourg 4.5%
- Cyprus, France and Slovenia 4.7%.

The countries with the highest intensity of imports are:

- Hungary 46.2%
- Estonia 41.4%
- Latvia 36.7%
- Czech Republic and Portugal 35%.

There is no correlation between the ratio of EU to Non- EU imports and import intensity.

By comparing Member State domestic demand (sales generated by companies domestically plus imports minus exports) with imports it is possible to analyse to what extent each EU country is able to meet its own Cybersecurity needs or has to meet its needs by imports. The following Table and Figure shows imports as a share of total demand in each EU Member State, showing how dependent EU countries are on Cybersecurity imports (from inside and outside the EU) to meet their needs.

Table 23 : Imports as a share of domestic demand in each EU Member State

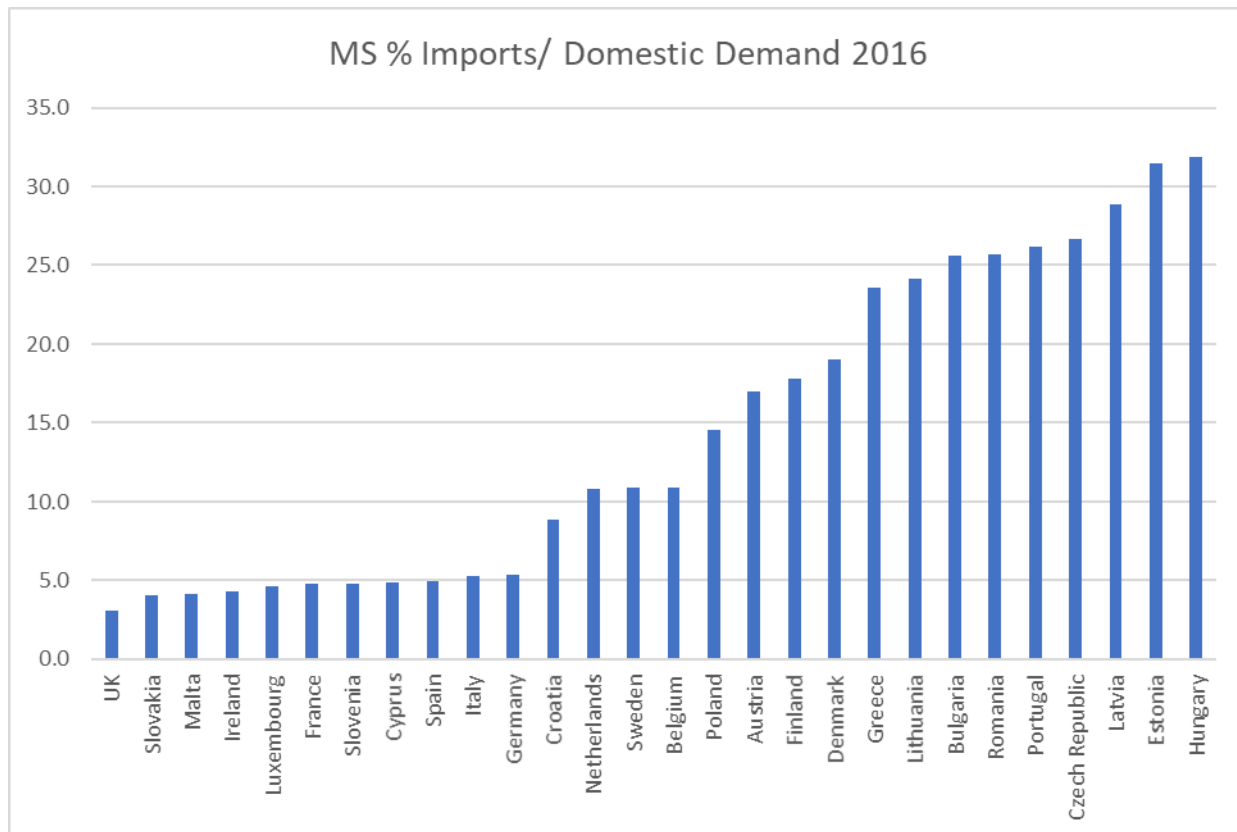
MS	MS % Imports/ Domestic Demand 2016	MS Domestic Demand (€m) 2016 (1,2,3)	Member State Imports (€m) 2016 (2)
UK	3.1%	30522.0	949.5
Slovakia	4.1%	1097.9	44.9
Malta	4.1%	96.9	4
Ireland	4.3%	1661.7	72
Luxembourg	4.6%	341.7	15.7
France	4.8%	23054.1	1102.9
Slovenia	4.8%	465.5	22.4
Cyprus	4.8%	183.8	8.9
Spain	4.9%	12256.1	603.8
Italy	5.3%	19829.4	1051.4
Germany	5.4%	32747.3	1753.9
Croatia	8.8%	318.1	28.1
Netherlands	10.8%	7152.1	774.1
Sweden	10.9%	3649.0	396.6
Belgium	10.9%	4847.8	529.8
Poland	14.5%	3457.2	503
Austria	17.0%	3665.3	622.5
Finland	17.8%	2224.5	395.7
Denmark	19.0%	2522.6	479.1
Greece	23.5%	1929.5	454.2
Lithuania	24.1%	389.2	93.9
Bulgaria	25.6%	922.1	236.1
Romania	25.7%	1526.8	392.8
Portugal	26.2%	1578.8	413.4
Czech Republic	26.6%	1593.3	424.3
Latvia	28.9%	489.2	141.2
Estonia	31.4%	346.1	108.8
Hungary	31.9%	1481.8	472.7
EU COMBINED	5.3%	160350	8504

1) Table 12 - EU Cybersecurity Sales compared with GDP EURM 2016

2) Table 15 - EU Imports by Country 2016 EURM

3) Table 18 - EU Exports by Country 2016 EURM

Figure 36 : Imports as a share of domestic demand in each EU Member State



EU Country Cybersecurity imports as a share of their domestic size average vary from 3.1% for the UK to above 25% for Bulgaria, Romania, Portugal, Czech Republic, Latvia, Estonia, Hungary. However, some of these imports into EU countries come from other EU Member States. The EU is a net importer of Cybersecurity solutions. It imports 5.3% of its Cybersecurity products and services from non-EU sources, even when international suppliers such as IBM that base supply operations in the EU are counted as EU suppliers in the market data.

1.1.29 Conclusions and Recommendations

Since the Cybersecurity Industry Market Analysis has investigated actual trade sales, which have been presented in this report, it should be clear that the accounting process does include global and international Cybersecurity companies operating and trading in the EU, and therefore being considered as European companies. Mechanisms to more clearly identify companies as European as opposed to non-European on the basis of identifiable attributes⁷, could lead to import figures being revised. Currently, the basis for a European company, is the legal entity being in a European Member State which contributes to the European Member State GDP.

⁷ Attributes such as EU-headquarters, R&D facilities, number of people in the European versus other international entities, origin and nationality of the management team, shareholders, ... could identify whether a company should be regarded as European or non-European.

The EU Country Cybersecurity Industry Market imports as a share of their domestic market size average vary from 3.1% for the UK to above 25% for Bulgaria, Romania, Portugal, Czech Republic, Latvia, Estonia, Hungary. However, some of these imports into EU countries come from other EU Member States. The EU, as a whole, according to these trade values imports 5.3% of its Cybersecurity products and services from outside of the EU. It should however be noted here that both non-EU-originating Cybersecurity products and services suppliers, and global or international suppliers with operational offices in Europe will likely not be counted as imports⁸. This is considered later in Section 0.

The value of Imports and import intensity (imports as a percentage of the domestic market) can be used to analyse current EU market share of international country markets. EU competitiveness compared with USA and China and can also be used to estimate international (as opposed to domestic and EU) market opportunity. This specific analysis of national imports (outside of the EU), linked with current EU export performance can be seen as the basis for EU competitive performance. This is considered further in Chapter 0.

The percentage of imports into each Member State from within the EU (as opposed to outside the EU) varies significantly by country, from 17% for the UK through to 53% for France (2016 figures). Member States on average import 30% of products/ services from other EU countries and 70% from outside the EU: their EU imports range from 20% for Encryption and Outsourced/ Managed Services through to 32% for Situational Awareness and System Recovery and Data Cleansing.

While the overall assumption in many cases is that most of the European Cybersecurity Industry Market is saturated by non-European product and services, based upon the actual market data, this should be considered an overstatement⁹. The total of over EUR 8 billion in imports is still significant.

Given the differences between the Member States in imports (e.g. France spending more in imports from within the EU, compared to Denmark mostly importing from outside the EU), some specific policies and recommendations can be suggested at least at Member State level.

EU Cybersecurity Exports

Cybersecurity exports are a measure of the products and services that leave the EU for countries outside of its geographic borders. In this section exports are analysed by: EU and Non- EU country; Cybersecurity product and service and destination market (within and without the EU).

⁸ This CIMA – Cybersecurity Industry Market Analysis-study is based upon actual trade data between supply and demand. The numbers reflect the values and the contents (types of products and services along the earlier presented categories) of the transactions that take place in Europe and the rest of the world, and where the income is being accounted for. Companies such as McAfee, Checkpoint and others having local representative subsidiaries, will in most cases be collecting sales revenues in their European offices. As a result, these sales will be accounted for in Europe. Many of these companies, and even more companies such as IBM, PwC, Accenture are international companies with both R&D facilities, employees and engineering and other staff in Europe. Some of these companies provide services to their non-European headquarters, which equally be accounted for in Europe. These setups make it quite hard to distinguish European from non-European companies, and their actual contribution to the European Cybersecurity Industry.

⁹ Taking into consideration the way the actual market data has been accounted for, in this case on the basis of actual sales between companies in Europe and between Europe and outside of Europe.

1.1.30 Key Learnings

The total EU export amounts to EUR 9.7 billion (versus the EUR 12.1 billion in imports). Export to non-EU countries amounts to EUR 6.1 billion (versus EUR 8.5 billion in import). The EU is a net importer of Cybersecurity products and services, with a net trade difference of EUR 2.4 billion. There are however trade differences between the various Member States. Most significant EU export Member States are Germany, UK, France and Italy. Slovakia and the UK are the Member States with the lowest proportion of exports to other EU countries as a proportion of their total exports. Relatively, Croatia is exporting most as a proportion of its total Cybersecurity Market size. Major contributors such as Germany (9.5%), UK (7.4%), France (5.8%) and Italy (5.7%) together contribute for nearly EUR 8 billion in exports. Both Outsourced / Managed Services, Cyber Insurance (74.5%) and Encryption (74%) are relatively the most exported types of products and services outside of the EU. Both Situational Awareness and System Recovery contribute to over EUR 3 billion in exports.

1.1.31 Analysis

Global exports for 2016 are estimated at EUR 48,000 million (obviously the same value as global imports), of which the EU exported EUR 9,718 million or 20% of the total. This make the EU a net importer of Cybersecurity products and services.

Figure 37 : Top Global Exporting Nations 2016 (m EUR) ranks the top 12 global exporters, with China the leading Cybersecurity exporter at EUR 14,287 million. Four EU countries- Germany, UK, France and Italy- are within the top 12.

Figure 37 : Top Global Exporting Nations 2016 (m EUR)

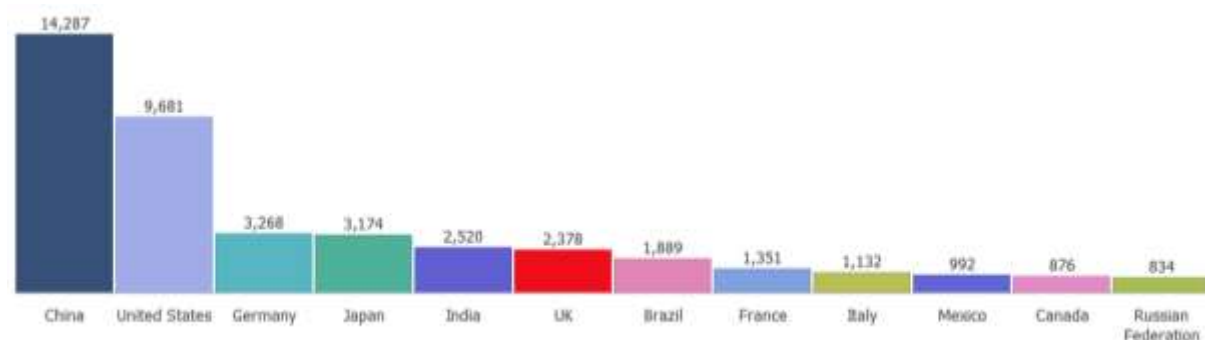


Table 24 : EU Exports by Country shows EU exports divided into exports within the EU and outside of the EU. The overall values of Non- EU exports is EUR 6,126 million or 63%, with 37% of exports between EU countries. The highest volume exporters are Germany, UK, France and Italy.

Table 24 : EU Exports by Country alphabetically and by Non-EU % export

Country	Exports	Exports EU	EU %	Exports Non- EU	Non- EU %	Country	Exports	Exports EU	EU %	Exports Non- EU	Non- EU %
Austria	218.2	98.3	45.1	119.8	54.9	Slovakia	56.0	7.0	12.5	49.0	87.5
Belgium	224.0	117.5	52.5	106.5	47.5	UK	2,377.5	441.7	18.6	1,935.9	81.4
Bulgaria	67.0	26.5	39.6	40.5	60.4	Croatia	47.0	9.9	21.1	37.1	78.9
Croatia	47.0	9.9	21.1	37.1	78.9	Cyprus	13.1	3.0	22.9	10.1	77.1
Cyprus	13.1	3.0	22.9	10.1	77.1	Ireland	106.3	25.5	24.0	80.8	76.0
Czech Republic	29.0	14.5	50.0	14.4	49.7	Slovenia	32.9	7.9	24.0	24.9	75.7
Denmark	32.5	14.5	44.6	18.0	55.4	Luxembourg	23.0	5.6	24.3	17.4	75.7
Estonia	25.7	14.9	58.0	10.8	42.0	Greece	70.7	21.1	29.8	49.6	70.2
Finland	35.2	12.6	35.8	22.6	64.2	Finland	35.2	12.6	35.8	22.6	64.2
France	1,350.8	690.2	51.1	660.6	48.9	Germany	3,267.6	1,267.5	38.8	2,000.1	61.2
Germany	3,267.6	1,267.5	38.8	2,000.1	61.2	Bulgaria	67.0	26.5	39.6	40.5	60.4
Greece	70.7	21.1	29.8	49.6	70.2	Italy	1,132.0	486.9	43.0	645.1	57.0
Hungary	12.9	7.7	59.7	5.2	40.3	Lithuania	20.7	8.9	43.0	11.7	56.5
Ireland	106.3	25.5	24.0	80.8	76.0	Denmark	32.5	14.5	44.6	18.0	55.4
Italy	1,132.0	486.9	43.0	645.1	57.0	Austria	218.2	98.3	45.1	119.8	54.9
Latvia	36.0	17.9	49.7	18.0	50.0	Poland	85.8	40.9	47.7	44.9	52.3
Lithuania	20.7	8.9	43.0	11.7	56.5	Sweden	30.6	14.9	48.7	15.7	51.3
Luxembourg	23.0	5.6	24.3	17.4	75.7	Latvia	36.0	17.9	49.7	18.0	50.0
Malta	5.1	4.1	80.4	1.0	19.6	Czech Republic	29.0	14.5	50.0	14.4	49.7
Netherlands	107.0	63.3	59.2	43.7	40.8	France	1,350.8	690.2	51.1	660.6	48.9
Poland	85.8	40.9	47.7	44.9	52.3	Belgium	224.0	117.5	52.5	106.5	47.5
Portugal	14.6	8.9	61.0	5.7	39.0	Spain	290.7	155.0	53.3	135.7	46.7
Romania	6.0	4.5	75.0	1.5	25.0	Estonia	25.7	14.9	58.0	10.8	42.0
Slovakia	56.0	7.0	12.5	49.0	87.5	Netherlands	107.0	63.3	59.2	43.7	40.8
Slovenia	32.9	7.9	24.0	24.9	75.7	Hungary	12.9	7.7	59.7	5.2	40.3
Spain	290.7	155.0	53.3	135.7	46.7	Portugal	14.6	8.9	61.0	5.7	39.0
Sweden	30.6	14.9	48.7	15.7	51.3	Romania	6.0	4.5	75.0	1.5	25.0
UK	2,377.5	441.7	18.6	1,935.9	81.4	Malta	5.1	4.1	80.4	1.0	19.6
Total	9,717.9	3,591.2	37.0	6,126.3	63.0	Total	9,717.9	3,591.2	37.0	6,126.3	63.0

The percentage of exports to the EU varies by country (see Figure 38). For the UK it is as low as 19%, while for Hungary, Malta, Netherlands, Portugal and Romania it is 60% or above.

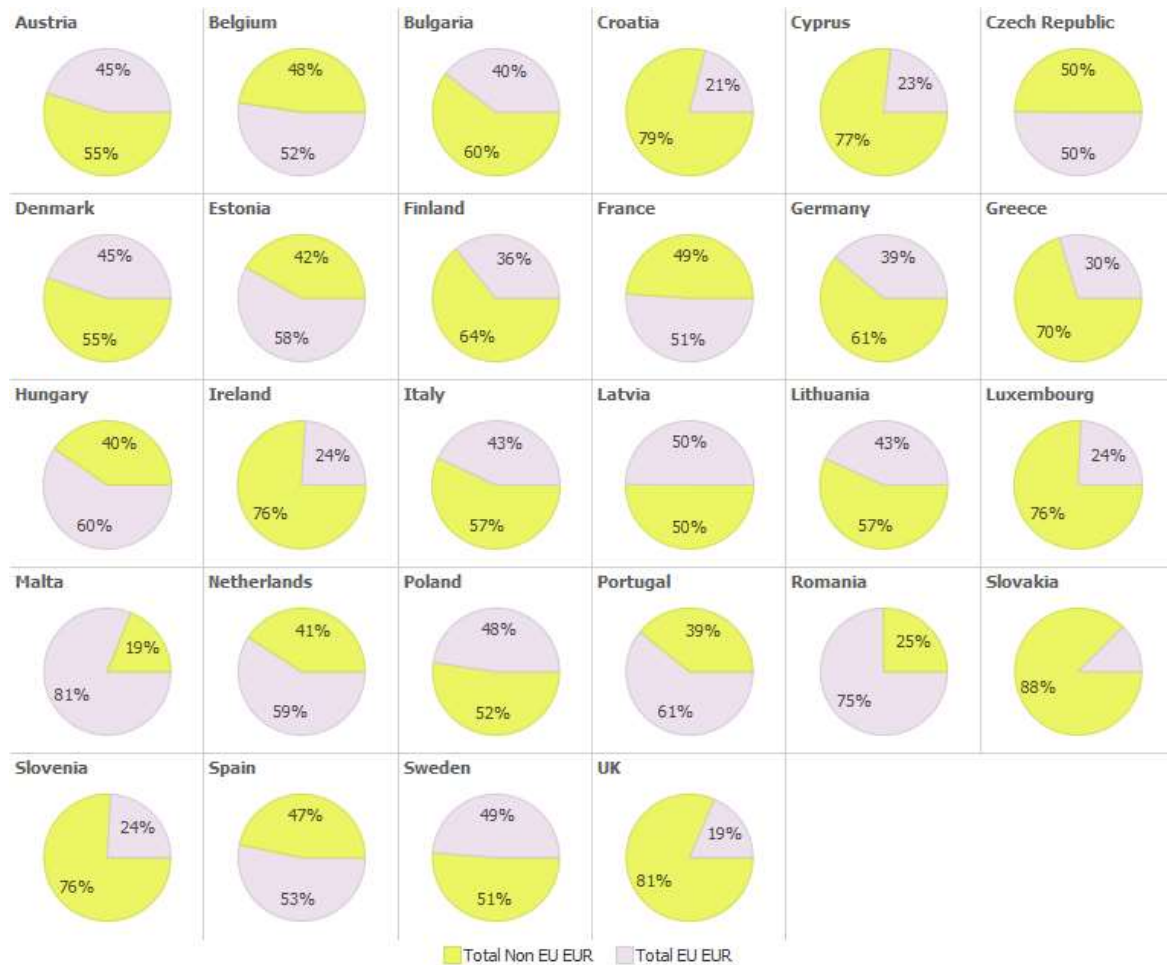
The countries with the highest percentage of exports to other EU countries are:

- Malta 80%
- Romania 75%
- Portugal 61%
- Hungary and Netherlands 59%
- Estonia 58%
- Spain 53%.

The countries with the lowest percentage of exports to other EU countries are:

- Slovakia 12%
- UK 19%
- Croatia 21%
- Cyprus 23%

Figure 38 : EU Country Exports to EU and Non- EU Countries 2016

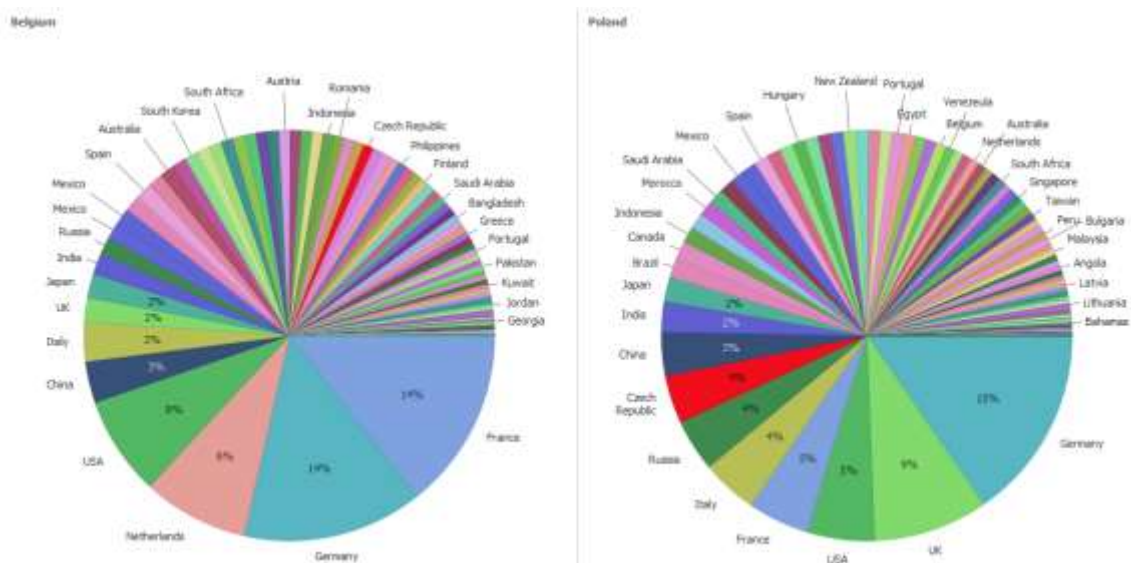


Looking at the possible implications of Brexit, the UK domestic demand of EUR 30,522 million is significant compared to EU-27 domestic demand of EUR 129,828 million (taken from Table 24), showing the benefits that could be available from lowering regulatory and other barriers between the UK and the EU-27 countries in this domain. Key points are:

- At present UK exports to the EU-27 are EUR 441.7 million (2016 figures) which meets a small share, 0.3%, of the EU-27 domestic demand of EUR 129,828 million.
- EU-27 exports to the UK are EUR 153.6 million (2016 figures) compared to EU-27 exports to other non-EU-27 countries of EUR 4,190.4 million: EU-27 exports to the UK are a significant but not large share, 3.5%, of the EU-27 exports to all non-EU-27 countries.
- If one looks at EU-27 Exports compared to Sales (i.e. taking out UK Sales and UK Exports) the EU-27 export intensity of exports compared to sales drops from the EU-28 level of 3.9% to 3.4%, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China (Table 29). EU-27 exporting activity without the UK is even lower than competitors relative to the sales activities delivered from within its borders.

The individual country level (as previously for imports in Figure 38 : EU Country Exports to EU and Non- EU Countries 2016) can be broken down for exports in more detail. In Figure 39 : EU and Non- EU Exports for Belgium and Poland, two examples are compared using the originating countries for imports.

Figure 39 : EU and Non- EU Exports for Belgium and Poland



Belgium and Poland experience similar export percentages to Germany (14-15%) and to China (3%) but the similarities end there. The top export markets for Belgium are France, Germany, Netherlands and the USA, while for Poland they are Germany, UK, USA and France. There are similarities in the leading export markets for the two countries, but significant differences in the ranking and the proportion of exports. As with imports, this analysis suggests that very different trading patterns exist within the EU. Similar analysis for each EU country, resulting in complex patterns of inter- trading within the EU is reported in Section O. At the EU-country level the percentage of exports by country vary enormously as shown by the following list of the top two export destinations for selected countries:

- Austria Germany and USA
- Bulgaria Russia and China
- Czech Republic Germany and UK
- Estonia Sweden and Finland
- Finland USA and UK
- France Germany and Italy
- Germany France and USA
- Italy Germany and France
- Latvia Russia and Lithuania
- Lithuania Russia and Latvia
- Netherlands Germany and Belgium
- Portugal UK and Spain
- Spain France and Portugal
- UK USA and China.

Exports can also be analysed by sub-sector. Table 25 : EU Exports by Sub-sector 2016 demonstrates that EU exports (average 37%) vary between 21% for Cyber Consultancy, Infrastructure and Outsourced/ Managed Services and 42% for Application Security and System Recovery & Data Cleansing.

The value of exports, as a means of measuring competitive performance has been conducted more intensively (by country and by more detailed analysis of Cybersecurity products and services) in **Appendix D : Exports by Country of Origin per EU Member State.**

Assessment of the intensity of exports by EU Member State by calculating a simple proxy measure- exports as a percentage of country sales are presented in Table 25 : EU Exports by Sub-sector 2016, which compares sales and imports for each country. The ratio of exports to sales is 6.2% for all of the EU, but ranges between 1-14% for individual countries.

Table 25 : EU Exports by Sub-sector 2016

Sub Sector	All Exports EURM	EU Exports EURM	EU % of Exports EURM	Non- EU Exports EURM	Non- EU % of Exports EURM
Anti Malware	369	135	36.5	234	63.5
Application Security	711	300	42.1	412	57.9
Business Continuity	469	164	35.1	304	64.9
Cyber Consultancy	287	90	31.3	197	68.7
Cyber Security Insurance	458	117	25.5	341	74.5
Encryption	195	51	26.0	144	74.0
Identity & Access	695	193	27.7	502	72.3
Infrastructure	945	308	32.6	637	67.4
Mobile	290	115	39.8	175	60.2
Outsourced/Managed Services	201	51	25.5	150	74.5
Situational Awareness	2,733	1,084	39.7	1,649	60.3
System Recovery & Data Cleansing	2,336	972	41.6	1,364	58.4
Training & Education	30	12	40.6	18	59.4
Total	9,718	3,591	37.0	6,126	63.0

Table 26 : EU Exports 2016 by Country – Exports vs Sales in (m EUR) – alphabetically and Exports as % of Sales

Country	Sales EURM	Exports EURM	Exports as % of Sales	Country	Sales EURM	Exports EURM	Exports as % of Sales
Austria	3.261	218	6.7	Croatia	337	47	13.9
Belgium	4.542	224	4.9	Estonia	263	26	9.8
Bulgaria	753	67	8.9	Germany	34.261	3.268	9.5
Croatia	337	47	13.9	Latvia	384	36	9.4
Cyprus	188	13	7.0	Bulgaria	753	67	8.9
Czech Republic	1.198	29	2.4	UK	31.950	2.378	7.4
Denmark	2.076	33	1.6	Cyprus	188	13	7.0
Estonia	263	26	9.8	Slovenia	476	33	6.9
Finland	1.864	35	1.9	Austria	3.261	218	6.7
France	23.302	1.351	5.8	Luxembourg	349	23	6.6
Germany	34.261	3.268	9.5	Lithuania	316	21	6.5
Greece	1.546	71	4.6	Ireland	1.696	106	6.3
Hungary	1.022	13	1.3	France	23.302	1.351	5.8
Ireland	1.696	106	6.3	Italy	19.910	1.132	5.7
Italy	19.910	1.132	5.7	Malta	98	5	5.2
Latvia	384	36	9.4	Slovakia	1.109	56	5.0
Lithuania	316	21	6.5	Belgium	4.542	224	4.9
Luxembourg	349	23	6.6	Greece	1.546	71	4.6
Malta	98	5	5.2	Poland	3.040	86	2.8
Netherlands	6.485	107	1.6	Spain	11.943	291	2.4
Poland	3.040	86	2.8	Czech Republic	1.198	29	2.4
Portugal	1.180	15	1.2	Finland	1.864	35	1.9
Romania	1.140	6	0.5	Netherlands	6.485	107	1.6
Slovakia	1.109	56	5.0	Denmark	2.076	33	1.6
Slovenia	476	33	6.9	Hungary	1.022	13	1.3
Spain	11.943	291	2.4	Portugal	1.180	15	1.2
Sweden	3.283	31	0.9	Sweden	3.283	31	0.9
UK	31.950	2.378	7.4	Romania	1.140	6	0.5
Total	157.973	9.718	6.2	Total	157.973	9.718	6.2

The countries with the highest proportion of exports to sales are:

- Croatia 14%
- Estonia and Germany 10%
- Latvia and Bulgaria 9%, and
- UK, Cyprus, Austria and Slovenia 7%.

The countries with the lowest proportion of exports to sales are:

- Romania, Hungary and Sweden 1%, and
- Denmark, Netherlands, Finland, Spain and Czech Republic 2%.

1.1.32 Conclusions and Recommendations

The EU Member States with the highest export intensity (proportion of exports to sales generated within their borders) are Croatia (14%), Estonia and Germany (10%), Latvia and Bulgaria (9%), and the UK, Cyprus, Austria and Slovenia (7%). The countries with the lowest proportions of exports to sales are Romania, Hungary and Sweden (1%), and Denmark, Netherlands, Finland, Spain and Czech Republic (2%).

The importance of the UK in this analysis should be noted. The trade deficit on the Cybersecurity Industry will drop significantly, as a result of Brexit. However, the UK is not contributing significantly to importing from the EU markets. UK is a significant player on the export market, as it contributes to nearly EUR 2.4 billion of the total of EUR 9.7 billion in exports (81% of it for outside the EU).

EU Competitiveness

Introduction

In Sections 0 and 0 of this report, EU imports and exports were calculated by country and by sub-sector of Cybersecurity for 2016. In Chapter 0 the previous metrics from Chapter 0 (including international inter- trading) are drawn together to review EU competitiveness. This analysis is based upon a series of data dashboards included at **Appendix D : Exports by Country of Origin per EU Member State**. The dashboards include the EU 28, EU 27, individual EU Member States and key competing nations- USA, China, Japan and India (based upon size of Cybersecurity sales). The value for the Cybersecurity sector in this report is higher than in most (not all) other research reports because the search for evidence covers a very broad base which allows the accommodation of national variations in definition without losing the ability to compare results across multiple continents or countries.

Trade Flow Analysis

1.1.33 Key Learnings

In terms of exports, EU is lagging behind in Cybersecurity exports in comparison to the 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. The EU is a net importer for all products and services apart from Cyber Insurances. All other global markets import all activities. The EU and the four nations are all competing fiercely for share of exports in Situational Awareness and System Recovery & Data Cleansing and to a lesser degree in Infrastructure, Identity & Access and Application Security.

1.1.34 Analysis

Figure 40 : Trade Flows for EU (m EUR) 2016 shows trade flows for the EU 28, with sales, imports and exports and the domestic market (calculated by sales+ imports – exports). The EU 28 market is EUR 160,351 million and shows that the EU is a net importer of Cybersecurity solutions¹⁰. This is not true of all Member States as Germany, France, UK, Italy, Croatia, Ireland, Luxembourg, Slovakia and Slovenia are all net exporters (see **Appendix D : Exports by Country of Origin per EU Member State**). The gap between imports and exports is higher for the EU 27, when the UK export performance is excluded.

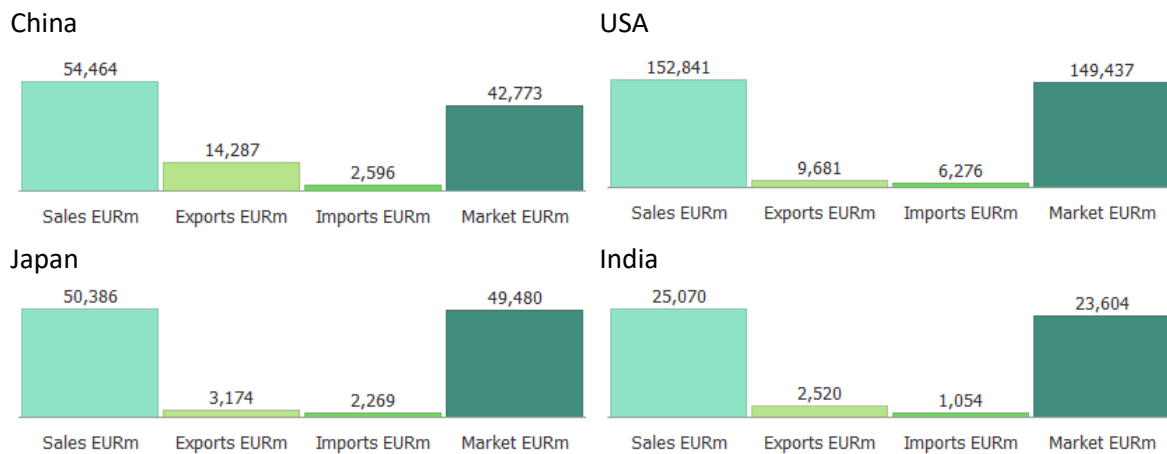
¹⁰ These import figures represent trade-flows into the EU from external suppliers. Sales from companies with operations in Europe, but which may have Headquarters outside the EU, are not counted as imports, as described in Section 0.

Figure 40 : Trade Flows for EU (m EUR) 2016



In comparison with the EU, the four leading competing nations- USA, China, Japan and India- are all net exporters (see Figure 37 and Figure 41), with China showing the greatest absolute difference between exports and imports and the lowest ratio of imports to exports.

Figure 41 : Trade Flows for Top Four Competing Nations (m EUR) 2016

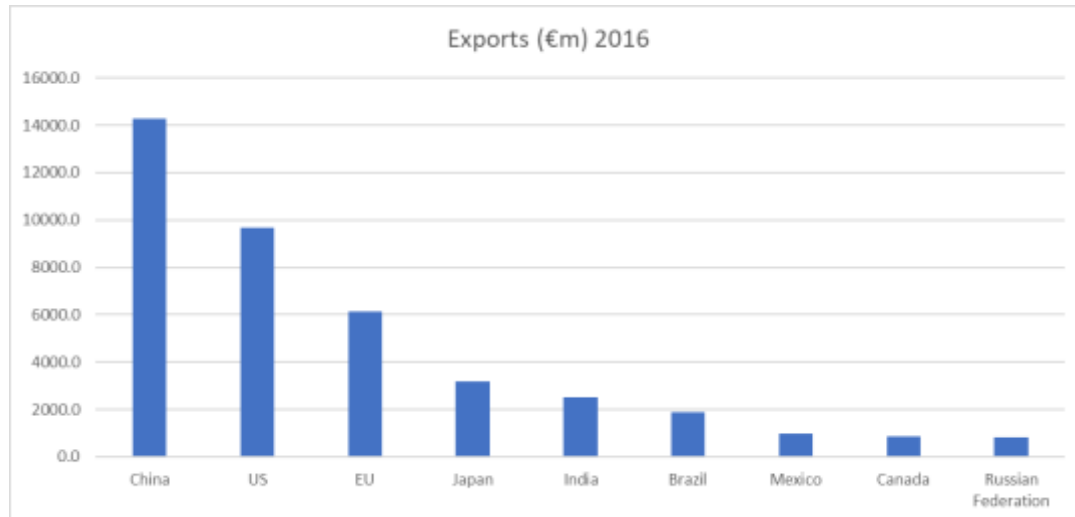


The following Table and Figure compares EU exports with other competing regions in 2016:

Table 27 : Comparison of EU and competitor region/ country Exports

Region/ Country	Exports (€m) 2016 (1)
China	14287.0
US	9681.0
EU	6126.3
Japan	3174.0
India	2520.0
Brazil	1889.0
Mexico	992.0
Canada	876.0
Russian Federation	834.0
1) Table 16: EU Exports by Country and Figure 28: Top Global Exporting Nations 2016	

Figure 42 : Comparison of EU and competitor region/ country Exports

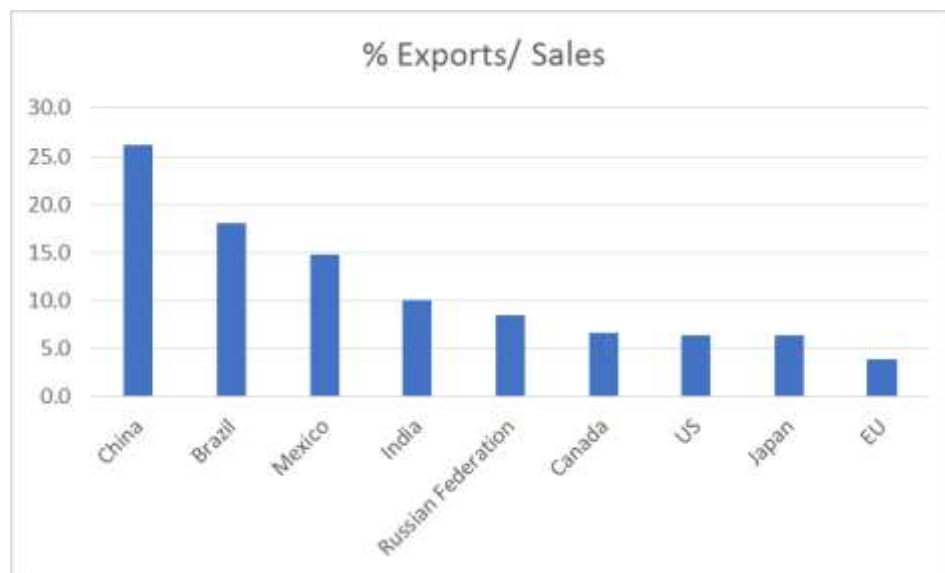


If one compares EU and competitor region/ country exports to sales activities delivered by companies within their borders, one gets a measure of their export intensity (exports over sales). See Table 28 : Comparison of EU and competitor region/ country Exports relative to their Sales and Figure 43 : Comparison of EU and competitor region/ country Exports relative to their Sales

Table 28 : Comparison of EU and competitor region/ country Exports relative to their Sales

Region/ Country	% Exports/ Sales	Exports (€m) 2016	Sales (€m) 2016
China	26.2	14287.0	54464.2
Brazil	18.1	1889.0	10436.2
Mexico	14.8	992.0	6722
India	10.1	2520.0	25070.2
Russian Federation	8.5	834.0	9783.3
Canada	6.6	876.0	13189.8
US	6.3	9681.0	152841
Japan	6.3	3174.0	50386
EU	3.9	6126.3	157973

Figure 43 : Comparison of EU and competitor region/ country Exports relative to their Sales



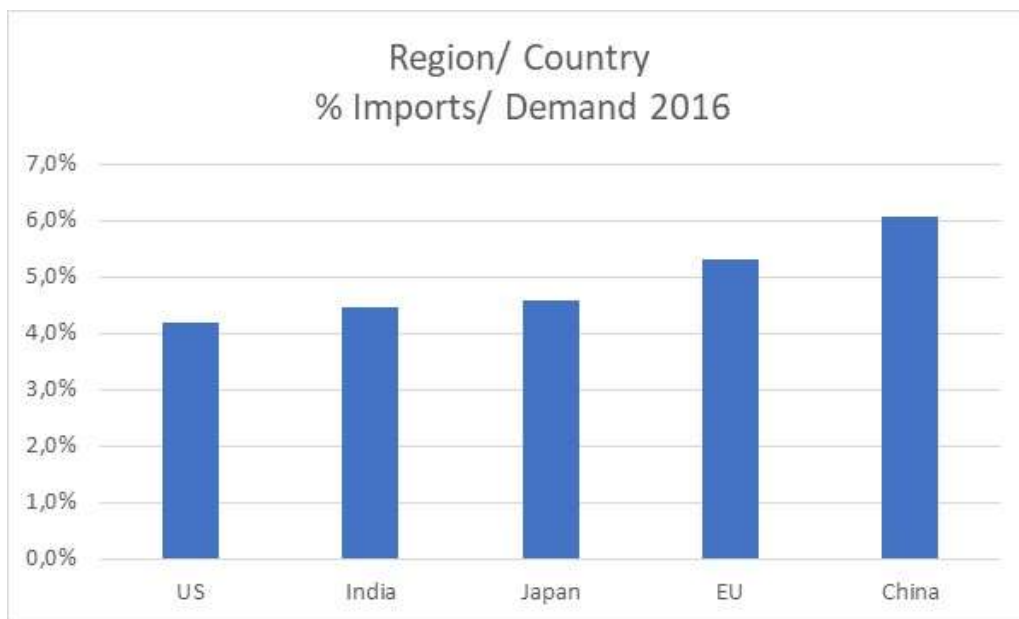
The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective.

Similarly, by comparing region/country domestic demand with imports it is possible to analyse to what extent the EU and other competing regions/ countries meets their Cybersecurity needs by imports rather than from internal suppliers. The following Table and Figure shows imports as a share of domestic demand for the EU and the top 4 competing regions/ countries, with the US importing 4.2% of its domestic demand, India 4.5%, Japan 4.6%, the EU 5.3% and China having the highest imports as a share of domestic demand at 6.1%.

Table 29 : Comparison of EU and top competitor region/ country Imports relative to their domestic demand

Region/ Country	Region/ Country % Imports/ Demand 2016	Domestic Demand (€m) 2016	Imports (€m) 2016 (3,4)	Sales (€m) 2016 (2)	Exports (€m) 2016 (1)
US	4.2%	149436.0	6276	152841	9681.0
India	4.5%	23604.2	1054	25070.2	2520.0
Japan	4.6%	49481.0	2269	50386	3174.0
EU	5.3%	160386.9	8540.2	157973	6126.3
China	6.1%	42773.2	2596	54464.2	14287.0

Figure 44 : Comparison of EU and competitor region/ country Imports relative to their domestic demand



Trade flows for the EU and the four competing nations at the sub-sector level are included in **Appendix E : Competitive Dashboards** and **Appendix F : Trade Flows by Sub-sector**. This analysis shows that:

- The EU 28 is a net importer for all sub-sectors of Cybersecurity, except for Cyber Insurance. The greatest disparities between imports and exports (over EUR 600 million) are in Situational Awareness and Systems Recovery
- The USA is a net exporter in all sub-sectors
- China is a net exporter in all sub-sectors, but to a lesser degree for Outsourced/ Managed Services and Cyber Consulting
- Japan is a net exporter in all sub-sectors, but to a lesser degree for Situational Awareness, Outsourced/ Managed Services, Infrastructure and Cyber Consulting
- India is a net exporter for all sub-sectors, although the difference between imports and exports is much lower than for the USA, China and Japan.

As a “trading bloc” the EU is, therefore, trailing the performance of the USA, China, Japan and India in the ratio of exports to imports.

In Figure 44 : Comparison of EU and competitor region/ country Imports relative to their domestic demand the sales by sub-sector for the EU 28 shows 21% of sales for Infrastructure and Situational Awareness, 17% for Application Security and 13% for System Recovery & Data Cleansing. The top four sub-sectors account for 72% of all sales.

Figure 45 : EU 28 Sales by Sub-sector (m EUR) 2016

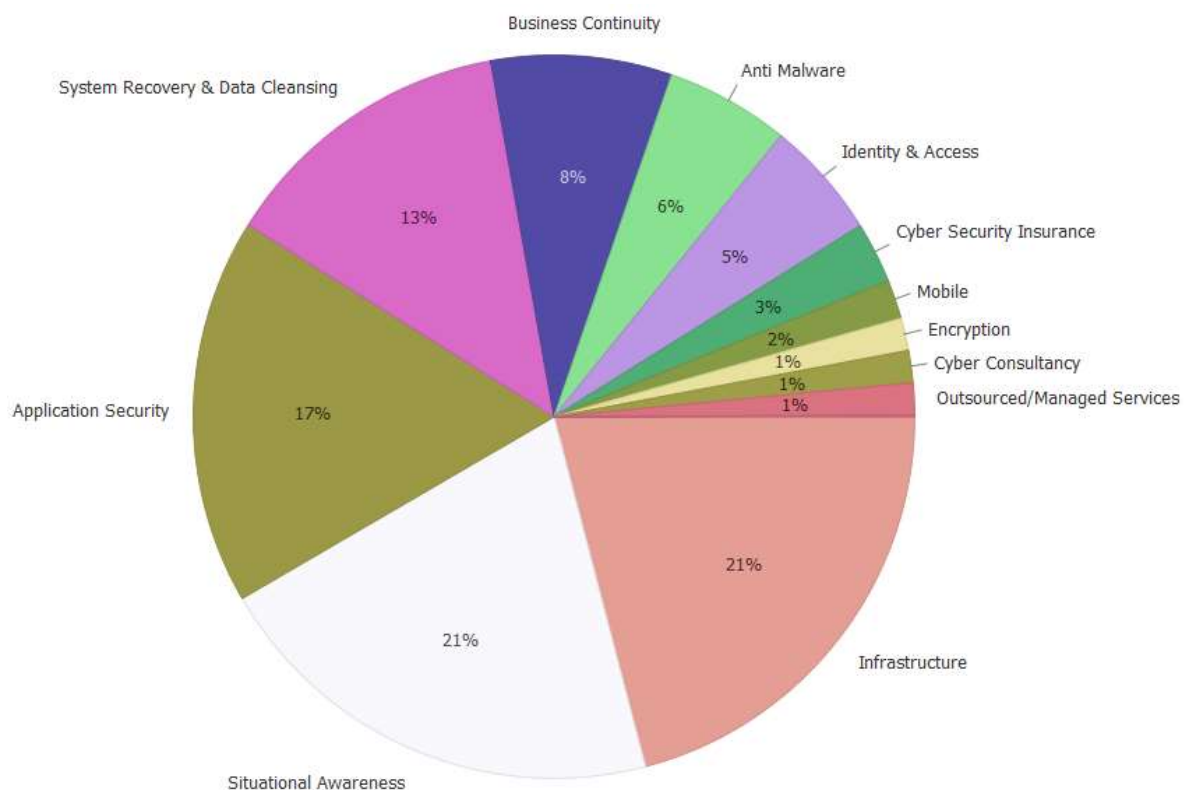


Figure 46 : Competing Nation Sales by Sub-sector (m EUR) 2016 shows the same data, but for the top four competing nations identified above. Each of the four cases differ from each other and also differ from the sales mix for the EU (Figure 45):

- China shows 27% of sales for Situational Awareness, 21% for System Recovery & Data Cleansing, 13% for Infrastructure, 8% for Application Security and 7% for Identity & Access and Business Continuity. The top four sub-sectors account for 69% of all sales.
- India shows 26% of sales for Situational Awareness, 24% for System Recovery & Data Cleansing, 12% for Infrastructure, 9% for Application Security and 8% for Identity & Access. The top four sub-sectors account for 71% of all sales.
- Japan shows 22% of sales for Application Security, 20% for Situational Awareness, 19% for Infrastructure, 11% for System Recovery & Data Cleansing and 10% for Business Continuity. The top four sub-sectors account for 72% of all sales.

- USA shows 20% of sales for Infrastructure and Application Security, 19% for Identity & Access Based Services, 18% for Situational Awareness, 11% for System Recovery & Data Cleansing and 9% for Anti Malware. The top four sub-sectors account for 69% of all sales.

Figure 46 : Competing Nation Sales by Sub-sector (m EUR) 2016



Each country, therefore, experiences slightly different demands and competes based upon different strengths. This is shown just as clearly by analysis of EU export performance in Figure 45 : EU 28 Sales by Sub-sector (m EUR) 2016

In Figure 46 : Competing Nation Sales by Sub-sector (m EUR) 2016 the exports by sub-sector for the EU 28 shows 28% of exports for Situational Awareness, 24% for System Recovery & Data Cleansing, 10% for Infrastructure, 7% for Application Security and Identity & Access. The top five sub-sectors account for 76% of all exports, but show a different ranking and different proportions when compared with sales at Figure 42 : Comparison of EU and competitor region/ country Exports. Exports for Situational Awareness and System Recovery are proportionally much higher and exports for Infrastructure and Application Security are much lower. There is no obvious explanation for this other than company- level successes in overseas markets.

Figure 47: EU 28 Exports by Sub-sector (m EUR) 2016

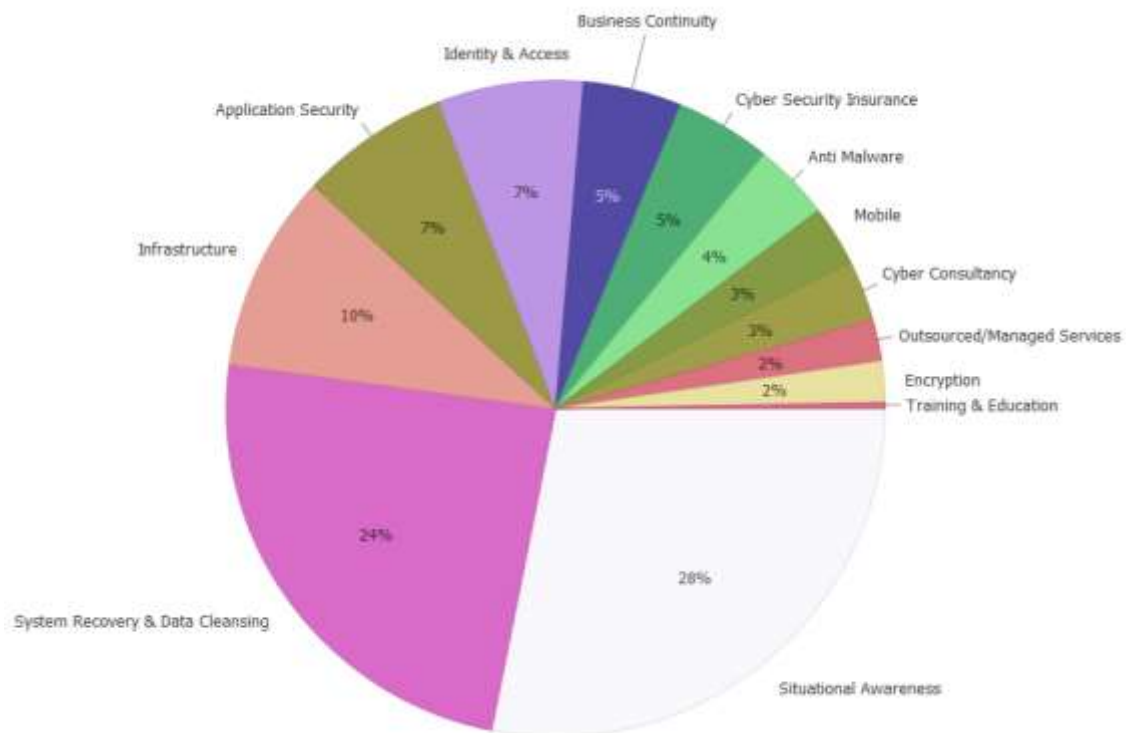


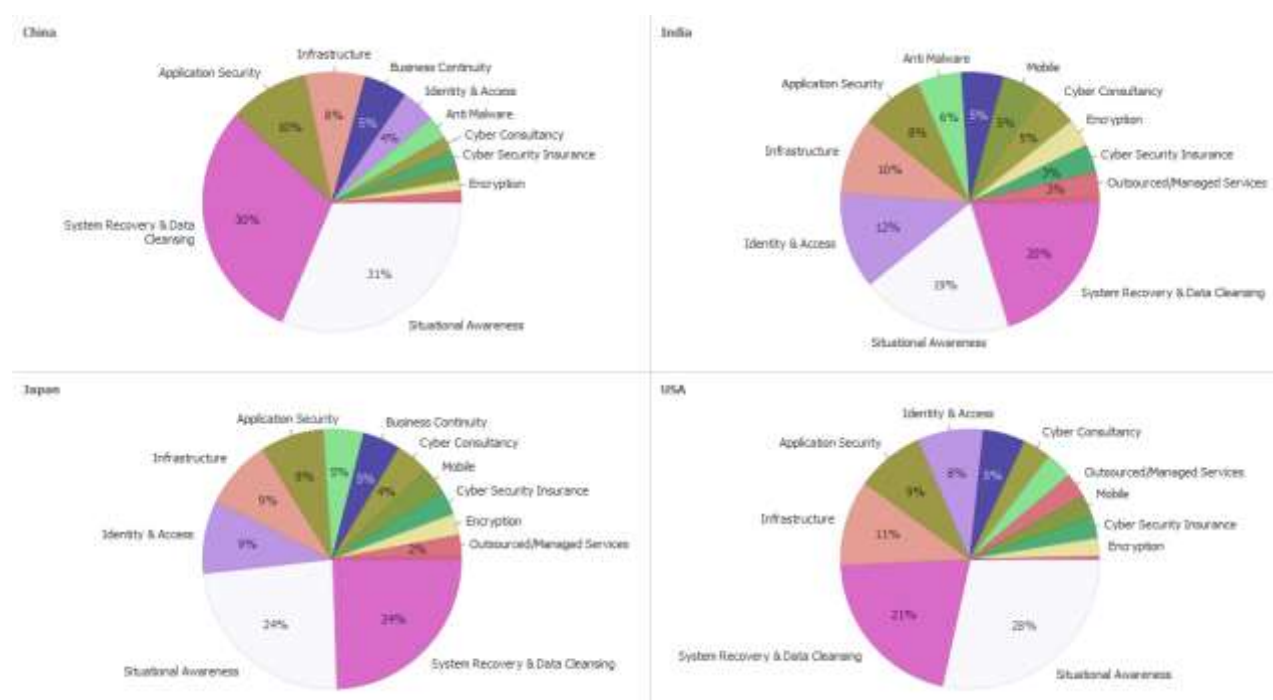
Figure 46 : Competing Nation Sales by Sub-sector (m EUR) 2016 shows the same data, but for the top four competing nations identified above. Each of the four cases once again differ from each other and also differ from the export mix for the EU (Figure 47). Export performance also differs from the sales performance shown at Figure 45 (because sales includes domestic consumption less imports):

- China shows 31% of exports for Situational Awareness, 30% for System Recovery & Data Cleansing, 10% for Application Security, 8% for Infrastructure and 5% for Business Continuity. The top five sub-sectors account for 84% of all exports but show different proportions when compared with sales at Figure 46. Exports for Situational Awareness, System Recovery and Application Security are proportionally higher and exports for Infrastructure and Business Continuity are lower.
- India shows 20% of exports for System Recovery & Data Cleansing, 19% for Situational Awareness, 12% for Identity & Access, 10% for Infrastructure and 8% for Application Security. The top five sub-sectors account for a much lower 69% of all exports (compared with the EU and China) and show similar rankings but different proportions when compared with sales at Figure 46. Exports for Situational Awareness, System Recovery, Infrastructure and Application Security are proportionally lower, while exports for Identity & Access are higher.
- Japan shows 24% of exports for System Recovery & Data Cleansing, 24% for Situational Awareness, 9% for Infrastructure, 9% for Identity & Access and 8% for Application Security. The top five sub-sectors account for a much lower 74% of all exports (compared with the EU and China) and show different rankings and different proportions when compared with sales at Figure 46. Exports for System Recovery and Identity & Access are proportionally higher, while exports for Situational Awareness, Infrastructure and Application Security are lower.
- USA shows 28% of exports for Situational Awareness, 21% for System Recovery & Data Cleansing, 20%, 11% for Infrastructure, 9% for Application Security and 8% for Identity & Access. The top five sub-sectors account for 77% of all exports and show different rankings

and different proportions when compared with sales at Figure 46. Exports for Situational Awareness, System Recovery and Identity & Access are proportionally higher, while exports for Infrastructure and Application Security are much lower.

This analysis confirms that the EU and the four nations are all competing fiercely for share of exports in Situational Awareness and System Recovery & Data Cleansing and to a lesser degree in Infrastructure, Identity & Access and Application Security.

Figure 48 : Competing Nation Exports by Sub-sector (m EUR) 2016



1.1.35 Conclusions and Recommendations

The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. **EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective.**

Similarly, by comparing region/country domestic demand with imports it is possible to analyse to what extent the EU and other competing regions/ countries meet their Cybersecurity needs by imports rather than from internal suppliers. The US imports 4.2% of its domestic demand, India 4.5%, Japan 4.6%, the EU 5.3% and China 6.1%. China has the highest imports as a share of domestic demand followed by the EU.

There appears to be added value from certification making sales and especially exports easier, and raising user awareness and confidence. However, there are potential negative effects related to the time and cost of approvals. For example, the existing common criteria take a very long time to get certified, and are only affordable for large players. In the UK, the cost (from EUR 50,000 to EUR 500,000) for national approvals is prohibitive and stifles innovation. Getting separate MS testing and approval to sell across Europe is a big burden, especially for SMEs.

Focus group participants generally agreed that there was a need for EU-wide Cybersecurity product standards that apply in all MS. **Agreement on ‘what is good in a Cybersecurity product’, the equivalent of an EU ‘crash test’ (like Euro NCAP for cars) for Cybersecurity products and services, could allow countries to run their own schemes built on a common agreement.** National-only standards are not useful to exporters, hindering inter-MS trading, and could be thought of as anti-competitive.

Concerns were raised in the Workshops about differences between MS on certification and it was felt that the EU can play a role in harmonising standards. **The EC should develop a single set of approval criteria for Cybersecurity products and services that applies across EU MS.** It was also felt that if there was such a set of common standards then there would be a reasonable chance of getting agreement with the US.

Market Share Analysis

In the final section of this report the emphasis is on comparative performance (market share) in exports. The research mapped the flow of imports and exports between major trading nations (including all member States of the EU) and compared all exports as a proportion of all country imports. For example, Cybersecurity imports into the USA were EUR 6,276 million from all major trading sources. This is represented by the size of the grey bar on Figure 49 : Share of Import Market for Major Global Trading Nations (non- EU) 2016. The size of imports received from the EU, China and Japan are then shown as a value on the line plot for each major source of imports.

1.1.36 Key Learnings

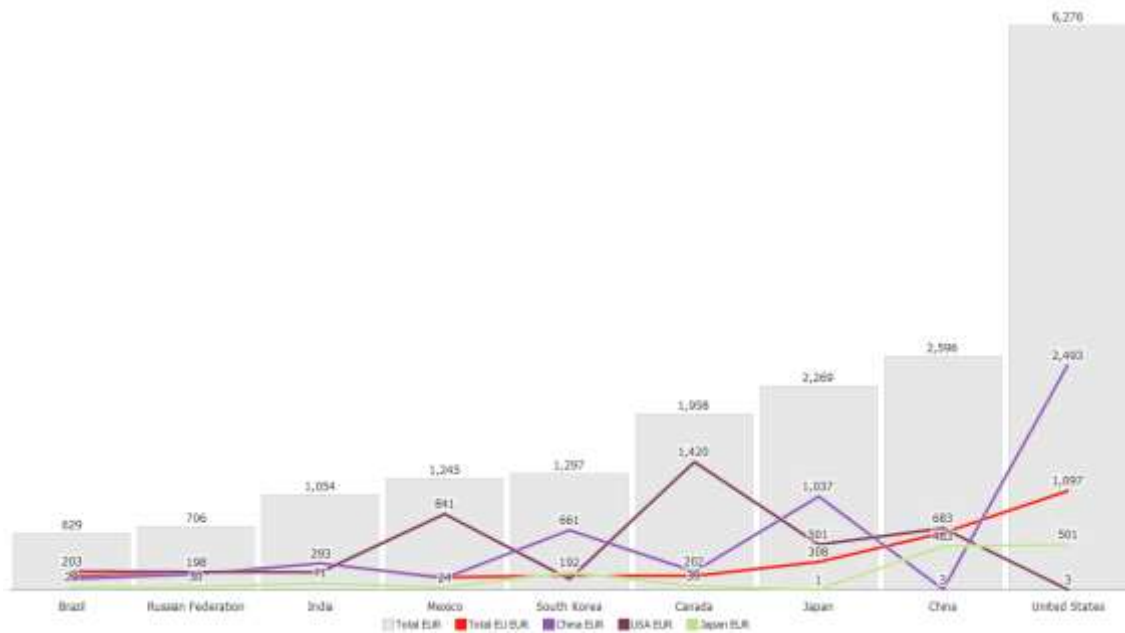
The most important trading nations for Cybersecurity for EU are China, USA and Japan. There is no single market where EU Cybersecurity products and services are the key market exports (like China and USA). On a global competing scale, EU is lagging behind the US as the main contributor to Cybersecurity products and services.¹¹ In the EU, China is the largest competitor. There is a lot of variation in import preferences across the EU.

1.1.37 Analysis

In Figure 49 : Share of Import Market for Major Global Trading Nations (non- EU) 2016 the chart includes the USA, China, Japan, South Korea, Mexico, India, Russian Federation and Brazil as “import markets” and the EU, USA, China and Japan as the major sources of imports. All values are in million EUR.

¹¹ US-originating, and non-European-originating companies operating in the EU (e.g. IBM quoted before) are counted as "European", due to the fact that their European trade organizations collect actual sales within Europe. This has been reported extensively in the Methodology (Chapter 0 – Research Methodology), and in previous remarks, as there is no distinctive way to identify European from non-European companies.

Figure 49 : Share of Import Market for Major Global Trading Nations (non- EU) 2016



- USA with 26% of China imports, 22% of Japanese imports and 73% of Canadian exports
- China with 40% of USA imports, 46% of Japanese imports and 10% of Canadian imports.

These results reinforce previous analysis, that EU nations (excluding the UK) are much more likely to trade with each other and that share of non- EU markets is correspondingly less. The influence of other “trading blocs” i.e. North America (USA, Canada and Mexico) and Asia (China, Japan, South Korea) on imports is also reinforced by this analysis.

Using the same conventions but different destination countries, Figure 49 : Share of Import Market for Major Global Trading Nations (non- EU) 2016 focuses on Cybersecurity imports into the main trading countries of the EU- Germany, UK, France, Italy, Netherlands, Austria, Spain, Belgium and Sweden.

In Figure 50 : Share of Import Market for Major EU Trading Nations 2016, the EU contributes to 32% of Germany imports, 53% of French imports, 42% of Italian imports and 17% of UK imports. This compares with:

- China with 25% of Germany imports, 10% of French imports, 17% of Italian imports and 17% of UK imports.
- USA with 23% of Germany imports, 18% of French imports, 16% of Italian imports and 25% of UK imports
- Japan with 3% of Germany imports, 4% of French imports, 5% of Italian imports and 7% of UK imports.

In all of the selected cases, except for the UK (USA) and Sweden (China), the EU is (as expected) the main source of imports into each Member State.

Figure 50 : Share of Import Market for Major EU Trading Nations 2016

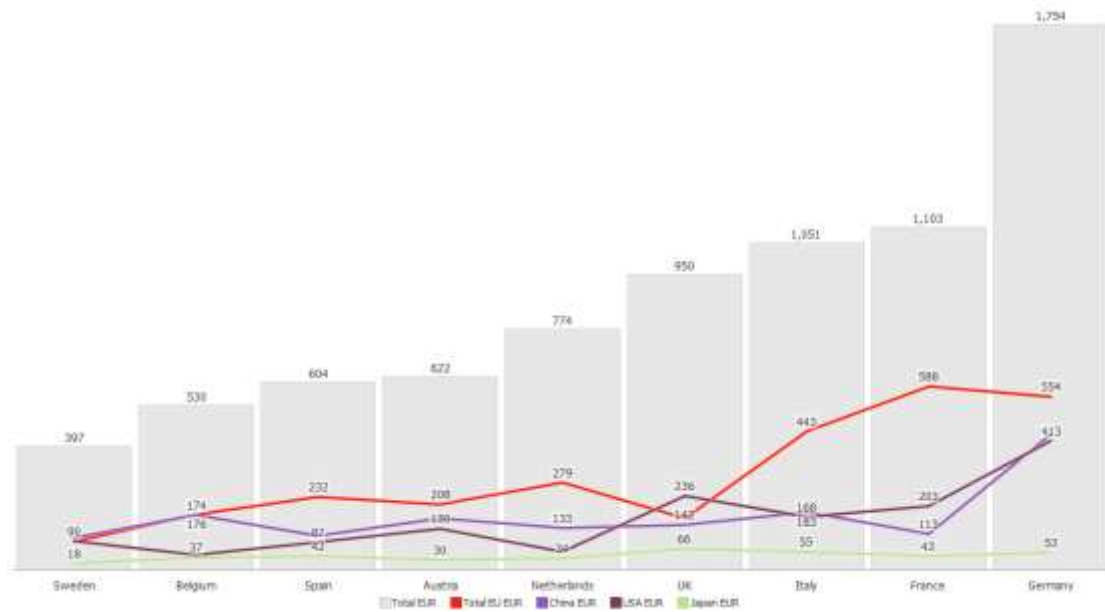
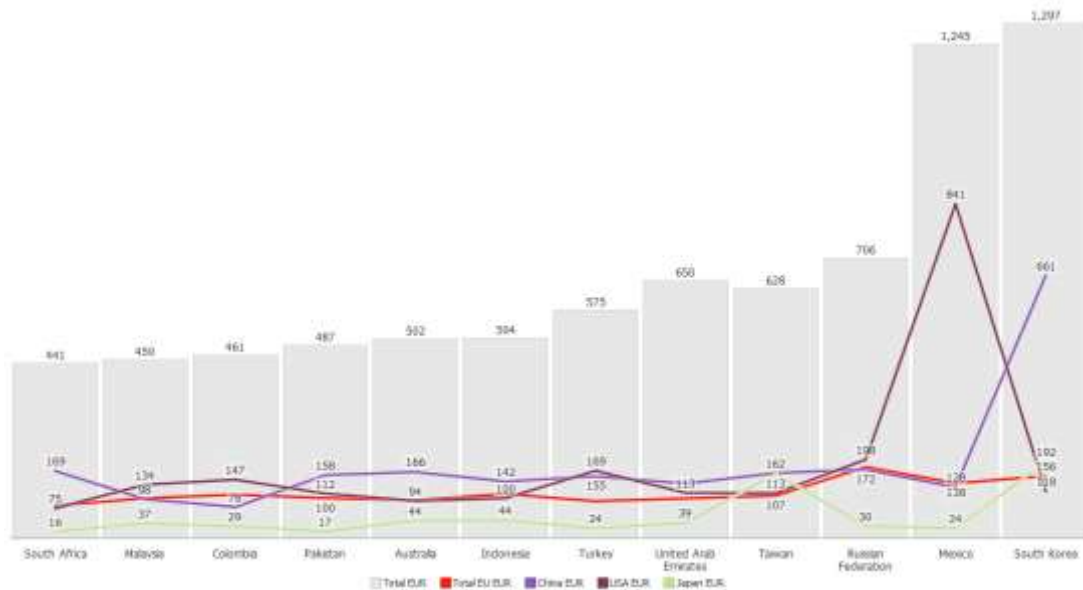


Figure 51 extends the analysis to the next tier of global countries and includes South Korea, Mexico, Russian Federation, Taiwan, UAE, Turkey, Indonesia, Australia, Pakistan, Colombia, Malaysia and South Africa.

Figure 51 : Share of Import Market for Second Tier Trading Nations (non- EU) 2016



In Figure 51, the EU share of imports varies between lows of 11% for Mexico 12% for South Korea to highs of 25% for Russia, 24% for Colombia and 22% for Malaysia and Indonesia. The average for imports from the EU for the 12 countries is 18%- the same percentage as for the USA and China.

Table 30 : Percentage Market Share Compared

	EU	USA	China	Total
South Korea	12	9	51	72
Mexico	11	68	10	89
Russia	25	28	24	77
Taiwan	17	18	26	61
UAE	15	17	21	53
Turkey	16	29	27	72
Indonesia	22	20	28	70
Australia	19	19	33	71
Pakistan	20	23	32	75
Colombia	24	32	17	73
Malaysia	22	30	22	74
South Africa	18	17	38	73
Average %	18	26	27	

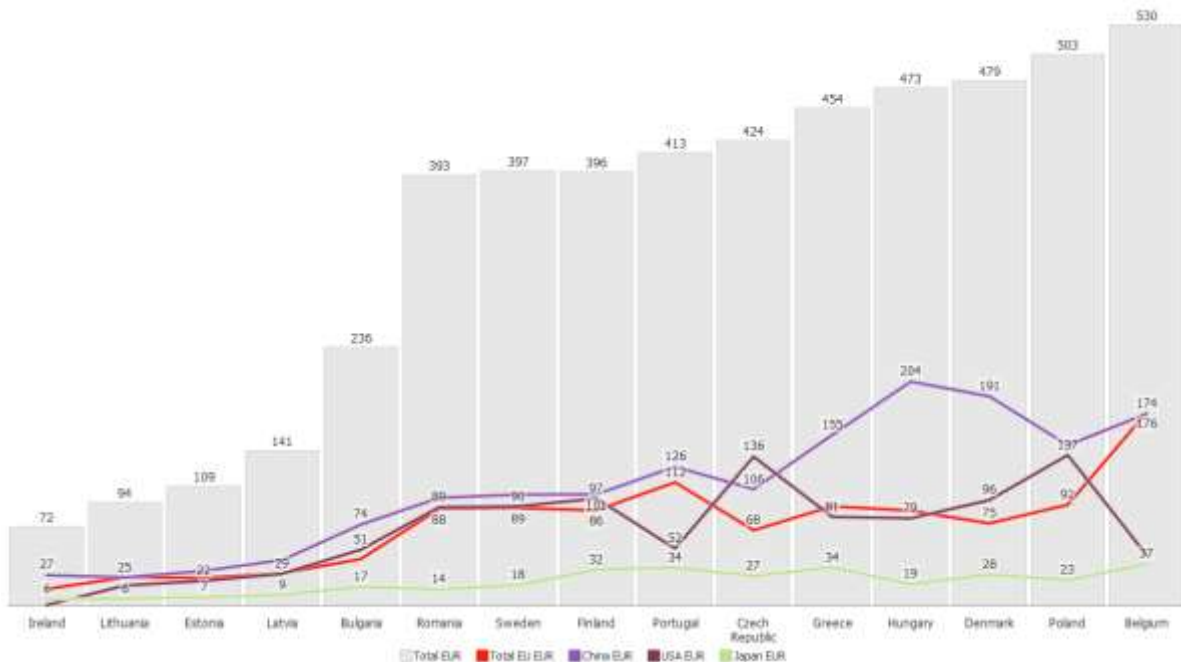
The comparative results between the EU, USA and China are listed in Table 30 : Percentage Market Share Compared. This shows that the USA accounts for an average of 26% (boosted by regional trading with Mexico and Colombia) and China accounts for 27% (boosted by regional trading with South Korea).

What stands out from this analysis is that the combined imports of the EU, USA and China typically account for 73% of imports (UAE, Taiwan and Mexico excepted).

It is also worth noting the higher than average levels of Chinese imports for South Africa, Australia and Pakistan.

The final analysis in Figure 52 is applied to the 15 middle ranking countries of the EU and follows on from the analysis in Figure 50.

Figure 52 : Share of Import Market for Middle Ranking EU Trading Nations 2016



In Table 31, the EU share of imports varies between lows of 12% for Latvia and 16% for Denmark and the Czech Republic, to a high of 33% for Belgium. The average for imports from the EU for the 15 countries is 21%- which is higher than for non- EU countries, but lower than the percentage for the larger EU countries.

Table 31 : Percentage Market Share Compared- EU

	EU	USA	China	Total
Belgium	33	9	33	75
Poland	18	27	29	74
Denmark	16	20	40	76
Hungary	18	17	43	78
Greece	20	18	34	72
Czech Republic	16	32	25	73
Portugal	27	13	30	70
Finland	22	24	25	71
Sweden	22	23	26	71
Romania	22	23	25	70
Bulgaria	18	22	31	71
Latvia	12	21	29	62
Estonia	23	21	28	72
Lithuania	27	19	27	73
Ireland	21	0	37	58
Average %	21	19	31	

The comparative results between the EU, USA and China are listed in Table 31. This shows that the USA accounts for an average of 19% and China accounts for 31% of imports for mid-size EU countries.

What stands out from this analysis is that the combined imports of the EU, USA and China typically account for 73% of imports (Ireland and Latvia excepted). This seems to be broadly true for all EU and non- EU countries

What also stands out is the higher level of Chinese imports, compared with the larger EU countries.

The single most important finding that emerges from this analysis of market share is that whilst the USA is the EU's main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries.

1.1.38 Conclusions and Recommendations

While the US continues to be the EU's main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries. **Any measures that help smaller EU countries access EU sources of supply will help to improve EU competitiveness overall.**

There are some growth markets where EU is a stronger exporter than US, and nearly China, such as South Korea, Indonesia, Russia and South Africa which could form an opportunity for a more coordinated EU export in Cybersecurity products and services.

From the workshop discussions, none of the participants indicated they were directly impacted from imports in the EU or beyond the EU from China. However, in all the workshops the direct impact in both local and international markets on imports from the US was highlighted. The question whether or not, and if so in what way, there will be an impact on trade from the measures announced in the Cybersecurity package¹² (in which the EU intends to put in place Cybersecurity certification regimes) could not be conclusively answered in the workshops with experts.

Focus group participants were divided on whether regulation would support EU competitiveness. Those in favour cited the example of the US and the PCI/DSS regulation, that led to a significant boost in training requirements together with the development of vulnerability products in the US. Others mentioned the GDPR, which is a European regulation, but all the US security vendors specialized in data protection have seemed to benefit from this development, while the EU is lagging behind in this technology. It was also mentioned that legislation may be a business opportunity for the security industry, but for those EU companies that are subjected to it, it is a burden. ECSO members noted that

¹² https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

the new NIS directive will stimulate EU critical infrastructure sectors to address Cybersecurity and this will create an opportunity for EU Industry, as well as supporting ENISA to set up a certification centre.

As indicated in the earlier sections, there are major differences in importing trends across EU countries, which could be more streamlined from an EU perspective and therefore improve overall EU performance as a Digital Single market on a global scale. Adding to that the further improvement and focus on some of the key EU export regions, by focusing international policies and collaboration agreements on Cybersecurity policy collaboration and joint research programs, this could further lead to an increase for EU Cybersecurity companies to play a more significant role in these countries.

During some workshops it was noted that some countries (like Sweden, Poland) are not so active in Cybersecurity exports, while the Member States are very active in Defence and Security activities on a global basis. **There are potential synergies between Defence and Security trade activities and Cybersecurity trade activities that could be exploited, to the benefit of Member State Cybersecurity companies.**

Finally, it should be investigated what the potential impact could be on developing an international trade scheme for Cybersecurity, similar to existing trade schemes on Defence and Security products and services. It is likely that those could be further extended to Cybersecurity. From earlier analysis of the contributing sectors to the Cybersecurity markets, from an export perspective the EU should be supporting the dual use of Cybersecurity products and services: promoting the use of the same technologies for civilian and defence purposes.

EU Supplier Analysis

1.1.39 Key Learnings

A key issue raised by analysis in previous sections is the extent to which EU demand is being met by EU developed and owned companies rather than global companies headquartered outside the EU that establish operations in the EU to meet EU demand. As shown in Section 9.5.2, Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia.

The definition of EU owned companies is subject to a degree of subjectivity and once a company sells its shares on the open market it is hard to ascribe the ownership of the company to any specific region of the world. However, it is possible using the CIMA methodology to identify those companies whose headquarters are located in Europe and this approach has been followed for the larger companies trading in Europe in the analysis below. The impact of International suppliers headquartered outside the EU but operating and selling within the EU is significant.

- The proportion of Cybersecurity suppliers selling within the EU that are EU headquartered companies rather than international companies (headquartered outside the EU) is 69% (2016 figures) in absolute terms (i.e. based on the number of companies of all sizes), varying between 57% and 85% across Member States.
- The proportion of EU Cybersecurity employment within the EU by EU headquartered companies is 73% (2016 figures), compared to 27% of employment by international companies (headquartered outside the EU). Cybersecurity employment within the EU by EU companies varies between 60% and 85% across Member States.
- The proportion of Cybersecurity Sales activities within the EU by international companies (headquartered outside the EU) is 25% (2016 figures), compared to 75% of Sales within the EU by EU headquartered companies. EU Cybersecurity Sales within the EU by International companies varies between 16% and 40% across Member States.
- Although the EU only imports 5.3% of its domestic demand (2016 figures - Section 10.2.2), a much larger portion of its demand is met by international companies headquartered outside the EU that

have established operations in the EU to access the EU market. The proportion of EU demand met by international companies from sales within the EU (as opposed to imports) lies between 21-25% (2016 figures) depending on how much of the international company sales activity in the EU is exported outside the EU. If one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.

1.1.40 Analysis

To analyse the impact of global companies headquartered outside the EU the most recent EU market data for 2016 was disaggregated to look at the impact of global non-EU companies on EU Sales and Employment. All international (non-EU) companies without a headquarters in Europe with turnover above GBP 50 million (EUR 55 million) were separated out from the sales and employment data (to account for them separately) to assess their impact on the EU Cybersecurity market. Trading evidence from such larger companies was examined to confirm their credentials (services etc), and their tax and trading situation was then examined to identify their trading status and then their ultimate registered HQ.

Figure 53 below shows the number of EU headquartered Cybersecurity companies operating in EU Member States in 2016.

Figure 53 : Number of EU Cybersecurity companies (headquartered in the EU) selling within EU Member States 2016

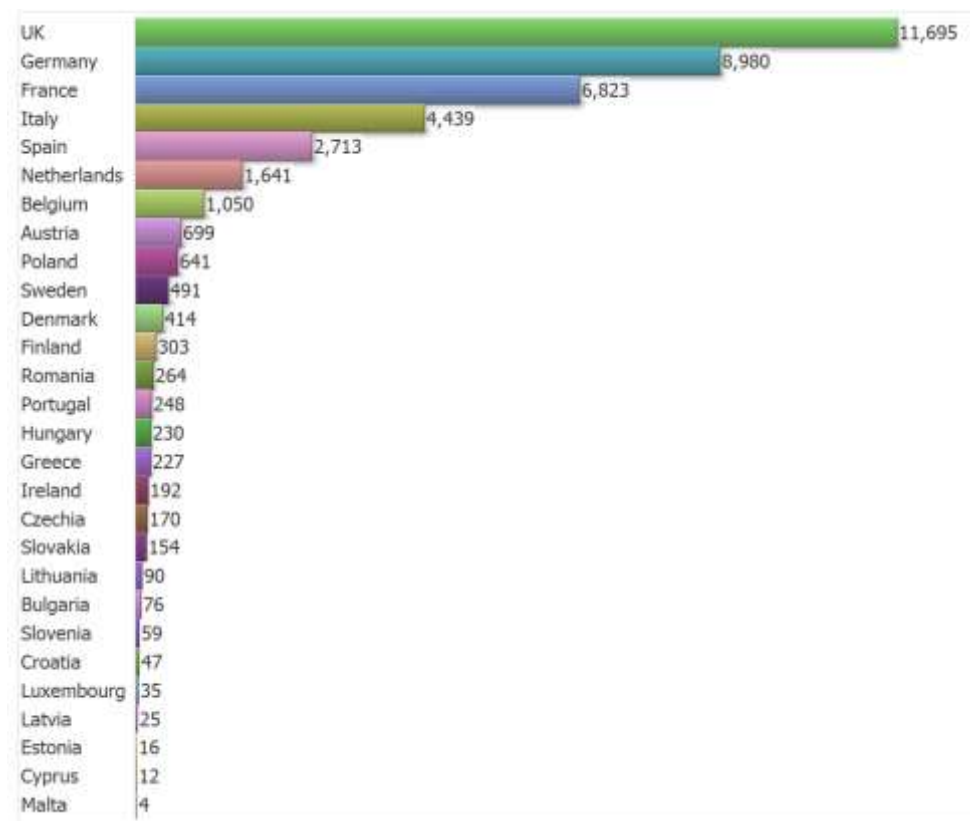


Table 32 compares the above data with company data from Section 9.4 and shows the proportion of Cybersecurity suppliers selling within the EU that are EU headquartered companies rather than international companies headquartered outside the EU.

Table 32 : Proportion of EU Cybersecurity suppliers (selling within the EU) that are EU headquartered companies 2016

Member State	Companies 2016	EU Companies 2016	Proportion of EU Companies 2016
Austria	880	699	79%
Belgium	1653	1050	64%
Bulgaria	92	76	83%
Croatia	65	47	72%
Cyprus	15	12	80%
Czech Republic	257	170	66%
Denmark	664	414	62%
Estonia	23	16	70%
Finland	365	303	83%
France	8476	6823	80%
Germany	12755	8980	70%
Greece	354	227	64%
Hungary	280	230	82%
Ireland	251	192	76%
Italy	6914	4439	64%
Latvia	30	25	83%
Lithuania	109	90	83%
Luxembourg	41	35	85%
Malta	7	4	57%
Netherlands	2239	1641	73%
Poland	922	641	70%
Portugal	336	248	74%
Romania	315	264	84%
Slovakia	229	154	67%
Slovenia	85	59	69%
Spain	4181	2713	65%
Sweden	687	491	71%
UK	18025	11695	65%
EU TOTAL	60250	41738	69%

The proportion of Cybersecurity suppliers selling within the EU that are EU headquartered companies rather than international companies (headquartered outside the EU) is 69% (2016 figures), in absolute terms (i.e. based on the number of companies of all sizes), varying between 57% and 85% across Member States.

Figure 54 below shows the number of employees in EU headquartered Cybersecurity companies operating in EU Member States in 2016, excluding employment by international companies.

Figure 54 : Number of employees in EU Cybersecurity companies in EU Member States 2016

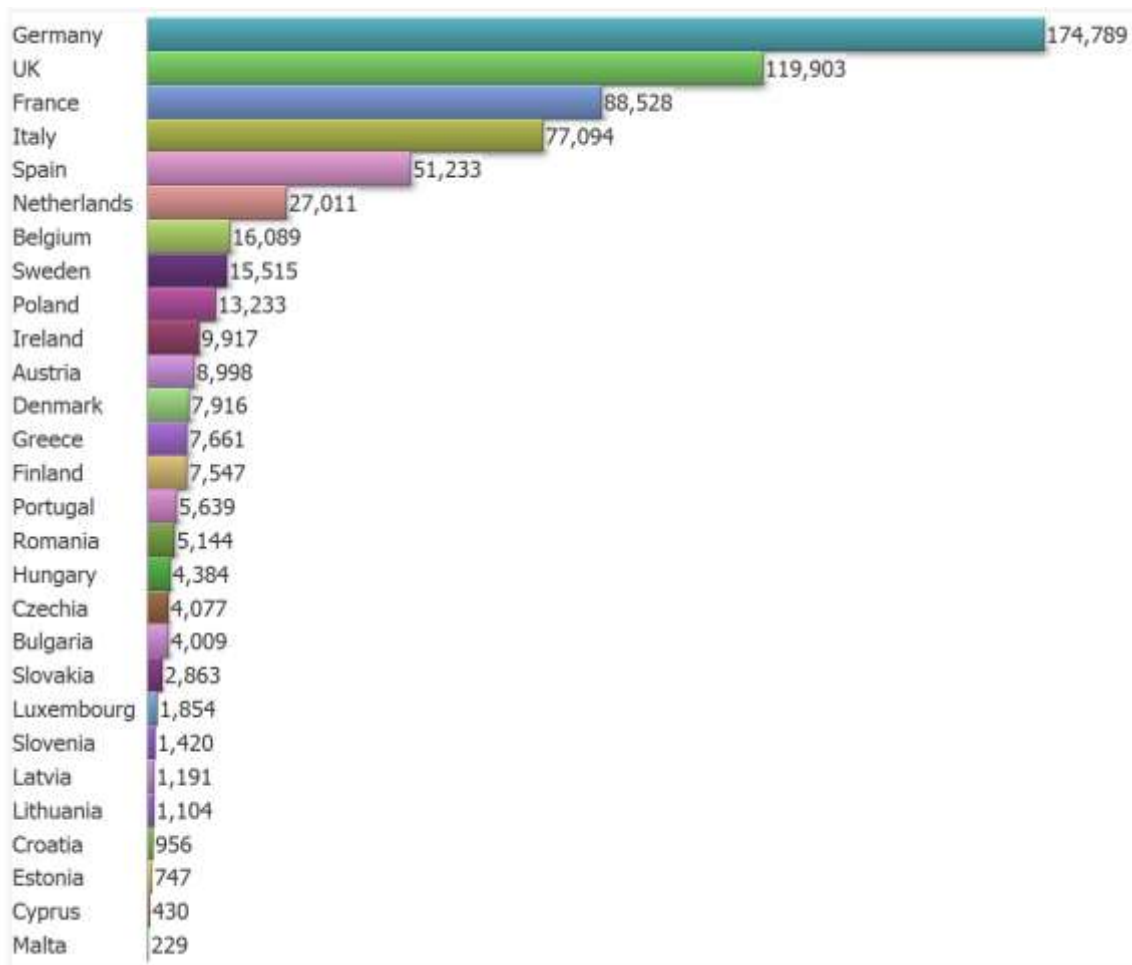


Table 33 compares the above data with employment data from Section 0 and compares Cybersecurity employment in the EU by EU headquartered companies with employment by international companies headquartered outside the EU.

Table 33 : Cybersecurity employment in the EU by EU and International companies 2016

Member State	Employees 2016	EU Company Employees 2016	EU employment by EU Companies 2016	EU employment by International Companies 2016
Germany	215523	174789	81%	19%
UK	150255	119903	80%	20%
France	146086	88528	61%	39%
Italy	124546	77094	62%	38%
Spain	73371	51233	70%	30%
Netherlands	38864	27011	70%	30%
Belgium	20417	16089	79%	21%
Poland	18985	13233	70%	30%
Sweden	18340	15515	85%	15%
Austria	13033	8998	69%	31%
Ireland	12554	9917	79%	21%
Denmark	11923	7916	66%	34%
Finland	9826	7547	77%	23%
Greece	9056	7661	85%	15%
Portugal	7147	5639	79%	21%
Czech Republic	6772	4077	60%	40%
Romania	6663	5144	77%	23%
Hungary	6098	4384	72%	28%
Bulgaria	5087	4009	79%	21%
Slovakia	4337	2863	66%	34%
Luxembourg	2355	1854	79%	21%
Slovenia	1943	1420	73%	27%
Latvia	1529	1191	78%	22%
Lithuania	1442	1104	77%	23%
Croatia	1437	956	67%	33%
Estonia	1020	747	73%	27%
Cyprus	649	430	66%	34%
Malta	327	229	70%	30%
EU TOTAL	909585	659481	73%	27%

The proportion of EU Cybersecurity employment within the EU by EU headquartered companies is 73% (2016 figures), compared to 27% of employment by international companies (headquartered outside the EU). Cybersecurity employment within the EU by EU companies varies between 60% and 85% across Member States.

Table 34 shows the Cybersecurity Sales activities across the EU in 2016 by EU headquartered companies and compares this with EU Sales data from Section 0, to calculate the proportion of Cybersecurity sales activities within the EU by EU companies, compared to international companies (headquartered outside the EU).

Table 34 : Cybersecurity Sales activities (m EUR) by EU companies and International companies in EU Member States 2016

Member State	Sales (€m) 2016	Sales (€m) by EU companies 2016	Proportion of Sales by EU companies 2016	Proportion of Sales by International companies 2016
Germany	34261	23811	69%	31%
UK	31950	23259	73%	27%
France	23302	19620	84%	16%
Italy	19910	15808	79%	21%
Spain	11943	8073	68%	32%
Netherlands	6485	5467	84%	16%
Belgium	4542	3792	83%	17%
Sweden	3283	2344	71%	29%
Austria	3261	2378	73%	27%
Poland	3040	1903	63%	37%
Denmark	2076	1372	66%	34%
Finland	1864	1485	80%	20%
Ireland	1696	1065	63%	37%
Greece	1546	1033	67%	33%
Czech Republic	1198	935	78%	22%
Portugal	1180	937	79%	21%
Romania	1140	793	70%	30%
Slovakia	1109	724	65%	35%
Hungary	1022	838	82%	18%
Bulgaria	753	535	71%	29%
Slovenia	476	398	84%	16%
Latvia	384	273	71%	29%
Luxembourg	349	286	82%	18%
Croatia	337	226	67%	33%
Lithuania	316	218	69%	31%
Estonia	263	169	64%	36%
Cyprus	188	113	60%	40%
Malta	98	81	82%	18%
EU TOTAL	157972	117936	75%	25%

The proportion of Cybersecurity Sales activities within the EU by international companies (headquartered outside the EU) is 25% (2016 figures), compared to 75% of Sales within the EU by EU headquartered companies. EU Cybersecurity Sales within the EU by International companies varies between 16% and 40% across Member States.

Table 35 compares the above sales figures for EU and international companies with EU trade flow data from Section 0, to estimate the proportion of EU demand met by international companies.

Table 35 : EU Cybersecurity Demand met by International companies (m EUR, %) 2016

EU Domestic Demand (€m) 2016	Imports (€m) 2016	Imports relative to domestic demand	Sales in EU by International Companies based in EU (€m) 2016	Exports (€m) 2016	International company share of domestic demand from sales inside EU (€m, % range) 2016
160386	8540	5.3%	40036	6126	33910 - 40036 (21% - 25%)

Although the EU only imports 5.3% of its domestic demand (2016 figures - Section 10.2.2), a much larger portion of its demand is met by international companies headquartered outside the EU that have established operations in the EU to access the EU market. The proportion of EU demand met by international companies from sales within the EU (as opposed to imports) lies between 21-25% (2016 figures) depending on how much of the international company sales activity in the EU is exported outside the EU. If one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.

1.1.41 Conclusions and Recommendations

The impact of International suppliers headquartered outside the EU but operating and selling within the EU is significant, with 'effective' imports from international companies of between 26-30% of EU demand in 2016, as explained earlier.

Analysis earlier in Chapter 10 indicates that EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders, and that the EU is not achieving its export potential when judged from this economic perspective. The presence in the EU of international operations established to support access to EU markets may be a factor in the EU's relatively low Cybersecurity exporting activity, since such international operations may not be arranged to address non-EU markets.

Further study should be considered to examine the implications and impact of the significant EU dependence on International suppliers on the EU Cybersecurity market, for example what the benefits and disadvantages of such international investment in Europe are.

Workshops

Introduction

In order to validate the initial data and to elicit views on the state and needs of the Cybersecurity industry, fifteen workshops were held in different Member States between June 2017 and October 2017 with representatives of the European Cybersecurity Industry and in some cases, the European Commission. Workshops were held in the following Member States (11) : Belgium (4), France, The Netherlands, Luxemburg, Germany, UK (2), Sweden, Poland, Greece, Italy and Spain. Selection of the Member States to organize the workshops was done on the basis of : 1) cost of organizing workshops, inviting participants, interest and responsiveness of local markets; 2) Cybersecurity market sizes, focusing first on the larger representative markets (Germany, UK, France, Italy, Spain, Netherlands, Belgium) and finding representative markets for the smaller relative contribution to the European Cybersecurity market (Sweden – Scandinavian markets, Poland – Eastern European Markets, Greece – Southern & Balkan markets). In collaboration with the European Cybersecurity Public Private Partnership ECSO, two workshops were held with the members of ECSO participating in the working group on market developments (WG2). A summary of the discussions and resulting recommendations is provided in **Appendix M : Results from workshops**.

Workshop Methodology

1.1.42 Validation Workshop

A first validation workshop was held jointly with ECSO in Brussels on June 6th 2017 together with ECSO members and a representative of the European Commission present. The first results were debated and reactions noted. Some major recommendations helped to shape further analysis of the document and the report :

- Consideration to indicate the originating markets, as this study indicates a major difference from the traditional market estimations. The CIMA market study indicates a size of Cybersecurity market ranging to nearly a quarter of the total ICT market. This was further documented with the other Cybersecurity domains such as Defence, Security, ICT, Insurance as other domains contributing to the total Cybersecurity market
- Consideration to drill down on some of the categories, resulting in a reshuffling of the Level 2 subcategory, for instance putting all relevant activities related to Intrusion Detection (IDS) under Infrastructure rather than under Identity and Access Management
- Consideration to include also intelligence on other major European markets such as Norway and Switzerland. These were included in some of the presentations, but were eventually not used in the overall market analysis. They have been added to this report.

1.1.43 Country Workshops

Typically, these workshops were attended by 10-25 people, with attendees from start-ups, SMEs, LEs and research institutes, thus providing a wide range of views. An example of the calling notice (for one of the UK workshops) is given below.

Participants were invited through various channels (direct marketing, public websites, social media, face to face invitations). Participation was free, upon registration to the activity. Most workshops took between 4 and 6 hours, presenting results, the methodology and entering into debate about the results, conclusions and recommendations. All comments and recommendations were recorded and

noted and serve for the description recommendations in the various chapters. Concerns about the data were validated, and where possible adapted and reconfigured.

Example invitation workshop :

Country workshop (UK)

The European market for Cybersecurity is estimated at around EUR 160 billion in 2016. The UK is one of the leading countries in terms of both demand and supply. The European Commission has initiated an analysis to better understand the current UK, European and global Cybersecurity market structure. You are invited to attend a workshop devoted to the presentation of the first quantitative results of this analysis and to share your perspectives on the needs and challenges in the Cybersecurity market. Workshops to present the results and inform the report are also being held in July and August 2017 in 9 European Countries and results combined.

Focus group participants will:

- Discover the European Commission's plans for stimulating the Cybersecurity market
- Hear ECSO's objectives and programme with a proposed budget of EUR 1,800 million
- Participate by sharing your views and influencing future European (and UK) policies
- Take away the latest 2016 UK data and its global context from the study which includes: market segmentation, employment, company numbers, in-country sales, import and export data plus other data.

During these workshops selected quantitative data were presented together with key Member State data. Discussions were held on the results, questioning the validity of the results, particularly for the Member State involved, and the rationale for the taxonomy and methodology. These discussions led to further investigation of some of the data during additional quantitative research.

Some of the discussions focused on recommendations for improving the current situation for the European Cybersecurity Industry as a whole, and some specific markets. New areas of interest from the demand side were identified during the workshops. These were identified using standardised questions at each workshop based on the structure below. It should be noted that the views reported below are the consolidated views of the attendees but they have not been further validated. Possible recommendations emerging from the discussions have been combined and validated against other workshops and expert views to provide a set of recommendations to the EC.

Example of briefing to workshop participants:

Some questions and topics for discussion and debate during the workshops:

Fragmentation

What are the causes of current market fragmentation?

What influences buying behaviour?

- Trust, Geographical provenance, Certification, Labels, User behaviour, ...

SWOT

- What are the strengths and weakness of the Member State Cybersecurity industry and how can policy makers assist in addressing them, e.g.?
- Standardization; Certification; Research and innovation; Licensing & IPR; Pre-commercial procurement and public procurement of innovation; Investment support

Role of government agencies

- What role should EU and national governments play in supporting Cybersecurity industry?

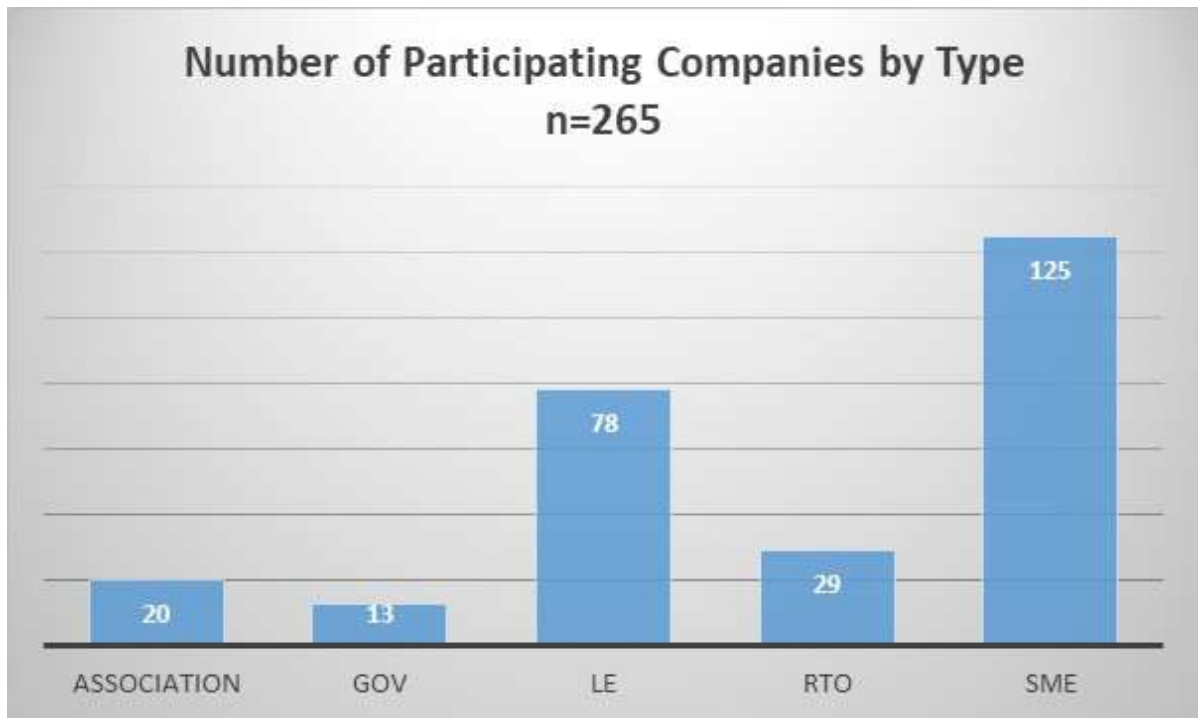
Workshop participation Summary

In total, nearly 1000 persons were able to see some of the preliminary results in various settings, public speaking opportunities and the validation and country workshops. In the country workshops, nearly 300 participants were counted. The country workshops were co-organised and supported by a local partner, and supporting partners engaged in facilitating, hosting, catering, participating in debates and inviting local companies to participate in the debate. Local strategic partners included :

1. ECSO : European Cybersecurity Organisation (the Cybersecurity Public Private Partnership with the European Commission), nearly 250 member companies
2. Belgium : LSEC – Leaders In Security, nearly 300 member companies
3. France : Pôle SCS - Pôle de compétitivité Solutions Communicantes Sécurisées, nearly 300 member companies
4. The Netherlands : HSD - The Hague Security Delta, nearly 200 member companies
5. Germany : ECO, nearly 1000 member companies
6. Sweden : Ericsson and Ciptor
7. Spain : INCIBE
8. Italy : Leonardo Italia
9. Greece : Demokritos and Satways
10. Poland : Cybersec Hub, nearly 80 partner companies

In Figure 55 a graphical representation of the participation of organizations participating to the workshops is presented by types of organizations: ME (micro-enterprises), SME (small and medium), LE (large), Associations, RTO (research and technology organizations) and GOV (government representations). From the almost 300 participants to the workshops, only the unique companies were counted for this representation, on their originating member state. In some cases, a company appears twice, as it had representatives from different legal entities from other member states participating.

Figure 55 : Number of participating companies in the Validation and Country workshops organized by CIMA



Taking the consideration of the representative Member States, organizations and companies from 18 different European Member States (out of the EU 28) participated directly (through active participation and contributions to the discussions) or indirectly (following the debates and receiving documentation, not actively contribution to the discussion) in the workshops.

Based upon this voluntary participation, after a selection of the locations, participants were a significant representation of the Cybersecurity Industry in Europe.

Figure 56 : Country representation of Participating Companies



Analysis related to the pre-defined study requirements

The quantitative analysis of the market data collected over the period 2014 to 2016, and discussions and debates during workshops in different European Member States delivered the following results to some of the preliminary questions raised for the study.

Potential impact from Critical Infrastructure operators on the Cybersecurity Industry

Critical operators are operators defined in Critical Infrastructure (CI) regulations¹³. These differ in the various European Member States, depending on the specific situation a country is in, at a given moment in time. Some of the CI domains defined include: Transport (and extended, Automotive), Energy, Finance, Health, Manufacturing. Some other domains include Water, Communications, ... In the NIS directive¹⁴, critical operators are extended to both Operators of Essential Services (OES) and Digital Service Providers (DSP). Telecom operators should also be considered as CI following the Directives.¹⁵

In 2016 there was an impact from Critical Infrastructure operators on the Cybersecurity Industry, as was reported in Section 0 EU Cybersecurity End- Users. Taking into account CI such as Water and Energy Utilities, Transport, Emergency Services, Communications, Financial Services and Healthcare the EU CI would account for 15.5% of the total EU Cybersecurity Market. In some Member States government services are also considered as CI, which would result in another 31.1% of the EU Cybersecurity Market. Adding to that, we could consider OES and DSP's as part of the Information Technology domain, which contributed in 2016 to the Cybersecurity Industry by nearly 4% of the EU Cybersecurity Market. Together, the CI, OES and DSP Operators would count for half of the EU Cybersecurity Market. However, in most Member States not the whole sector should be considered as critical or essential services, but a specific series of operators and only specific parts or components of these operators infrastructures. Whether they are critical or essential has typically been a decision by the Member States, but has not been made publicly available.

In addition, due to the ongoing transposition of the NIS Directive in all the Members States, apart from Germany which has transposed the NIS Directive during the first half of 2017 into German regulations – the impact from the Directive will mostly be seen from 2017 onwards. It is expected that due to additional requirements for protection, management and reporting of CI and OES, there will be an increase in demand of Cybersecurity Products and Services in 2018 and 2019.

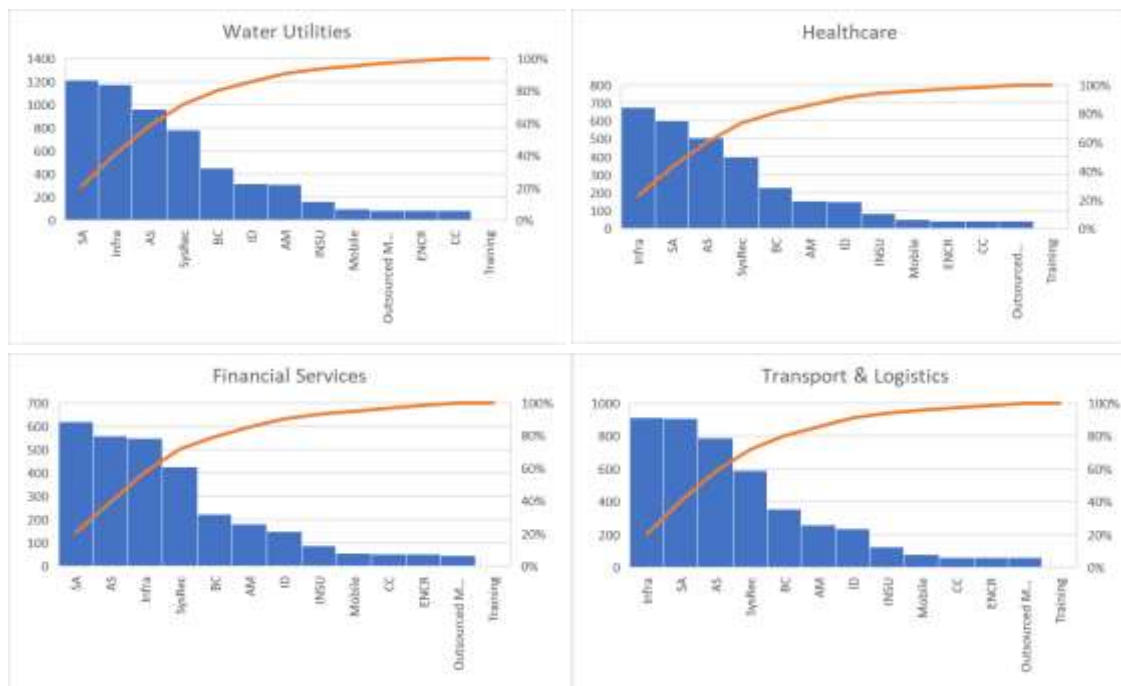
For many of these sectors, such as Water & Energy Utilities, Healthcare, Financial Services and Transport, still a lot of spending was spent into Infrastructure, Situational Awareness and Application Security, next to System Recovery and Data Cleansing (sub-level category 2).

¹³ COUNCIL DIRECTIVE 2008/114/EC, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, European Council, 23.12.2008. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>

¹⁴ European Parliament and COUNCIL DIRECTIVE (EU) 2016/1148, The Directive on security of network and information systems (NIS Directive). <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>

¹⁵ DIRECTIVE 2002/21/EC, common regulatory framework for electronic communications networks and services, (Telecom Regulation) http://www.bipt.be/public/files/en/1694/3236_en_en_directive_2002_21_erg.pdf

Figure 57 : comparing differences between CI sectors



When comparing the spending patterns from the different CI, there is a slight relative difference in the spending from Water and Energy utilities, together with Financial Services more focusing on Situational Awareness. A significant difference appears from the relative impact of Application Security in Financial Services vs other sectors.

There clearly is an impact from the CI operators (and in addition OES and DSP operators) on the CSI, but the type of impact and its magnitude remain yet unclear. This was also confirmed during the different workshops, where companies clearly indicated that they had not yet seen any significant effect from the NIS Directive or its transposal on their offerings.

Who are the large exporters and who are their clients?

In Section 0 the EU Cybersecurity Supply reports on the number and range of EU Cybersecurity suppliers, by size and representing sector. Section 0 EU Cybersecurity Exports reports on the market exports and the relative contribution of EU exports.

In **Appendix K : Top 500 Global Cybersecurity Companies** represents in red the top European Cybersecurity companies on a global level. These have been marked in Red, but represent only 14% of the list.

In Chapter 0 EU Competitiveness the target markets of these exports were identified in comparison to other global and EU markets.

The company list was based upon research into the major global exporting companies into 15 major economies (USA, China, Japan, Canada, Germany, Indonesia, Mexico, France, Saudi, India, Singapore, South Korea, Italy, Brazil and Russia). Not all companies exported into all 15 countries.

In Table 25 : EU Exports by Sub-sector 2016 and Table 21 : EU Imports by Sub-sector 2016 (m EUR) – alphabetical and top down non-EU % imports the subcategories of Cybersecurity were compared in volumes of total exports and imports vs the exports and imports beyond the EU. This analysis indicated a wide variety of responses to exporting:

- Companies exporting from one or two location within the EU- examples include BAE Systems, Clearswift and DriveLock
- Companies exporting from multiple locations (same entity) across the EU- examples include Accenture, Verizon, Symantec and Panda Security
- Companies exporting from multiple locations (multiple entities) across the EU- examples include SAP and Atos.

In total, the 250 companies included in this research export from a total of 750 locations across Europe, demonstrating a complex matrix of how exports occur, before even attempting to map their destinations.

What does cross border trade flow in EU look like and how can it be improved?

Section 0 Trade Flow Analysis is dedicated to this topic, but should be considered in relation to analysis and conclusions from Sections 0 Market Share Analysis, 0 EU Cybersecurity Exports and 0 EU Cybersecurity Imports.

Cross border trade flow in EU exists, but varies greatly on a per Member State basis. Results of both analysis and workshops have led to the following potential courses of action:

1. In countries heavily relying on imports from outside of EU (Denmark, UK, Slovakia, ...), emphasize the existence and strengths of EU Cybersecurity products and services
2. Consider the impact of UK on the total Cybersecurity Market size, being an important contributor to the size of the Cybersecurity Industry in EU, but a rather limited impact on the contribution to and from EU. Further improvement of trade relations between UK and EU could strengthen both markets, in favour over US and China.
3. Investigating the potential for dual use, the use of civilian Cybersecurity products and services for Defence industry and reversely, using military Cybersecurity technologies for civilian use
4. Setting EU policies recommending Member States to emphasize the use of EU Cybersecurity products and services over non-EU in public procurements, which account for a significant stake in the EU
5. Aiming to raise the total of EU Cybersecurity trade flows to EUR 2 billion by 2022, and therefore decreasing the total non-EU imports resulting in a larger contribution of EU on a global level
6. Supporting the development of a Digital Single Cybersecurity market, supporting free flow of Cybersecurity products and services between EU, addressing issues such as certification and standard schemes on an EU-wide level.
7. Identifying key Cybersecurity companies per Member State, on the basis of their appearance in the global high growth list, and their significance in local markets and supporting the cross border trade flows with a group of 280 to 560 companies (10 to 20 companies per Member State). This will also improve the cross border trade flow beyond the EU.

While the improvement of trade flows between EU Member States is important and recommended, more significantly the improvement of trade flows between EU and the rest of the world should be strengthened. On the basis of stronger EU market endorsement, support from Member States is required, leveraging existing trade agreements (in Defence, Security, ...), targeting specific high growth markets (such as Taiwan, Pakistan, India, ...) or targeting markets with a relative higher import from EU (such as South Korea, South Africa and Russia), developing additional promotional support on a Digital Single Security market with key EU Cybersecurity companies.

Additional perspectives can be found in **Appendix E : Competitive Dashboards** where specific dashboard on EU28, EU27 and USA, China, Japan, India, and individual EU countries have been reported.

What does the products & services landscape in Europe look like? (A perspective of the surveyed segments.)

In Chapter 0 EU Cybersecurity Market the landscape of products and services in Europe have been analysed and reported. In addition **Appendix B : EU Sales by Sub-sector and Purchaser Industry**, **Appendix E : Competitive Dashboards**, where specific dashboard on EU28, EU27 and USA, China, Japan, India, and individual EU countries have been reported – and **Appendix H : Taxonomy – Cybersecurity Data Level 2 – 4 Definitions** report on the topic of products & services landscape.

In this Cybersecurity Industry Market Analysis, a taxonomy has been developed scoping more than 1100 product and services categories, fitting all products and services in the market which have been traded in 2016. These 1100 product and services categories have been regrouped on three different levels and are being reported on a level 2 category system presenting Infrastructure, Situational Awareness, Application Security and System Recovery & Data Cleansing as the biggest categories of products and services in Europe, representing over 72% of the total Cybersecurity Market in Europe.

All products and services have been growing on average 17%, with Encryption the highest growth of 31% and Training and Education (which is the smallest category) only growing 4%. There is a difference in products and services categories per Member State, indicating the level of maturity of a particular market. In countries such as Poland, Portugal, Romania, Croatia, Latvia, Hungary and Greece significantly less is spent in Infrastructure and significantly more in System Recovery and Data Cleansing. However, the same can be stated for UK, which is to be considered one of the more mature markets. There the contribution of Situational Awareness spent is significantly higher than the other group of countries.

In the following Tables (Table 36 through to Table 42) some samples have been drawn from the leading Member States (Germany, UK, France, Italy, Spain, Netherlands, Belgium) in terms of top selling Products and Services categories.

There is a lot of variation in top products and services, the amounts spent and the overall type of expenditure in the various markets. Intrusion Detection is in the top 15 of all the respective Member States. In UK that is also the case, but where a large amount of investment in Germany is in the top 10 categories, UK's spending is far more diverse. In UK, over 177 product and services level 5 categories contributed to over EUR 50 million in 2016. In Germany this was the case for 111 Cybersecurity products and services level 5 categories. There is more variety in purchasing in UK than in Germany. This could also be an indicator indicating the levels of maturity of a specific market. France, Italy and Spain are in similar situations to Germany. In many cases the type of spending will be heavily depending on the availability of products and services. In UK "Specialist Anti-Malware" is the second highest sale activity, with the level 5 product category of Malware Forensics for Commercial Applications nearly EUR 332 million, whereas in France the second highest is related to Situational Awareness.

Table 36 : GERMANY : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	997.84
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	839.15
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Comm	680.13
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	678.43
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Anal	606.20
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Analysis for Comm	576.00
Application Security	Vulnerability Assessment	Automated Causality Analysis	Automated Casualty Analysis for Commerci	522.20
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	510.10
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation Commercial Ap	495.33
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	462.24
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Specia	438.92
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Anal	382.95
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Commercial	357.34
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Commercial Applicat	353.82
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specialist Research	339.63

Table 37 : UK : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	334.72
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Commercial Applicat	331.93
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Comm	291.73
System Recovery & Data Cle	System Recovery & Data Cleansing	Data Verification	Data Verification Services for Commercial A	285.36
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	279.89
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Commercial	255.87
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Commercial App	244.58
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Analysis for Comm	240.62
System Recovery & Data Cle	System Recovery & Data Cleansing	Data Formatting	Data Formatting Services for Commercial Aj	235.77
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specialist Research	222.58
System Recovery & Data Cle	System Recovery & Data Cleansing	Data Updation	Data Updation for Commercial Applications	215.34
Situational Awareness	External Cyber Threat Intelligence	Cyber Law Enforcement	Cyber Law Inforcemen tCommercial Applica	214.25
Encryption	Identity Management	PIN sentry	Chip authentication programme Cards	208.10
System Recovery & Data Cle	System Recovery & Data Cleansing	Data Verification	Data Verification Services for Specialist Res	207.99
Application Security	Vulnerability Assessment	Automated Causality Analysis	Automated Casualty Analysis for Commerci	204.16

Table 38 : FRANCE : Top 15 Product and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	750.60
Situational Awareness	Low level Situational Awareness*	Automated Damage Assessment	Automated Damage Assessment for Comm	453.39
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	413.11
Business Continuity	IT/Cyber Forensics	Automated Forensics	Automated Forensics for Commercial Applic	398.09
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Commercial	395.46
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	377.24
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Commercial App	367.68
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ne	314.73
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation Commercial Ap	306.60
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Anal	275.89
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Specialist Rese	259.25
Situational Awareness	Low level Situational Awareness*	Automated Damage Assessment	Automated Damage Assessment for Specia	257.65
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation Specialist Rese	243.34
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Specialist R	232.53
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Anal	232.11

Table 39 : ITALY : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	818.02
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Commercial Applicati	530.80
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	488.14
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specialist Research	358.61
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	331.98
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	311.26
Business Continuity	IT/Cyber Forensics	Automated Forensics	Automated Forensics for Commercial Applic	295.79
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Analysis for Comm	254.68
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Analy	215.67
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Analy	213.58
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Specia	210.13
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Comm	209.07
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	205.42
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	194.96
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Commercial App	194.13

Table 40 : SPAIN :Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	257.26
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Commercial Applicati	256.80
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	213.58
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Commercial App	191.84
Application Security	Vulnerability Assessment	Automated Causality Analysis	Automated Casualty Analysis for Commerci	186.97
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Information Flow Analy	166.70
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Analysis for Comm	165.06
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	154.52
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Comm	153.29
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specialist Research	152.52
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Applications for Co	150.23
Business Continuity	IT/Cyber Forensics	Automated Forensics	Automated Forensics for Commercial Applic	138.41
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Commercial	109.28
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	106.66
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Specia	103.62

Table 41 :The Netherlands : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Commercial Applicati	211.11
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	202.47
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Applications for Co	153.08
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specialist Research	149.09
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Ho	117.82
Application Security	Vulnerability Assessment	Automated Causality Analysis	Automated Casualty Analysis for Commerci	114.41
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for Commercial App	107.95
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Applications for Sp	104.97
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation Commercial Ap	102.54
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Analysis for Comm	99.80
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	96.86
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analysis for Specia	71.44
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Public Organisations	69.21
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Response Commercial	68.33
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection Systems Net	65.33

Table 42 : BELGIUM : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems Ne	Automated Intrusion Detection	210.09
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Respons	123.50
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems Ho	Automated Intrusion Detection	100.78
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analy	85.90
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems Ne	Automated Intrusion Detection	84.39
Situational Awareness	Low level Situational Awareness*	Automated Damage Assessment	Automated Damage Assessm	71.88
Business Continuity	IT/Cyber Forensics	Automated Forensics	Automated Forensics for Spec	62.85
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems Ne	Automated Intrusion Detection	57.46
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analy	55.85
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for C	51.03
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation C	50.10
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Appli	48.31
Business Continuity	IT/Cyber Forensics	Automated Forensics	Automated Forensics for Com	47.23
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems Ho	Automated Intrusion Detection	46.35
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation S	42.05

To further identify differences, we've added the top products and services level 5 category for Switzerland, indicating a higher investment in Application Security related to automated attack trend analysis and Malware Forensics rather than Intrusion Detection Systems. Some of these products and services indicate a different type of need, which is related to the level of maturity of certain markets (which have already been investing in IDS and infrastructure in the previous years).

Table 43 : SWITZERLAND : Top 15 Products and Services Level 5 Category

Level 2	Level 3	Level 4	Level 5	Total €m
Application Security	Vulnerability Assessment	Automated Attack Trend Analysis	Automated Attack Trend Anal	87.77
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Comm	81.70
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection	57.89
Infrastructure	Intrusion Detection	Automated Intrusion Response	Automated Intrusion Respons	53.64
Application Security	Vulnerability Assessment	Automated Vulnerability Analysis	Automated Vulnerability Analy	50.18
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Appli	48.68
Anti Malware	Specialist Anti Malware	Malware Forensics	Malware Forensics for Specia	48.61
Infrastructure	Intrusion Detection	Automated Intrusion Detection Systems	Automated Intrusion Detection	41.47
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Informati	40.55
Application Security	Vulnerability Assessment	Automated Causality Analysis	Automated Casualty Analysis	38.20
Application Security	Vulnerability Assessment	Automated Alert Correlation	Automated Alert Correlation C	34.75
Business Continuity	IT/Cyber Forensics	Forensic Data Recovery	Forensic Data Recovery for C	33.97
Application Security	Vulnerability Assessment	Cyber Vulnerability Data	Cyber Vulnerability Data Appli	33.76
Situational Awareness	Low level Situational Awareness*	Automated Damage Assessment	Automated Damage Assessm	32.11
Situational Awareness	Low level Situational Awareness*	Automated Taint and Information Flow Ar	Automated Taint and Informati	31.72

Overall the Cybersecurity products & services landscape in Europe looks very fragmented from a per country comparison perspective. But taking the consideration of the taxonomy used for the Cybersecurity Industry Market Analysis, it becomes clear that on a level 2 category system many similarities can be drawn.

More detail on these markets and the detailed perspective per Member State can be found in Section 0 Introduction to the EU Country Level Data and **Appendix E : Competitive Dashboards**.

What is the Role of standardization, certification, audit, trust labels on the European Cybersecurity Industry Market?

At this time, it has not been feasible to directly relate the role of standardization, certification, audit and trust labels to the European Cybersecurity Industry Market on the basis of the quantitative data analysis. Product sales and/or definitions do not include the notification of certified or labelled products and services. Neither has there been a connection to some of the Cybersecurity Industry Market companies, their levels of certifications and labels to the actual products and services impacted.

Any results published would in addition be very challengeable, as the time of the certification and expiration dates have to be reported, including the certification authority for further verification.

In the context of the new Cybersecurity Package, it could be considered that Cybersecurity products and services that require some form of certification take into account the challenges related to the identification of the role on the Cybersecurity Industry Market. Notwithstanding the challenge related to the quantitative data, the topic was discussed in depth during all the country workshops. Overall the participants consider certification and standardization having a positive effect on the European Cybersecurity Industry Market, but the reactions were related to:

1. the current mechanism to allow for certification is expensive, time consuming and affects the quality differentiators of the products (in that they would miss out on additional features and functionalities for the cause of the certification process), or even utilize outdated technologies in order to comply
2. certified products are outdated when they reach the market
3. product development for certification requires an expensive production process, which end users are not always willing to consider
4. there are many different certification systems, they are not aligned.
5. products certified in one country might need to recertify in another country
6. the only industry-wide accepted Cybersecurity product certification scheme is common criteria (the Common Criteria for Information Technology Security Evaluation – CC)¹⁶ with only few Certification Authorities, and few customers requiring CC-levels.
7. it was commonly agreed that an improved certification scheme would further drive the market growth, as many customers are purchasing mainly on the basis of price or are agnostic on products.
8. Voluntary certification schemes or self-certification came highly recommended as a mechanism to allow faster and decent implementation of certification on an industry-wide level, on the basis of commonly identified standard practices (such as security by default, self-certifying security by design, transparency on data collection, ...). Such a scheme could be further improved with a Light certification scheme, that requires formal processes and evaluation procedures. The final step would be an in-depth analysis and audit of the product or service, for either critical infrastructure or similar needs and requirements.

It is clear that Cybersecurity certification, standardization and trust labels only have a very small impact on the current Cybersecurity Industry Market, but that it is expected to quickly grow once additional certification schemes, bodies and further harmonization have been agreed.

What are the key learnings from the data on the role of government?

What is the expected role of the government from the qualitative discussions?

¹⁶ <https://www.commoncriteriaportal.org/>

In Section 0 EU Cybersecurity End- Users, Public was identified as the single largest professional Cybersecurity end-user market, after splitting the Private end-user market in different sub-categories. This is complex as public sector may not be government but for example agencies who act independently of government. Because purchases by public bodies, are often aggregated e.g. as service offerings, it is difficult to determine which products and services are sold into which procurements. The relative contribution that government represents within this domain of Public end-user market, is of course partially linked to the Cybersecurity strategy from governments and potentially resulting Cybersecurity activities for both government itself, public administration and the overall country activities.

However, the expected role of the government should not be underestimated as being only a Cybersecurity end user. As indicated in the different chapters, it can play a more important role.

From the data analysis perspective, Government can influence strongly the impact of the EU Cybersecurity market on national level, by ensuring procurement processes focus in the first place on EU Cybersecurity products and solutions providers. Considering the total import of products and services from outside the EU a EUR 2 billion market in 2017, an additional effort to focus on EU products and services would support the global positioning and strengthening the EU Cybersecurity companies.

Even considering the estimated limited impact from certification and standardization schemes on Cybersecurity today, this is expected to rise significantly as a result of the proposed Cybersecurity Package. Governments have an important role in ensuring the country-wide and fast adoption of the to be agreed Cybersecurity certification mechanism for ICT products and services. Harmonization and a Digital Single Cybersecurity Market in combination with a policy and actions supporting EU products and services, will significantly raise both interest and demand for EU companies also abroad.

Member State Governments should continue raising the bar for Cybersecurity measures from a policy perspective and continuing to applying these measures for public administration purposes as the Government leads by example in Cybersecurity activities and measures.

The Cybersecurity Industry is seeking to get Government support in improved trade and exports, as many EU countries and early stage Cybersecurity companies today, do not all have the same capabilities in getting recognition from outside of the EU. The public sector should consider utilizing trade policy actions to improve Cybersecurity demand to companies from EU. This should also entail the utilization of dual-usage (civilian technologies to be used for defence purposes and conversely), to further reap the benefits of these agreements and to become better qualified in supporting military-grade Cybersecurity solutions abroad. In addition, Governments can consider the use of EU relations to support their gaps for Cybersecurity solutions by utilizing additional experts from other Member States. This way, countries with less direct Cybersecurity for Defence purposes can strengthen their current Defence trade relations with additional Cybersecurity solutions coming from other Member States. These recommendations were made during the various workshops and supplemented by the support of companies to create larger EU-based Cybersecurity Competence Centres in the Member States, on the basis of the existing available expertise.

Cybersecurity experts are willing to support Government in moments of crisis, either on specific case basis for cybercriminal related offenses, for the protection of the critical infrastructure, or in the overall management of major Cybersecurity incidents such as state sponsored attacks or other major crises. The Cybersecurity Industry in the EU sees the benefit in cooperating with Governments and further strengthening the Cybersecurity expertise on a Member State and EU level, both from policy, justice, law enforcement or educational purposed.

SWOT Analysis of the European Cybersecurity Industry

From the obtained data analysis, and as a result from the workshops, the following SWOT analysis was compiled¹⁷:

Cybersecurity market SWOT

Strengths	Weaknesses
- The EU accounted for 26% of the global market in 2016, just ahead of the 25% for the USA. Europe as a whole is the single largest Cybersecurity market in the world. [Chapter 0] - The EU Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, with the number of EU companies and EU employment by sub-sector growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly out to 2021. [Chapter 0] - Cybersecurity activities and companies have emerged from a range of market sectors where Europe is strong (ICT, defence/ aerospace and security) – this offers future opportunities. [Chapter 0] - The high density of strong academic institutions working in Cybersecurity located near Industry companies requiring access to this expertise is an EU strength (e.g. compared to Asia), as is the quality and low cost of education in the EU (e.g. compared to the US). [Chapter 0] - There has been an overall increase in the Cybersecurity investment in critical infrastructures among European enterprises.	- Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia. [Chapter 0] - The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential. [Chapter 0] - The EU, as a whole, imports 5.3% of its Cybersecurity products and services from non-EU sources. The EU is a net importer for all sub-sectors of Cybersecurity, except for Cyber Insurance. Major competitors (US, China, India, Japan) are net exporters in all sub-sectors. [Chapter 0] - Although the EU only imports 5.3% of its domestic demand (2016 figures), if one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016. [Chapter 0] - The European Cybersecurity market is geographically fragmented. [Chapters 0 and 0] - The governments of some countries need to further broaden their knowledge about their Cybersecurity market and its necessities. [Chapter 0] - There is a difference in market maturity of products and services in each country [Chapter 0]. - The European suppliers by themselves will not be able to cover the whole demand of a group of end users Cybersecurity products and services.

¹⁷ We have used the Porter's five forces methodology to develop the SWOTs. The Porter's five forces methodology is based on five pillars: bargaining power of consumers, bargaining power of suppliers, threat of new entrances, threat of substitute products or services, rivalry among existing firms.

	• Some countries did/do not have a specific legislation for Cybersecurity prior to the NIS Directive transposition. • There is a lack of commercial relationships among actors in the 28 Member States. • The need for compliance with local legislation is causing difficulties to European providers when selling their products and services.
Opportunities • The global Cybersecurity market has grown rapidly over the last 3 years (above 18%) with the number of EU (and global) companies and employment growing at a similar rate, and is forecast to continue growing rapidly at a similar rate out to 2021. [Chapter 0] • Forecast sales growth for the EU between 2016- 2021 (17.8%-20.3%) is above the forecast global average of 16-18% and is broadly in-line with historical EU growth in Cybersecurity. [Chapter 0] • The Digital Single Market will promote Cybersecurity in the EU. • The new NIS directive will stimulate EU critical infrastructure sectors to address Cybersecurity and this will create an opportunity for EU Industry. [Chapter 0] • Public users form a significant part of the EU End User market in sales terms (at least 31%) and so public procurement policies can significantly influence the Cybersecurity market. Public Procurement could be split into two: (1) for commodity purchasing, (2) strategic with an industrial policy. [Chapter 0] • China followed by the US is the main competitor to EU suppliers in EU markets ¹⁸and specifically in the smaller EU countries. Any measures that help smaller EU countries access EU sources of supply will help to improve EU competitiveness overall. [Chapter 0]	Threats • Looking at global sales figures the USA is the dominant country in terms of sales (25.3% of global sales) followed by China (9%), Japan (8.3%) and Germany (5.7%). [Chapter 0] • While the USA is the EU's main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries. [Chapter 0] • Most of the main providers are from the United States. • Foreign markets are planning to hire more certified professionals. • Foreign markets impose more barriers on European providers than the European market on foreign providers. • Government-driven innovation funding programmes in Asia and the US give international competitors a competitive advantage compared to Europe, but this applies more widely than Cybersecurity. [Chapter 0]

¹⁸ As earlier reported throughout this document, this number might be distorted as US-originating, and non-European-originating companies operating in the EU (e.g. IBM) are counted as "European", due to the fact that their European trade organizations (e.g. IBM Belgium) collect actual trade values within Europe. This has been reported extensively in the Methodology (Chapter 0 – Research Methodology), and in other chapters.

Conclusions and Recommendations

on the Cybersecurity Industry Market Analysis of the European Market

State of Play

The European Cybersecurity Industry was a EUR 160 billion market in 2016, employing nearly 1 million people. The market has grown 17.4% between 2015 and 2016 and is expected to grow 11.3% in Europe increasing to 12.7% by 2022. This is slightly under the global anticipated growth rate of 12.1 % increasing to 13.5% by 2022. The Cybersecurity Industry comprises not only people involved in providing services and technologies, but also Cybersecurity operators within both private and public organizations.

The European public spending in Cybersecurity exceeds 30% of the whole market, and as a result it is the largest single demand sector. The Cybersecurity demand in Europe has been growing slightly slower than the Cybersecurity demand in the rest of the world, but it is anticipated that many new regulations could further drive the growth of the Cybersecurity Industry as a whole.

The European Cybersecurity industry employed 909,585 citizens in 2016. Based upon an annual growth of 17.5% since 2015, it is anticipated that during 2017 over 1 million people will be working in the Cybersecurity industry in Europe. With nearly 60,000 companies servicing the market, the European Industry could be considered highly fragmented. However, this is similar to the global Cybersecurity market. Physical infrastructure, including the expansion of existing infrastructure and the continuous upgrading of existing networks and infrastructure, is an important component of expenditure. Managed services and application security services are also showing continuous growth.

The Cybersecurity market is being serviced today both by pure play Cybersecurity providers, traditional ICT technology and services providers and traditional Security products and services providers. Major domains of interest continue to be Identity and Access, Situational Awareness, Application Security, System Recovery, Business Continuity, Encryption and Anti-Malware. Five European Member States generate over 75% of the total European market. The UK is the second largest market in Europe, but is mostly trading outside of Europe.

Overall Conclusions

The global Cybersecurity market has grown rapidly over the last 3 years (above 18%) with the number of global companies and employment growing at the same rate, and is forecast to continue growing rapidly at a similar rate out to 2021. The **global Cybersecurity market has grown rapidly across all sub-sectors** over the last 3 years, varying from 5% for Training and Education to 25% for Identity and Access and for Outsourced/ Managed Services in 2015/16. Each Cybersecurity sub-sector is forecast to continue growing rapidly at similar rates (above 10% per annum to 2021 except for Training and Education).

Considering investment, it is clear that most investment overall has been going into technologies and supporting advisory services, such as integration, whilst training and education was clearly not in balance with this investment in overall architecture. This has been a trend for over the last 3 years, and is set to continue. Most investment has gone into Situational Awareness, with related activities in systems, technologies, services and people supporting a better understanding of the information related to Cybersecurity incidents.

On a global basis, with less than 1% spent in training and education, and overall less than 5% for direct services (in combination with consultancy and managed services), it is clear that Cybersecurity has mainly been a technology market. While it is likely that additional **Training and Education** will be included in many cases with products and services, it is clear that there is a **significant underspend in comparison**. It should be **highly recommended to facilitate the further development of resources of Training and Education, positively support investment in educating people and taking structural measures to improve overall skills and capabilities**, as they are considered to be a key component in the Cybersecurity challenge.

Considering sales, the **USA is the dominant country in terms of global sales** (25.3%) followed by China (9%), Japan (8.3%) and Germany (5.7%). Forecast growth rates for the top 20 countries in sales terms to 2020 are all above 10% per annum, varying between 10-11% for South Korea through to 19.6-21.2% for Taiwan and 35-38.5% for Pakistan. The USA and Germany are forecast to grow faster (13.2-14.5%) than all of the other Top 20 countries apart from Taiwan and Pakistan.

In Sales terms the **EU (including the UK) represented 26% of the global market in 2016, above the USA** at 25%, **making the EU the single largest Cybersecurity market in the world when integrated effectively into a single market**. If this representation of the EU as a single player can be consolidated, and further reinforced by additional measures in the EU to strengthen European Cybersecurity companies in Europe, it would be anticipated that this would support the increased representation of European companies in global markets.

A European Digital Single Market for Cybersecurity could then be considered as a powerful trade entity. Considering the differences in growth areas, there are multiple growth opportunities within the EU (Germany, UK, Austria, Belgium, ...) and throughout Europe as there are opportunities for European companies to seek out to other global market opportunities both from a historical perspective (Chile, UAE, ...) and from a forecasted growth perspective (South Korea, Russia, South Africa, ...). During the workshops (see also Chapter 0), participants from the various European Member States recommended stronger activity from the European market players in other global markets. **EU Cybersecurity companies should be encouraged to reap the potential benefits of the anticipated further global growth of Cybersecurity products and service until 2021. The EU should consider actively and proactively taking actions to encourage the development of an EU Digital Single Cybersecurity market**, also utilising this strategy in international trade relations beyond diplomacy, to prevent risks and dangers from cybercriminal activities happening from and within the EU.

The EU Cybersecurity market has **grown rapidly** over the last 3 years (**above 17%**) with the number of EU companies and EU employment growing at the same rate, and is forecast to continue growing rapidly at a similar rate to 2021. The forecast growth rates to 2021 are significantly higher (above 19%) for Germany and the UK than other Member States. Since these Member States (Germany, UK, France, Italy, Spain, the Netherlands and Belgium) are contributing most to the EU Cybersecurity market, the gap in absolute terms between these countries and the other European countries will continue to exist and grow further.

Considering regional differences in the EU, it was confirmed during the workshops that many Eastern European countries are lagging behind in terms of maturity of Cybersecurity in terms of number of companies and local expertise, innovation and market acceptance. While in Western European markets, many companies and governments have included Cybersecurity policies and deployed Cybersecurity products and services, supporting the development of the local markets, these aspects are only just being considered in many other parts of Europe. These Member States may be able to learn and adopt best practices from the leading European Member States, and should be stimulated to work more closely with market leaders and innovators from the more mature Member States.

It appears that **more mature Cybersecurity Member States** (in terms of the Cybersecurity market size, number of companies and employment, and on a per capita basis as per description in the next paragraphs), tend to have a slightly different spending pattern, indicating that less is being spent in preventive measures (Situational Awareness, Identity and Access, Encryption) than in mitigation and remediation measures (System Recovery / Data Cleansing).

Considering the size of Cybersecurity companies, the average number of employees is 15, but this varies across the EU from 8 in the UK to over 40 in Estonia, Ireland, Latvia, Bulgaria and Luxembourg. From trends in company size from 2014 to 2016, it can be seen that, as the EU Cybersecurity market has developed and sales have grown, the average size of a Cybersecurity company across the EU has fallen, though not substantially, with small falls in most Member States. In addition, the largest economies tend to have lowest average company size, as they have more extensive and more mature ecosystems with a higher proportion of small companies. Overall in the EU Cybersecurity companies comprise 39% micro, 35% small, 18% medium and 8% large companies: these proportions are almost identical at the global level. However, the distribution of company sizes varies significantly across Member States, e.g. micro-companies are 32% of companies in Denmark through to 44% in Germany.

It also appears that the level of fragmentation of some markets provides an indication of the level of maturity of Member States. While this is not shown by the quantitative data, more innovative and new companies are being formed in countries like UK, while in less mature Member States a higher level of concentration seems to appear, at least temporarily. During the workshops, a recurring theme for discussion was the high number of companies throughout Europe and the high employment numbers in comparison to the expectations of the participants. Concerns were expressed about this resulting high level of fragmentation of the market, as a result of these many companies, which are especially in the more mature markets (and the countries relatively contributing more to the European Cybersecurity market). Therefore an overall recommendation from all workshops was to develop companies that could be considered European Cybersecurity market leaders, supporting them to become more prominent and possibly larger and stronger to participate on a global scale.

Europe is the location for the corporate headquarters of 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia.

Cybersecurity activities and companies have not emerged primarily from the ICT sector, but from across a range of market sectors. Looking at the sectors involved in delivering Cybersecurity products and services for the EU in 2016, 31% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 22% originates from companies whose core business is ICT, 19% originates from companies whose core business is Defence/ Aerospace and 13% from companies whose core business is Security.

It should be recommended that in countries where there is a significantly higher contribution from Cybersecurity companies (Denmark, Latvia, Greece), these companies can be additionally supported from a European level to get a better appreciation in other countries. At the same time, in countries, where other traditional industries are contributing more significantly to the Cybersecurity market (Belgium, Sweden, Germany somewhat) the benefits of these pure play companies should be reaped to support the traditional system integrator and security domains.

It should also be highly recommended to further investigate the impact of Cybersecurity technologies into the Defence domains and conversely, to reap the benefits of dual use. Many large companies that can be attributed to the Defence category, can start to further integrate some of the pure play Cybersecurity company offerings on a global basis and as a result further strengthen their global position. This should be further supported at both Member State and European level.

Considering now the EU End User markets, in sales terms this comprises **Private users (45% of sales), Public users (31%) and “Other” users (25%)**. The “Other” category is large because it includes retail activities (10%) and un-attributable activities (10%). The Public sector Cybersecurity market ranges between 24% (Germany) to 48% (UK) and the Private sector Cybersecurity market ranges between 41% (Austria) to 49% (Czech Republic, France and Poland).

EU Country Cybersecurity Industry Market imports as a share of their average domestic market size vary from 3.1% for the UK to above 25% for Bulgaria, Romania, Portugal, Czech Republic, Latvia, Estonia, Hungary. However, some of these imports into EU countries come from other EU Member States. The EU, as a whole, only imports 5.3% of its Cybersecurity products and services from non-EU sources.

The value of imports and import intensity (imports as a percentage of the domestic market) can be used to analyse current EU market share of international country markets, EU competitiveness compared with USA and China and can also be used to estimate international (as opposed to domestic and EU) market opportunities. This specific analysis of national imports (from outside of the EU), linked with current EU export performance can be seen as the basis for EU competitive performance.

The percentage of imports into each Member State from within the EU (as opposed to outside the EU) varies significantly by country, from 17% for the UK through to 53% for France (2016 figures). Member States on average import 30% of products/ services from other EU countries and 70% from outside the EU: their EU imports range from 20% for Encryption and Outsourced/ Managed Services through to 32% for Situational Awareness and System Recovery and Data Cleansing.

Given the significant amount spent by the public sector in Cybersecurity (EUR 48,831 million), and both relative and absolute differences between the Member States (46% and 49% public spending respectively in Belgium and Poland for instance), or given the variations in imports from outside of the EU both relatively and absolutely between the Member States (France spending more on import from within EU, vs Denmark doing mostly imports from outside of EU) – some specific policies and recommendations towards a more proactive European Cybersecurity import policy can be proposed, as well as strengthening the position of the EU Cybersecurity companies globally.

The EU Member States with the **highest export intensity** (proportion of exports to sales generated within their borders) are **Croatia (14%), Estonia and Germany (10%)**, Latvia and Bulgaria (9%), and the UK, Cyprus, Austria and Slovenia (7%). The countries with the lowest proportions of exports to sales

are Romania, Hungary and Sweden (1%), and Denmark, Netherlands, Finland, Spain and Czech Republic (2%).

The importance of the UK in this analysis should be noted. The trade deficit on the Cybersecurity Industry might drop, as a result of Brexit. However, the UK is not contributing significantly to importing from the EU markets. UK is a significant player on the export market, as it contributes to nearly EUR 2.4 billion of the total of EUR 9.7 billion in exports (81% of it for outside the EU).

The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective.

Similarly, by comparing region/country domestic demand with imports it is possible to analyse to what extent the EU and other competing regions/ countries meet their Cybersecurity needs by imports rather than from internal suppliers. The US imports 4.2% of its domestic demand, India 4.5%, Japan 4.6%, the EU 5.3% and China 6.1%. China has the highest imports as a share of domestic demand followed by the EU.

However, although the EU only imports 5.3% of its domestic demand (2016 figures), the proportion of EU demand met by international companies from sales by operations established within the EU lies between 21-25% (2016 figures) depending on how much of the international company sales activity in the EU is exported outside the EU. **If one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the 'effective' imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.**

While the US continues to be the EU's main competitor in global markets (followed closely by China), China is the main competitor in EU markets and specifically in the smaller EU countries. There are some growth markets where EU is a stronger exporter than US, and close to China, such as South Korea, Indonesia, Russia and South Africa which could form an opportunity for a more coordinated EU export policy in Cybersecurity products and services.

From the workshop discussions, none of the participants indicated to be directly impacted from imports in EU or beyond EU from China. However, in all cases the tendency was **the direct impact in both local and international markets on imports from the US**. It could be expected that there will be an impact from the earlier announced Cybersecurity package¹⁹ in which the EU intends to put in place Cybersecurity certification regimes on the Member States. Such a certification mechanism, intended to increase the security of ICT products and services (including Cybersecurity products and services) might have an adverse effect on the imports from outside of EU. However, at the same time, given the current level of imports from outside of EU, such a regime might also have an adverse effect on the security of the EU markets in the case these certification schemes might become too complex and difficult and become a strong barrier for US and Chinese Cybersecurity products and services to be imported, if no EU certified Cybersecurity products and services exist as potential replacements.

As indicated in the earlier sections, there are major differences in importing trends amongst EU countries, which could be more streamlined from an EU perspective and therefore improve the overall EU performance as a Digital Single market on a global scale. Adding to that the further improvement

¹⁹ https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

and focus to some of the key EU export regions, by focusing international policies and collaboration agreements on Cybersecurity policy collaboration and joint research programs, this could further lead to an increase for EU Cybersecurity companies to play a more significant role in these countries.

During some workshops it was noted that some countries (like Sweden, Poland) are not so active in Cybersecurity exports, while the Member States are very active in Defence and Security activities on a global basis. It was recommended to investigate the use of existing capabilities of Member States in their international trade to the benefit of other Member States' capabilities in Cybersecurity products and services. Those Member States could as a result also increase their own Cybersecurity capabilities, by supporting the development of EU Cybersecurity companies locally.

Finally, the potential impact should be investigated of developing an international trade scheme for Cybersecurity, similar to existing trade schemes on Defence and Security products and services. It is likely that those could be further extended to Cybersecurity. From earlier analysis of the contributing sectors to the Cybersecurity markets, from an export perspective the EU should be supporting the dual use of Cybersecurity products and services : promoting the use of the same technologies for civilian and defence purposes.

Priorities and Needs

Cybersecurity in Europe should no longer be considered as part of the traditional IT or ICT domain, nor of the Security domain, but should be considered as an independent domain with its specific needs and priorities. Whilst the Cybersecurity supply is relatively mature, the European Cybersecurity demand is still relatively immature. Both its complexity and the resulting barriers of costs and resources continue to be challenges for organizations to adopt Cybersecurity.

It is anticipated that many of the new and developing European regulatory frameworks such as GDPR, NIS Directive, PSD2, .. imply putting in place additional security measures. Their requirements will further increase the demand and grow the Cybersecurity Industry as a whole, but it is questionable whether the European Cybersecurity Industry is capable of serving this increased demand, both in size and with sufficient innovative solutions. This is partially the result of regulations being developed independently of the developing industry as a whole. Many of the current needs are being served with existing solutions and technologies, due to lack of support and maturity of some innovative European suppliers. Many of the new solutions are not finding their way into the market, or lack the speed to scale up, or confidence that they offer the right solutions to the existing challenges. Due to this uncertainty, the anticipated market needs are being supplied by traditional providers. In order to be able to fully support the demand, the Cybersecurity Industry needs to be supported and guided to ensure that these regulatory transformations can be successfully adopted. In general, the adoption of the Cybersecurity Industry to the regulations is equally hard as for any other organization operating in Europe.

The need to find and develop resources is a challenge common to any growth market. Even with 1 million citizens participating in Cybersecurity in Europe, there is a continuous scarcity in skilled professionals. Cybersecurity continues to be limited to higher education or self-study. Commercial training programs are available, but the European Cybersecurity Industry has to rely upon a wide variety of self-certification mechanisms, totally unrelated to the European regulatory requirements.

Increasingly the ICT sector and the Cybersecurity industry are being challenged with an increased demand of security warranties and standardization efforts. But like any other, the Cybersecurity Industry is challenged by insecure infrastructures, legacy systems and the need to harden solutions. The Cybersecurity Industry needs to have infrastructure operators to be equally knowledgeable and

responsible when setting requirements, implementing insecure components and carelessly operating them.

Finally, with the public sector already being one of the largest Cybersecurity Industry markets today, public authorities continue to have a responsibility in leading by example in Cybersecurity. Governments and public administrations should be putting in place Cybersecurity managers and coordinators ensuring data protection and incident response, in close collaboration with their peers and the Cybersecurity Industry.

Recommendations to be considered from the CIMA analysis findings

The following recommendations are proposed drawing on specific results from the quantitative analysis of the CIMA data and are complementary to the qualitative recommendations from the workshops. Key results and associated recommendations based on these results are listed below:

1) Coordinated EU export support in areas where there is strong export competition with international competitors (Situational Awareness and System Recovery and Data Cleansing, followed by Infrastructure, Identity and Access and Application Security etc) should be considered. The EU exports are only 3.9% of its sales activities, compared to 6.3% for the US and Japan, 10.1% for India, 18.1% for Japan, and 26.2% for China. EU exporting activity is much lower than competitors relative to the sales activities delivered from within its borders: the EU is not achieving its export potential when judged from this economic perspective.

2) There are some growth markets where the EU is a stronger exporter than the USA, and similar to China, such as South Korea, Indonesia, Russia and South Africa, which could form a strong opportunity for a more coordinated EU export drive in Cybersecurity products and services. There are also potential opportunities from a forecast growth perspective (such as Pakistan and Taiwan). The USA continues to be the EU's main competitor in global markets followed closely by China.

3) A more strategic approach to public sector expenditure on Cybersecurity could have a significant impact on the European Cybersecurity market and strengthen the positioning of EU Cybersecurity companies globally. Public Procurement could be split into two: (1) for commodity purchasing, (2) strategic with an industrial policy. Public sector expenditure by the EU public sector in Cybersecurity is substantial (EUR 48,831 million or 31% of the market) and so public procurement policies can significantly influence the Cybersecurity market.

4) Any measures that help smaller EU countries access EU sources of supply will help to improve EU competitiveness overall. While the USA is the EU's main competitor in global markets (followed closely by China), China followed by the US is the main competitor to EU suppliers in EU markets and specifically in the smaller EU countries.

5) Further study should be considered to examine the implications and impact of the significant EU dependence on International suppliers on the EU Cybersecurity market, for example what the benefits and disadvantages of such international Cybersecurity investment in Europe are. Although the EU only imports 5.3% of its domestic demand (2016 figures), the proportion of EU demand met by international companies from sales by operations established within the EU lies between 21-25% depending on how much of the international company sales activity in the EU is exported outside the

EU. If one combines Cybersecurity imports from outside the EU with Cybersecurity sales made by International companies from operational bases established within the EU, the ‘effective’ imports from international companies headquartered outside the EU are between 26-30% of demand in 2016.

6) Further study of the impact of Cybersecurity technologies in the Defence domain and their relationship to Cybersecurity activities for other applications, to investigate measures that would help the EU obtain the full benefits of dual use, should be considered. Cybersecurity activities and companies have not emerged solely from the ICT sector, but from across a range of market sectors. Looking at the sectors involved in delivering Cybersecurity products and services for the EU in 2016, 34% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 24% originates from companies whose core business is ICT, 20% originates from companies whose core business is Defence/ Aerospace and 14% from companies whose core business is Security. There are for example potential synergies between Defence and Security trade activities and Cybersecurity trade activities that could be exploited, to the benefit of Member State Cybersecurity companies. It should be investigated what the potential impact could be on developing an international trade scheme for Cybersecurity, similar to existing trade schemes on Defence and Security products and services. It is likely that those could be further extended to Cybersecurity.

7) The apparent low EU investment in Cybersecurity Training and Education, and slow growth in the EU Training and Education market compared to other sub-sectors, highlights the need for EU investment including structural measures to improve overall EU skills and capabilities. Each EU Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum out to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%. While it is likely that additional Training and Education will be included in many cases with products and services, it is clear that there is a significant underspend in comparison to other sub-sectors, such as Infrastructure, Situational Awareness and Application Security.

Recommendations to be considered from the discussions and workshops

The following recommendations were drawn from a series of MS workshops including with ECSO on the position of the Cybersecurity PPP related to the recent Cybersecurity Package and should be considered going forward. In some cases (public procurement, trade promotion) they reinforce and add to the above recommendations that are based on quantitative data analysis. Key views and suggestions by participants can be summarised as follows:

1. Create and support a European industrial policy for Cybersecurity, supporting the Cybersecurity Industry, as an integrated component of the Digital Single Market, associated with the European Cybersecurity Strategy
 - a. Ensure the development of an industrial policy for Cybersecurity in the Member States, in line with the European policy.
 - b. The European Cybersecurity Industry policy should recognize the existence of the European **Cybersecurity Industry as a whole**, and the specific European Cybersecurity suppliers.
 - c. The policy should **recommend that public procurement supports European industry**.
 - d. Cybersecurity clusters exist in a number of Member States and represent the views of small and large businesses and academia. Their views should be sought to inform MS and EC policy.
2. Ensure the use by the European institutions and Member States and ensure the success of the PPI instruments by **using Public Procurement for Innovations** in Cybersecurity in close collaboration with the Cybersecurity Industry and the Cybersecurity PPP ECSO.

- a. To encourage the innovative SME sector, the EC and MS governments **should lead by example in public procurements**, and mandate that all bids with Cybersecurity content contain a defined SME proportion.
 - b. National MS standards should be prohibited for all public procurements.
3. A series of European initiatives have led to the development of Cybersecurity centres of excellence. This should be strengthened by:
 - a. Supporting the development and growth **at European level and by the Member States of regional and local** Centres of Excellences such as the Cybersecurity clusters, by guaranteeing their independence as intermediaries by means of specific projects or financing.
 - b. Developing a European Centre of Excellence and further empowering the development of a **NIST-like organization**, providing recommendations, putting in place joint industrial developments and sandboxing environments, setting standards in conjunction with regulatory developments.
 - c. Supporting the development and existence of large European Cybersecurity market operators, by ensuring they receive parts of public procurement and in return demanding the inclusion of independent European Cybersecurity Products and Services Innovators.
 - d. Continuing to support the development and interactions with the Cybersecurity PPP ECSO, and identifying it as a Cybersecurity Centre of Excellence.
4. A **continuous dialogue with regulators**, authorities and policy makers should lead to providing more clarity in the interpretation of the regulations and guidance towards its implementation. These dialogues should have an impact on the final interpretation of the regulations and directives. They should be considered as further guidelines in a court of law.
5. In addition, in order for the regulatory changes to be successfully adopted by the majority of organizations, additional efforts are required from both regulators, the EC and the Member States in terms of awareness and further guidance and clarifications. These actions should be implemented in a coordinated way together with the Cybersecurity Industry.
6. The EC should define dynamic baseline requirements for certification schemes and standards for products, services, people and other components. A single set of approval criteria for Cybersecurity products and services that applies across the EU would allow Member States to run their own schemes built on a common agreement while encouraging inter-MS trading. These schemes should be on a self-certification basis, but built upon the standards set by the EC, on a rolling basis. Suggested specific measures could include:
 - a. Creating EU wide standards for Cybersecurity that are mandated for public procurement and seen as best practice by other purchasers. These (through different inter-locking standards) should cover all aspects of Cybersecurity including:
 - i. Product standards
 - ii. Qualification recognitions
 - iii. Service provision
 - b. To support exports, these standards should also be rationalised with existing or emerging International standards.
 - c. Certification costs should be constrained by cost reduction mechanisms or otherwise reduced by government action, for example by developing Certification Centres to approve “products” against EU-wide standards in a cost effective and timely manner.
7. The EC should further **ensure the organization and support of a lively investor interest** which includes the financial support of an incubator platform in the 10 leading European markets, and financial instruments for innovative Cybersecurity investors supported through co-investment mechanisms. In addition, recognising that venture funding is risk averse which constrains growth, it is recommended that the Venture Capital market be stimulated by the

provision of significant tax incentives for higher risk investments. These instruments and mechanisms should be additionally promoted through the existing Cybersecurity incubators and regional Cybersecurity clusters.

8. Similar to the mechanisms used in other industries, **balancing the international trade between Europe and other markets**, the EU should further empower some of the European technology developers to further drive the growth of the domain in Europe and lower the dependencies on non-European markets such as the USA and China.
9. Specific activities should be undertaken to support the international trade to existing identified markets, by specific promotional activities such as Cybersecurity made in Europe, promoting the expertise and innovations made in Europe within and beyond European borders. This activity should be aligned to the support of a European directory of self-certified companies and products, supported by the Member States, to be guided through solutions for existing and upcoming regulatory frameworks.

Many components of the recommendations are achievable within two years upon the installation of the policy, some of them taking an immediate effect. The estimated additional efforts needed are mainly the result of redirection of some of the existing resources and budget (such as public procurement), existing investment capabilities (from PPI mechanisms and co-investment mechanisms). Additional resources will be needed to further support the local initiatives and promotional activities of Cybersecurity awareness and improve the take-up of the regulatory schemes by the Cybersecurity industry itself. For the international promotional campaigns, it would be anticipated that an additional budget for co-investment for international trade would amount to 10 million EUR on an annual basis. The total estimated additional budget required to support the further growth of the European Cybersecurity Industry is estimated to be EUR 80 million up to 2022. In conjunction with the recommended and adapted policies on national level, this could lead to an annual increase of EUR 2 billion for EU Cybersecurity Industry.

The presented recommendations are expected to further increase the demand in Europe and beyond Europe for Cybersecurity products and services. It is anticipated that the current estimated growth rate underestimates the real market potential, and that growth rates of up to 20% on an annual basis can be achieved with an active policy. These would amount to an annual growth of over EUR 30 billion of which an annual EUR 5 billion in additional export trade could be expected. This additional growth will need to be supported by a similar growth rate in the number of employees participating in the Cybersecurity Industry for at least the next 3 years. Existing mechanisms are being put in place to further automate the Cybersecurity challenge by supporting the existing experts, as well as the further growing of the existing skill sets and experts serving them.

These recommendations will be essential for a European Cybersecurity market to continue to flourish in the next 3 to 5 years and further drive the growth of the Cybersecurity markets beyond the European borders.

Appendix A : EU Country Level Data

Introduction

The following tables show three levels of Cybersecurity data and three metrics (sales, employment and forecast growth) for each country.

At three levels of disaggregation the data becomes extremely granular, especially for the smaller sub-sectors of Cybersecurity.

The logic in the following tables is:

- If a country activity has a sales value, it will have an associated growth forecast
- If a country activity has no sales value, no growth forecast is shown
- If a country activity has a sales value it *may* have an employment value associated with it, but if the sales value is very small then the employment value may appear as zero (to prevent double counting employment across multiple market activities).

This is especially true of activities in the “Training & Education” sub-sector, which has been split out as a separate sub-sector for the first time for the CIMA research. Previously, “Training & Education” activities were incorporated within the existing 12 sub-sectors on the assumption that these activities were often implicit in, or associated with, the delivery of new systems and software. It is difficult to fully separate out the employment element for “Training & Education” from activities like Consultancy, or installation/ maintenance and, as a result, some employment values may be understated.

Individual Member State data

Data for each individual Member State are presented, in alphabetical order, in the following Sections.

1.1.44 Austria

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	6.49	50	4.2	4.3	4.4	4.6	4.7	4.8
Anti Malware	Anti Virus/Worm	39.62	286	9.5	9.7	10.0	10.3	10.6	10.9
Anti Malware	Malware	6.11	33	5.0	5.1	5.2	5.4	5.5	5.7
Anti Malware	Specialist Anti Malware	136.79	446	14.2	14.7	15.2	15.6	16.0	16.6
Application Security	Application Code Security	6.51	42	4.4	4.5	4.6	4.8	4.9	5.1
Application Security	Content Filtering & Monitoring	5.21	38	6.9	7.1	7.3	7.5	7.8	8.0
Application Security	Patch Management	4.81	36	5.2	5.3	5.5	5.6	5.8	6.0
Application Security	Vulnerability Assessment	502.15	1679	15.7	16.2	16.7	17.2	17.7	18.2
Business Continuity	Business Continuity/Recovery	25.86	86	17.3	17.9	18.5	19.0	19.6	20.2
Business Continuity	Computer Forensics	14.32	100	20.5	21.2	21.4	21.8	22.1	22.4
Business Continuity	IT/Cyber Forensics	244.61	739	16.0	16.5	16.9	17.3	17.9	18.5
Cyber Consultancy	Access Management	0.78	4	7.1	7.3	7.4	7.7	7.8	8.1
Cyber Consultancy	Anti Spam Solutions	0.62	1	5.9	6.0	6.2	6.4	6.6	6.8
Cyber Consultancy	Anti Virus/Worm	0.47	0	5.0	5.1	5.3	5.5	5.7	5.8
Cyber Consultancy	Application Code Security	0.55	4	3.9	4.0	4.1	4.2	4.3	4.5
Cyber Consultancy	Business Continuity/Recovery	0.45	3	4.5	4.7	4.8	4.9	5.1	5.2
Cyber Consultancy	Computer Forensics	0.82	6	5.2	5.3	5.5	5.6	5.8	6.0
Cyber Consultancy	Content Filtering & Monitoring	0.39	1	4.8	4.9	5.1	5.2	5.3	5.5
Cyber Consultancy	Corporate Services	32.80	233	23.8	24.5	24.8	25.1	25.5	25.8
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.65	4	5.5	5.7	5.9	6.0	6.2	6.3
Cyber Consultancy	Firewalls	0.23	0	6.2	6.3	6.5	6.7	6.9	7.1
Cyber Consultancy	Identity Management	0.98	5	6.1	6.3	6.5	6.7	7.0	7.2
Cyber Consultancy	Intrusion Detection	0.62	1	5.7	5.8	5.9	6.1	6.3	6.5
Cyber Consultancy	Malware	0.69	4	6.3	6.5	6.6	6.8	7.1	7.2
Cyber Consultancy	Messaging Security	0.80	4	4.8	5.0	5.1	5.3	5.4	5.6
Cyber Consultancy	Mobile Security/Device management	0.77	5	3.7	3.8	3.9	4.1	4.2	4.3
Cyber Consultancy	Patch Management	0.60	1	5.2	5.4	5.6	5.7	5.8	6.0
Cyber Consultancy	PC/Mobile/End Point Security	0.44	1	5.6	5.8	5.9	6.0	6.3	6.5
Cyber Consultancy	Vulnerability Assessment	0.67	4	5.2	5.4	5.5	5.7	6.0	6.1
Cyber Consultancy	Wireless Security	0.50	1	7.3	7.5	7.7	8.0	8.3	8.5
Cyber Security Insurance	Business Interruption from Network Downtime	11.85	84	10.9	11.2	11.5	11.9	12.2	12.6
Cyber Security Insurance	Cyber Extortion	10.30	77	10.8	11.1	11.4	11.8	12.1	12.4
Cyber Security Insurance	Investigation of Privacy Breach	2.68	19	11.3	11.7	12.0	12.3	12.6	13.0
Cyber Security Insurance	Loss of Third Party Data	14.66	107	10.7	11.0	11.3	11.7	12.1	12.4
Cyber Security Insurance	Loss or Damage to Digital Assets	10.56	73	10.9	11.3	11.7	12.0	12.4	12.8
Cyber Security Insurance	Multi-Media Liability	9.24	65	10.4	10.7	11.1	11.4	11.7	12.1
Cyber Security Insurance	Reputational Damage	5.26	36	10.1	10.4	10.7	11.0	11.3	11.6
Cyber Security Insurance	Security and Privacy Breaches	14.32	97	10.8	11.2	11.5	11.8	12.1	12.5
Cyber Security Insurance	Theft of Money and Digital Assets	7.87	55	10.5	10.8	11.1	11.5	11.8	12.1
Cyber Security Insurance	Third Party Breach Notification	5.29	35	11.0	11.4	11.8	12.1	12.4	12.7
Encryption	Digital Signatures	11.11	74	27.4	28.2	28.4	28.9	29.4	29.9
Encryption	Encryption/PKI/Digital Certificates	9.79	61	16.0	16.6	16.8	17.2	17.3	17.5
Encryption	Storage Security, including Cloud	20.47	144	26.2	27.2	27.6	27.9	28.4	28.7
Identity & Access	Access Management	15.20	78	7.0	7.2	7.4	7.6	7.8	8.0
Identity & Access	Authentication	26.37	186	29.3	30.2	30.6	30.9	31.4	31.8
Identity & Access	Identity Management	91.18	590	23.6	24.3	24.7	25.0	25.3	25.7
Identity & Access	Intrusion & Anomaly Prevention	12.14	92	28.7	29.6	30.0	30.5	30.9	31.3
Identity & Access	Messaging Security	34.26	211	12.5	12.9	13.1	13.4	13.5	13.8
Infrastructure	Data Management	21.75	161	19.9	20.5	20.8	21.0	21.3	21.6
Infrastructure	Firewalls	10.77	64	5.6	5.8	5.9	6.1	6.3	6.5
Infrastructure	Infrastructure Monitoring	10.63	77	27.4	28.4	28.6	29.1	29.4	29.9
Infrastructure	Infrastructure Resilience	11.37	88	31.1	32.2	32.6	32.9	33.4	33.9
Infrastructure	Intrusion Detection	713.33	2242	18.4	18.9	19.4	19.8	20.3	20.8
Infrastructure	Outsourced/Managed Services	12.03	106	28.7	29.7	30.2	30.6	31.0	31.4
Infrastructure	Storage Security, including Cloud	37.38	259	28.7	29.7	30.1	30.4	30.8	31.1
Mobile	Mobile Security/Device management	18.21	124	5.8	6.0	6.2	6.4	6.6	6.8
Mobile	PC/Mobile/End Point Security	11.54	58	10.0	10.3	10.7	11.0	11.4	11.7
Mobile	VPN	12.73	89	28.5	29.1	29.5	29.7	30.2	30.5
Mobile	Wireless Security	15.61	98	5.5	5.6	5.8	6.0	6.2	6.4
Outsourced/Managed Services	Access Management	0.15	0	7.0	7.3	7.5	7.7	7.9	8.2
Outsourced/Managed Services	Anti Spam Solutions	0.10	0	6.1	6.3	6.5	6.7	6.9	7.1
Outsourced/Managed Services	Anti Virus/Worm	0.17	0	4.6	4.8	4.9	5.1	5.2	5.3
Outsourced/Managed Services	Application Code Security	0.31	0	5.5	5.7	5.9	6.1	6.2	6.4
Outsourced/Managed Services	Business Continuity/Recovery	0.10	0	8.2	8.4	8.6	8.8	9.1	9.4
Outsourced/Managed Services	Content Filtering & Monitoring	0.18	0	8.0	8.2	8.5	8.7	8.9	9.2
Outsourced/Managed Services	Cyber Services	38.18	267	27.2	28.1	28.4	28.7	29.0	29.4
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.23	0	5.8	6.0	6.2	6.4	6.6	6.8
Outsourced/Managed Services	Firewalls	0.23	0	4.4	4.6	4.7	4.8	4.9	5.1
Outsourced/Managed Services	Identity Management	0.64	1	6.0	6.2	6.4	6.6	6.8	6.9
Outsourced/Managed Services	Intrusion Detection	0.16	0	4.6	4.7	4.8	4.9	5.0	5.1
Outsourced/Managed Services	Malware	0.05	0	5.1	5.3	5.5	5.6	5.8	6.0
Outsourced/Managed Services	Messaging Security	0.32	0	6.5	6.6	6.8	7.1	7.3	7.5
Outsourced/Managed Services	Mobile Security/Device management	0.28	0	5.0	5.1	5.3	5.4	5.6	5.7
Outsourced/Managed Services	Patch Management	0.14	0	6.5	6.7	6.9	7.1	7.3	7.5
Outsourced/Managed Services	PC/Mobile/End Point Security	0.16	0	6.0	6.2	6.3	6.5	6.7	6.9
Outsourced/Managed Services	Vulnerability Assessment	0.22	0	4.0	4.1	4.3	4.4	4.6	4.7
Outsourced/Managed Services	Wireless Security	0.21	0	6.0	6.2	6.3	6.5	6.7	6.9
Situational Awareness	Darkweb	2.51	17	9.8	10.0	10.1	10.3	10.4	10.6
Situational Awareness	External Cyber Threat Intelligence	173.96	608	17.3	17.9	18.2	18.5	18.8	19.2
Situational Awareness	High Level Situational Awareness	154.17	612	13.8	14.3	14.7	15.1	15.6	16.0
Situational Awareness	Internal Cyber Threat Intelligence	25.44	63	14.4	14.9	15.1	15.4	15.7	15.9
Situational Awareness	Low Level Situational Awareness	150.26	479	14.7	15.1	15.6	16.0	16.5	17.0
Situational Awareness	Media Monitoring	12.34	81	9.8	10.0	10.2	10.4	10.5	10.6
Situational Awareness	Proactive Cyber Surveillance	88.90	302	19.4	20.0	20.2	20.5	20.7	21.0
System Recovery & Data Cleansing	Data Recovery Services	122.86	400	18.4	18.9	19.1	19.4	19.7	19.9
System Recovery & Data Cleansing	Manual Data Cleansing	56.13	214	18.0	18.5	18.8	19.0	19.2	19.5
System Recovery & Data Cleansing	System Recovery & Data Cleansing	206.48	717	16.0	16.5	16.7	16.9	17.1	17.4
Training & Education	Access Management	0.26	0	5.7	5.9	6.1	6.2	6.4	6.6
Training & Education	Anti Spam Solutions	0.07	0	6.9	7.0	7.3	7.5	7.7	8.0
Training & Education	Anti Virus/Worm	0.01	0	4.7	4.8	5.0	5.1	5.3	5.5
Training & Education	Application Code Security	0.14	0	4.1	4.3	4.4	4.5	4.6	4.8
Training & Education	Business Continuity/Recovery	0.02	0	3.9	4.0	4.1	4.3	4.3	4.5
Training & Education	Computer Forensics	0.01	0	4.3	4.4	4.6	4.7	4.8	5.0
Training & Education	Content Filtering & Monitoring	0.09	0	6.0	6.2	6.4	6.6	6.8	7.0
Training & Education	Encryption/PKI/Digital Certificates	0.11	0	7.3	7.5	7.8	8.0	8.2	8.4
Training & Education	Firewalls	0.06	0	4.9	5.0	5.2	5.3	5.5	5.7
Training & Education	Identity Management	0.43	1	4.4	4.6	4.7	4.8	5.0	5.2
Training & Education	Intrusion Detection	0.11	0	5.8	6.0	6.1	6.3	6.5	6.7
Training & Education	Malware	0.06	0	6.0	6.2	6.4	6.6	6.7	6.9
Training & Education	Messaging Security	0.18	0	5.1	5.3	5.4	5.5	5.7	5.9
Training & Education	Mobile Security/Device management	0.18	0	5.5	5.6	5.8	6.0	6.2	6.4
Training & Education	Patch Management	0.02	0	5.4	5.5	5.7	5.8	6.0	6.2
Training & Education	PC/Mobile/End Point Security	0.34	1	5.7	5.8	6.0	6.1	6.4	6.5
Training & Education	Vulnerability Assessment	0.09	0	5.7	5.9	6.1	6.3	6.4	6.6
Training & Education	Wireless Security	0.15	0	5.2	5.4	5.5	5.6	5.8	6.0

1.1.45 Belgium

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	9.44	73	7.4	7.6	7.9	8.1	8.4	8.6	
Anti Malware	Anti Virus/Worm	48.19	406	8.9	9.2	9.5	9.7	10.1	10.4	
Anti Malware	Malware	11.91	82	6.4	6.6	6.8	7.0	7.2	7.5	
Anti Malware	Specialist Anti Malware	162.56	624	15.8	16.3	16.8	17.3	17.8	18.4	
Application Security	Application Code Security	7.40	68	5.4	5.6	5.7	5.9	6.1	6.2	
Application Security	Content Filtering & Monitoring	6.18	50	6.1	6.3	6.5	6.7	6.9	7.1	
Application Security	Patch Management	6.50	36	4.5	4.6	4.8	4.9	5.1	5.2	
Application Security	Vulnerability Assessment	856.96	3072	18.0	18.6	19.1	19.7	20.3	21.0	
Business Continuity	Business Continuity/Recovery	24.23	86	13.9	14.3	14.7	15.1	15.5	16.0	
Business Continuity	Computer Forensics	18.36	131	18.4	19.0	19.2	19.5	19.8	20.2	
Business Continuity	IT/Cyber Forensics	442.06	2113	18.3	18.8	19.4	20.0	20.6	21.3	
Cyber Consultancy	Access Management	0.99	8	7.2	7.4	7.7	7.9	8.2	8.4	
Cyber Consultancy	Anti Spam Solutions	0.78	4	6.5	6.7	7.0	7.1	7.4	7.6	
Cyber Consultancy	Anti Virus/Worm	0.71	4	5.3	5.4	5.6	5.7	5.9	6.1	
Cyber Consultancy	Application Code Security	0.67	5	4.4	4.5	4.7	4.8	5.0	5.1	
Cyber Consultancy	Business Continuity/Recovery	0.97	4	6.3	6.5	6.7	6.9	7.0	7.3	
Cyber Consultancy	Computer Forensics	0.80	4	6.1	6.3	6.4	6.6	6.8	7.0	
Cyber Consultancy	Content Filtering & Monitoring	0.77	6	7.7	7.9	8.1	8.4	8.6	8.9	
Cyber Consultancy	Corporate Services	35.49	287	20.3	20.9	21.1	21.5	21.7	22.0	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.77	5	5.6	5.8	6.0	6.1	6.4	6.5	
Cyber Consultancy	Firewalls	0.33	1	4.5	4.6	4.7	4.8	5.0	5.2	
Cyber Consultancy	Identity Management	1.46	8	5.8	5.9	6.1	6.3	6.5	6.7	
Cyber Consultancy	Intrusion Detection	0.66	6	3.5	3.6	3.7	3.8	3.9	4.0	
Cyber Consultancy	Malware	0.93	6	5.2	5.3	5.4	5.6	5.8	5.9	
Cyber Consultancy	Messaging Security	0.73	3	3.9	4.1	4.2	4.3	4.5	4.5	
Cyber Consultancy	Mobile Security/Device management	1.40	10	6.4	6.6	6.8	7.0	7.2	7.4	
Cyber Consultancy	Patch Management	0.80	6	7.2	7.5	7.7	7.9	8.2	8.4	
Cyber Consultancy	PC/Mobile/End Point Security	0.50	3	4.4	4.5	4.6	4.8	4.9	5.1	
Cyber Consultancy	Vulnerability Assessment	0.65	5	4.3	4.5	4.6	4.7	4.8	5.0	
Cyber Consultancy	Wireless Security	0.60	4	7.3	7.5	7.7	8.0	8.3	8.5	
Cyber Security Insurance	Business Interruption from Network Downtime	14.13	94	10.2	10.5	10.9	11.2	11.6	12.0	
Cyber Security Insurance	Cyber Extortion	12.64	93	11.1	11.5	11.8	12.2	12.5	12.9	
Cyber Security Insurance	Investigation of Privacy Breach	4.01	25	12.8	13.2	13.5	14.0	14.4	14.9	
Cyber Security Insurance	Loss of Third Party Data	17.27	120	10.8	11.2	11.5	11.8	12.2	12.6	
Cyber Security Insurance	Loss or Damage to Digital Assets	12.21	84	10.4	10.7	11.0	11.3	11.7	12.1	
Cyber Security Insurance	Multi-Media Liability	12.24	81	10.6	10.9	11.2	11.6	12.0	12.3	
Cyber Security Insurance	Reputational Damage	5.70	41	9.3	9.6	9.8	10.1	10.4	10.7	
Cyber Security Insurance	Security and Privacy Breaches	17.82	126	10.9	11.2	11.6	11.9	12.2	12.6	
Cyber Security Insurance	Theft of Money and Digital Assets	10.81	81	11.7	12.0	12.3	12.7	13.1	13.5	
Cyber Security Insurance	Third Party Breach Notification	6.47	42	9.8	10.1	10.4	10.8	11.1	11.5	
Encryption	Digital Signatures	15.13	103	23.9	24.6	25.1	25.4	25.8	26.1	
Encryption	Encryption/PKI/Digital Certificates	11.54	72	14.4	14.9	15.1	15.3	15.6	15.9	
Encryption	Storage Security, including Cloud	22.43	178	23.4	24.1	24.4	24.7	25.0	25.4	
Identity & Access	Access Management	21.19	197	6.4	6.6	6.9	7.1	7.4	7.6	
Identity & Access	Authentication	32.06	204	27.8	28.5	29.0	29.2	29.6	30.0	
Identity & Access	Identity Management	98.45	662	22.0	22.7	22.9	23.3	23.6	23.9	
Identity & Access	Intrusion & Anomaly Prevention	14.53	98	25.6	26.3	26.7	27.0	27.3	27.5	
Identity & Access	Messaging Security	22.12	114	8.2	8.4	8.5	8.7	8.9	9.0	
Infrastructure	Data Management	25.09	220	16.4	17.0	17.2	17.5	17.7	17.9	
Infrastructure	Firewalls	12.00	101	5.1	5.2	5.4	5.5	5.7	5.9	
Infrastructure	Infrastructure Monitoring	11.16	89	24.1	24.8	25.1	25.3	25.8	26.1	
Infrastructure	Infrastructure Resilience	13.51	115	27.3	28.3	28.6	29.1	29.3	29.6	
Infrastructure	Intrusion Detection	1046.90	4214	18.0	18.6	18.9	19.3	19.7	20.1	
Infrastructure	Outsourced/Managed Services	13.29	137	24.4	25.1	25.5	25.9	26.1	26.5	
Infrastructure	Storage Security, including Cloud	41.57	307	25.8	26.6	26.8	27.2	27.5	27.8	
Mobile	Mobile Security/Device management	25.94	178	6.2	6.4	6.6	6.8	7.0	7.2	
Mobile	PC/Mobile/End Point Security	20.09	114	8.6	8.9	9.1	9.4	9.7	10.0	
Mobile	VPN	13.75	115	25.6	26.3	26.7	27.0	27.3	27.6	
Mobile	Wireless Security	17.11	142	4.4	4.5	4.6	4.8	4.9	5.1	
Outsourced/Managed Services	Access Management	0.25	1	7.7	7.8	8.1	8.3	8.6	8.9	
Outsourced/Managed Services	Anti Spam Solutions	0.12	0	4.6	4.7	4.9	5.1	5.3	5.4	
Outsourced/Managed Services	Anti Virus/Worm	0.25	2	7.1	7.2	7.4	7.6	7.9	8.2	
Outsourced/Managed Services	Application Code Security	0.33	4	4.6	4.8	4.9	5.1	5.2	5.4	
Outsourced/Managed Services	Business Continuity/Recovery	0.10	0	5.1	5.2	5.4	5.6	5.7	5.9	
Outsourced/Managed Services	Content Filtering & Monitoring	0.18	0	7.8	8.0	8.3	8.5	8.8	9.0	
Outsourced/Managed Services	Cyber Services	41.04	325	24.0	24.7	25.0	25.4	25.7	26.0	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.22	1	4.0	4.2	4.3	4.4	4.5	4.6	
Outsourced/Managed Services	Firewalls	0.50	3	5.9	6.1	6.3	6.4	6.6	6.8	
Outsourced/Managed Services	Identity Management	0.56	3	6.2	6.4	6.6	6.8	7.0	7.2	
Outsourced/Managed Services	Intrusion Detection	0.16	1	3.3	3.4	3.4	3.5	3.6	3.6	
Outsourced/Managed Services	Malware	0.04	0	4.8	4.9	5.1	5.2	5.4	5.6	
Outsourced/Managed Services	Messaging Security	0.43	1	6.7	6.9	7.1	7.3	7.6	7.8	
Outsourced/Managed Services	Mobile Security/Device management	0.60	3	9.5	9.9	10.2	10.4	10.7	11.0	
Outsourced/Managed Services	Patch Management	0.16	1	6.9	7.2	7.4	7.6	7.8	8.0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.18	0	5.7	5.9	6.1	6.3	6.4	6.6	
Outsourced/Managed Services	Vulnerability Assessment	0.33	1	4.0	4.1	4.3	4.4	4.5	4.7	
Outsourced/Managed Services	Wireless Security	0.23	0	4.8	4.9	5.1	5.2	5.4	5.6	
Situational Awareness	Darkweb	2.83	19	8.1	8.3	8.4	8.5	8.7	8.8	
Situational Awareness	External Cyber Threat Intelligence	207.83	784	18.4	18.9	19.2	19.5	19.9	20.2	
Situational Awareness	High Level Situational Awareness	178.50	690	13.9	14.3	14.8	15.2	15.7	16.1	
Situational Awareness	Internal Cyber Threat Intelligence	44.70	170	19.1	19.7	20.0	20.2	20.5	20.9	
Situational Awareness	Low Level Situational Awareness	212.73	796	15.6	16.0	16.5	17.0	17.6	18.2	
Situational Awareness	Media Monitoring	13.13	101	8.6	8.9	9.0	9.1	9.2	9.4	
Situational Awareness	Proactive Cyber Surveillance	95.58	284	15.4	15.9	16.1	16.3	16.5	16.7	
System Recovery & Data Cleansing	Data Recovery Services	135.79	489	16.7	17.2	17.4	17.6	17.9	18.1	
System Recovery & Data Cleansing	Manual Data Cleansing	67.62	280	19.1	19.7	19.9	20.1	20.4	20.7	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	299.38	1173	19.0	19.5	19.8	20.1	20.3	20.5	
Training & Education	Access Management	0.33	3	9.2	9.5	9.8	10.1	10.3	10.7	
Training & Education	Anti Spam Solutions	0.11	0	6.9	7.1	7.4	7.6	7.8	8.0	
Training & Education	Anti Virus/Worm	0.01	0	5.2	5.3	5.4	5.6	5.8	6.0	
Training & Education	Application Code Security	0.14	0	6.1	6.2	6.5	6.7	6.9	7.1	
Training & Education	Business Continuity/Recovery	0.11	0	5.9	6.1	6.3	6.4	6.6	6.8	
Training & Education	Computer Forensics	0.01	0	10.4	10.8	11.2	11.5	11.8	12.1	
Training & Education	Content Filtering & Monitoring	0.14	1	8.2	8.4	8.7	8.9	9.2	9.5	
Training & Education	Encryption/PKI/Digital Certificates	0.14	0	5.1	5.2	5.4	5.6	5.7	5.9	
Training & Education	Firewalls	0.07	0	6.3	6.4	6.6	6.8	7.0	7.2	
Training & Education	Identity Management	0.62	4	6.6	6.8	7.1	7.2	7.5	7.7	
Training & Education	Intrusion Detection	0.11	0	5.0	5.2	5.3	5.5	5.6	5.8	
Training & Education	Malware	0.07	0	6.3	6.5	6.7	6.9	7.2	7.3	
Training & Education	Messaging Security	0.20	1	4.4	4.5	4.7	4.8	4.9	5.1	
Training & Education	Mobile Security/Device management	0.34	1	6.2	6.4	6.6	6.8	7.0	7.2	
Training & Education	Patch Management	0.02	0	4.2	4.3	4.5	4.6	4.8	4.9	
Training & Education	PC/Mobile/End Point Security	0.33	3	7.0	7.2	7.4	7.7	7.9	8.1	
Training & Education	Vulnerability Assessment	0.15	0	5.5	5.7	5.9	6.1	6.2	6.4	
Training & Education	Wireless Security	0.25	1	5.2	5.4	5.5	5.7	5.8	6.0	

1.1.46 Bulgaria

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	1.38	7	4.0	4.1	4.2	4.3	4.5	4.6
Anti Malware	Anti Virus/Worm	5.41	26	5.5	5.6	5.8	6.0	6.2	6.3
Anti Malware	Malware	2.53	17	8.3	8.5	8.8	9.0	9.3	9.6
Anti Malware	Specialist Anti Malware	51.51	461	20.1	20.5	21.1	21.7	22.4	23.2
Application Security	Application Code Security	1.42	8	5.5	5.7	5.8	6.0	6.2	6.3
Application Security	Content Filtering & Monitoring	1.15	7	6.3	6.4	6.6	6.8	7.0	7.2
Application Security	Patch Management	0.92	5	4.2	4.3	4.4	4.5	4.7	4.8
Application Security	Vulnerability Assessment	134.03	1116	17.2	17.7	18.3	18.8	19.5	20.1
Business Continuity	Business Continuity/Recovery	6.00	34	18.2	18.8	19.5	20.1	20.6	21.2
Business Continuity	Computer Forensics	2.67	18	10.3	10.6	10.7	11.0	11.2	11.4
Business Continuity	IT/Cyber Forensics	55.59	238	13.5	13.8	14.2	14.7	15.1	15.7
Cyber Consultancy	Access Management	0.18	1	6.6	6.7	7.0	7.2	7.4	7.6
Cyber Consultancy	Anti Spam Solutions	0.10	0	5.8	5.9	6.1	6.3	6.5	6.8
Cyber Consultancy	Anti Virus/Worm	0.15	1	3.6	3.8	3.9	3.9	4.0	4.2
Cyber Consultancy	Application Code Security	0.12	0	6.4	6.6	6.8	7.1	7.2	7.5
Cyber Consultancy	Business Continuity/Recovery	0.14	0	4.3	4.4	4.6	4.6	4.8	5.0
Cyber Consultancy	Computer Forensics	0.14	1	3.0	3.1	3.1	3.2	3.3	3.4
Cyber Consultancy	Content Filtering & Monitoring	0.09	0	4.3	4.5	4.6	4.7	4.9	5.1
Cyber Consultancy	Corporate Services	5.83	40	9.5	9.8	9.9	10.0	10.2	10.3
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.15	1	4.2	4.4	4.5	4.7	4.8	4.9
Cyber Consultancy	Firewalls	0.07	0	5.6	5.7	5.9	6.0	6.3	6.5
Cyber Consultancy	Identity Management	0.23	1	5.0	5.2	5.4	5.5	5.7	5.9
Cyber Consultancy	Intrusion Detection	0.11	1	5.0	5.2	5.3	5.5	5.6	5.8
Cyber Consultancy	Malware	0.14	1	6.1	6.3	6.5	6.7	6.9	7.2
Cyber Consultancy	Messaging Security	0.22	1	6.9	7.1	7.3	7.5	7.7	7.9
Cyber Consultancy	Mobile Security/Device management	0.15	1	6.3	6.4	6.7	6.9	7.1	7.3
Cyber Consultancy	Patch Management	0.11	0	6.5	6.7	6.9	7.1	7.3	7.5
Cyber Consultancy	PC/Mobile/End Point Security	0.10	0	7.5	7.7	8.0	8.2	8.5	8.7
Cyber Consultancy	Vulnerability Assessment	0.12	0	7.2	7.5	7.7	7.9	8.2	8.4
Cyber Consultancy	Wireless Security	0.10	1	5.7	5.8	6.0	6.2	6.4	6.6
Cyber Security Insurance	Business Interruption from Network Downtime	2.93	21	11.0	11.3	11.7	12.1	12.4	12.8
Cyber Security Insurance	Cyber Extortion	2.53	18	11.0	11.3	11.6	11.9	12.3	12.6
Cyber Security Insurance	Investigation of Privacy Breach	0.80	5	10.7	11.0	11.3	11.6	12.0	12.3
Cyber Security Insurance	Loss of Third Party Data	3.78	27	10.5	10.8	11.1	11.4	11.8	12.2
Cyber Security Insurance	Loss or Damage to Digital Assets	2.35	16	9.8	10.1	10.4	10.7	11.1	11.4
Cyber Security Insurance	Multi-Media Liability	2.29	15	10.3	10.6	10.9	11.3	11.6	11.9
Cyber Security Insurance	Reputational Damage	1.24	9	10.4	10.7	11.0	11.3	11.6	12.0
Cyber Security Insurance	Security and Privacy Breaches	3.72	26	11.1	11.4	11.8	12.1	12.5	12.9
Cyber Security Insurance	Theft of Money and Digital Assets	1.93	14	11.3	11.6	11.9	12.3	12.6	13.0
Cyber Security Insurance	Third Party Breach Notification	1.31	9	9.6	9.8	10.1	10.5	10.7	11.1
Encryption	Digital Signatures	1.62	17	11.2	11.6	11.8	11.9	12.0	12.1
Encryption	Encryption/PKI/Digital Certificates	1.76	12	7.5	7.7	7.9	8.0	8.2	8.3
Encryption	Storage Security, including Cloud	3.65	29	11.9	12.2	12.4	12.5	12.7	12.9
Identity & Access	Access Management	3.26	15	5.8	5.9	6.1	6.3	6.5	6.7
Identity & Access	Authentication	4.08	26	11.9	12.2	12.4	12.5	12.6	12.8
Identity & Access	Identity Management	16.09	109	10.4	10.7	10.8	11.0	11.2	11.4
Identity & Access	Intrusion & Anomaly Prevention	2.42	15	12.5	12.9	13.1	13.2	13.4	13.5
Identity & Access	Messaging Security	5.57	24	13.9	14.2	14.5	14.7	14.9	15.1
Infrastructure	Data Management	3.93	27	8.6	8.9	9.0	9.1	9.2	9.3
Infrastructure	Firewalls	2.11	8	4.7	4.8	5.0	5.1	5.2	5.4
Infrastructure	Infrastructure Monitoring	2.08	12	12.1	12.5	12.7	12.8	13.0	13.2
Infrastructure	Infrastructure Resilience	2.13	17	12.7	13.2	13.4	13.5	13.6	13.7
Infrastructure	Intrusion Detection	135.71	682	16.6	17.0	17.3	17.7	18.0	18.3
Infrastructure	Outsourced/Managed Services	1.86	17	11.3	11.7	11.8	11.9	12.1	12.3
Infrastructure	Storage Security, including Cloud	6.08	38	11.7	12.1	12.2	12.4	12.5	12.7
Mobile	Mobile Security/Device management	3.78	15	6.0	6.1	6.3	6.5	6.7	6.9
Mobile	PC/Mobile/End Point Security	3.23	25	9.2	9.4	9.7	10.0	10.3	10.6
Mobile	VPN	1.97	19	13.1	13.5	13.6	13.8	14.0	14.2
Mobile	Wireless Security	1.88	11	4.4	4.5	4.7	4.8	4.9	5.1
Outsourced/Managed Services	Access Management	0.07	0	12.9	13.3	13.7	14.1	14.5	15.0
Outsourced/Managed Services	Anti Spam Solutions	0.01	0	5.0	5.2	5.3	5.5	5.6	5.7
Outsourced/Managed Services	Anti Virus/Worm	0.06	0	6.9	7.0	7.3	7.5	7.7	8.0
Outsourced/Managed Services	Application Code Security	0.07	0	5.6	5.8	6.0	6.2	6.3	6.5
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Content Filtering & Monitoring	0.01	0	6.30	6.50	6.60	6.80	7.10	7.40
Outsourced/Managed Services	Cyber Services	5.95	38	10.70	11.10	11.20	11.30	11.40	11.60
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.05	0	10.40	10.70	11.00	11.30	11.70	12.10
Outsourced/Managed Services	Firewalls	0.07	0	7.40	7.60	7.80	8.10	8.30	8.60
Outsourced/Managed Services	Identity Management	0.12	0	6.30	6.40	6.70	6.90	7.10	7.30
Outsourced/Managed Services	Intrusion Detection	0.01	0	5.60	5.70	5.80	5.90	5.90	6.00
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Messaging Security	0.10	0	5.70	5.90	6.10	6.30	6.40	6.70
Outsourced/Managed Services	Mobile Security/Device management	0.07	0	3.30	3.40	3.50	3.60	3.70	3.80
Outsourced/Managed Services	Patch Management	0.01	0	5.60	5.80	5.90	6.10	6.30	6.40
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	4.40	4.50	4.60	4.70	4.90	5.10
Outsourced/Managed Services	Vulnerability Assessment	0.04	0	6.90	7.10	7.30	7.50	7.70	7.90
Outsourced/Managed Services	Wireless Security	0.01	0	5.30	5.50	5.70	5.90	6.00	6.20
Situational Awareness	Darkweb	0.56	4	4.20	4.30	4.30	4.40	4.40	4.50
Situational Awareness	External Cyber Threat Intelligence	42.10	310	16.00	16.50	16.70	17.00	17.30	17.60
Situational Awareness	High Level Situational Awareness	35.65	282	12.20	12.50	12.90	13.30	13.70	14.10
Situational Awareness	Internal Cyber Threat Intelligence	8.33	75	17.40	18.00	18.30	18.50	18.80	19.10
Situational Awareness	Low Level Situational Awareness	48.02	258	17.90	18.40	18.90	19.50	19.90	20.60
Situational Awareness	Media Monitoring	2.39	19	3.80	3.80	3.90	3.90	4.00	4.00
Situational Awareness	Proactive Cyber Surveillance	16.64	121	14.10	14.60	14.80	14.90	15.10	15.30
System Recovery & Data Cleansing	Data Recovery Services	29.47	210	18.20	18.80	19.00	19.20	19.50	19.80
System Recovery & Data Cleansing	Manual Data Cleansing	13.56	96	15.90	16.40	16.60	16.80	17.00	17.20
System Recovery & Data Cleansing	System Recovery & Data Cleansing	52.28	406	16.80	17.30	17.50	17.70	17.90	18.20
Training & Education	Access Management	0.04	0	4.10	4.30	4.40	4.50	4.60	4.80
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.02	0	4.10	4.30	4.40	4.60	4.80	5.00
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0
Training & Education	Content Filtering & Monitoring	0.01	0	7.40	7.50	7.70	7.90	8.20	8.50
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0
Training & Education	Identity Management	0.09	0	5.40	5.50	5.70	5.90	6.10	6.30
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0
Training & Education	Malware	0.00	0	0	0	0	0	0	0
Training & Education	Messaging Security	0.02	0	2.90	2.90	3.10	3.10	3.30	3.40
Training & Education	Mobile Security/Device management	0.02	0	7.80	8.00	8.30	8.50	8.70	9.00
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0
Training & Education	PC/Mobile/End Point Security	0.09	0	6.90	7.10	7.30	7.50	7.80	8.00
Training & Education	Vulnerability Assessment	0.01	0	7.90	8.00	8.30	8.60	8.90	9.20
Training & Education	Wireless Security	0.02	0	4.00	4.10	4.20	4.30	4.50	4.60

1.1.47 Croatia

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	1.10	6	5.10	5.30	5.40	5.60	5.80	6.00	
Anti Malware	Anti Virus/Worm	3.44	31	8.30	8.60	8.80	9.10	9.30	9.60	
Anti Malware	Malware	0.62	2	3.60	3.70	3.80	3.90	4.10	4.20	
Anti Malware	Specialist Anti Malware	6.30	18	19.90	20.50	21.20	21.70	22.20	22.90	
Application Security	Application Code Security	0.86	4	5.10	5.20	5.40	5.60	5.70	5.90	
Application Security	Content Filtering & Monitoring	1.08	5	5.70	5.90	6.10	6.30	6.50	6.70	
Application Security	Patch Management	0.40	3	4.00	4.10	4.20	4.30	4.50	4.60	
Application Security	Vulnerability Assessment	23.76	60	16.20	16.70	17.20	17.70	18.20	18.70	
Business Continuity	Business Continuity/Recovery	4.66	12	18.20	18.70	19.30	19.80	20.50	21.10	
Business Continuity	Computer Forensics	2.09	14	14.30	14.70	14.90	15.20	15.40	15.70	
Business Continuity	IT/Cyber Forensics	12.73	49	12.50	12.90	13.30	13.70	14.10	14.50	
Cyber Consultancy	Access Management	0.12	1	5.00	5.20	5.30	5.50	5.70	5.80	
Cyber Consultancy	Anti Spam Solutions	0.10	0	5.40	5.50	5.70	5.80	6.00	6.20	
Cyber Consultancy	Anti Virus/Worm	0.12	0	6.70	6.90	7.10	7.30	7.50	7.70	
Cyber Consultancy	Application Code Security	0.09	0	5.50	5.60	5.80	5.90	6.10	6.30	
Cyber Consultancy	Business Continuity/Recovery	0.10	2	4.10	4.20	4.30	4.50	4.60	4.70	
Cyber Consultancy	Computer Forensics	0.15	1	5.60	5.80	5.90	6.10	6.30	6.50	
Cyber Consultancy	Content Filtering & Monitoring	0.09	1	6.20	6.30	6.50	6.70	6.80	7.10	
Cyber Consultancy	Corporate Services	5.45	39	15.40	15.90	16.10	16.30	16.60	16.80	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.12	1	9.20	9.50	9.90	10.20	10.50	10.80	
Cyber Consultancy	Firewalls	0.07	0	5.50	5.70	5.80	6.00	6.10	6.30	
Cyber Consultancy	Identity Management	0.16	1	4.40	4.50	4.60	4.80	4.90	5.00	
Cyber Consultancy	Intrusion Detection	0.10	0	4.10	4.30	4.40	4.60	4.70	4.80	
Cyber Consultancy	Malware	0.12	0	7.10	7.30	7.50	7.80	8.10	8.30	
Cyber Consultancy	Messaging Security	0.15	1	6.40	6.50	6.80	7.00	7.20	7.40	
Cyber Consultancy	Mobile Security/Device management	0.14	0	6.90	7.10	7.30	7.50	7.70	8.00	
Cyber Consultancy	Patch Management	0.09	0	7.20	7.40	7.70	7.90	8.10	8.40	
Cyber Consultancy	PC/Mobile/End Point Security	0.09	0	7.20	7.40	7.60	7.90	8.10	8.30	
Cyber Consultancy	Vulnerability Assessment	0.11	0	7.70	7.90	8.20	8.40	8.70	8.90	
Cyber Consultancy	Wireless Security	0.09	0	5.30	5.50	5.70	5.80	6.00	6.20	
Cyber Security Insurance	Business Interruption from Network Downtime	2.23	16	11.30	11.70	12.00	12.40	12.70	13.10	
Cyber Security Insurance	Cyber Extortion	2.08	15	11.60	12.00	12.40	12.70	13.10	13.60	
Cyber Security Insurance	Investigation of Privacy Breach	0.59	4	10.30	10.60	10.90	11.10	11.60	11.90	
Cyber Security Insurance	Loss of Third Party Data	2.90	21	10.70	11.00	11.30	11.60	12.00	12.40	
Cyber Security Insurance	Loss or Damage to Digital Assets	1.97	14	10.70	11.00	11.40	11.70	12.10	12.50	
Cyber Security Insurance	Multi-Media Liability	1.81	13	10.60	11.00	11.30	11.60	11.90	12.30	
Cyber Security Insurance	Reputational Damage	1.08	8	10.70	11.00	11.40	11.60	12.00	12.30	
Cyber Security Insurance	Security and Privacy Breaches	2.89	20	10.70	11.00	11.30	11.70	12.00	12.40	
Cyber Security Insurance	Theft of Money and Digital Assets	1.57	11	11.70	12.10	12.40	12.70	13.10	13.50	
Cyber Security Insurance	Third Party Breach Notification	0.93	7	10.30	10.60	11.00	11.30	11.70	12.00	
Encryption	Digital Signatures	1.77	13	19.80	20.30	20.60	21.00	21.40	21.60	
Encryption	Encryption/PKI/Digital Certificates	1.74	11	11.60	12.00	12.10	12.30	12.60	12.80	
Encryption	Storage Security, including Cloud	3.19	21	16.80	17.30	17.50	17.80	18.00	18.20	
Identity & Access	Access Management	1.19	8	6.80	7.00	7.30	7.50	7.70	7.90	
Identity & Access	Authentication	4.63	34	21.50	22.10	22.40	22.60	22.90	23.20	
Identity & Access	Identity Management	12.73	104	18.00	18.50	18.80	19.00	19.20	19.50	
Identity & Access	Intrusion & Anomaly Prevention	2.02	17	21.50	22.30	22.50	22.70	22.90	23.20	
Identity & Access	Messaging Security	2.78	15	15.80	16.30	16.50	16.80	17.10	17.40	
Infrastructure	Data Management	4.14	34	12.90	13.20	13.40	13.60	13.80	13.90	
Infrastructure	Firewalls	0.98	6	6.00	6.20	6.30	6.50	6.70	6.90	
Infrastructure	Infrastructure Monitoring	1.74	11	18.60	19.10	19.20	19.50	19.70	19.80	
Infrastructure	Infrastructure Resilience	1.75	16	20.40	21.00	21.20	21.50	21.60	21.90	
Infrastructure	Intrusion Detection	25.96	87	14.80	15.20	15.60	15.90	16.20	16.60	
Infrastructure	Outsourced/Managed Services	1.84	11	18.80	19.30	19.60	19.80	20.10	20.30	
Infrastructure	Storage Security, including Cloud	6.36	34	17.90	18.40	18.60	18.90	19.10	19.30	
Mobile	Mobile Security/Device management	1.70	12	9.40	9.70	9.90	10.30	10.60	10.90	
Mobile	PC/Mobile/End Point Security	1.69	8	10.50	10.80	11.10	11.50	11.80	12.20	
Mobile	VPN	2.08	16	20.30	20.90	21.10	21.40	21.70	21.90	
Mobile	Wireless Security	2.29	10	5.60	5.70	5.90	6.00	6.30	6.40	
Outsourced/Managed Services	Access Management	0.01	0	6.30	6.50	6.60	6.90	7.10	7.30	
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Virus/Worm	0.04	0	8.20	8.50	8.70	9.00	9.30	9.50	
Outsourced/Managed Services	Application Code Security	0.07	0	5.90	6.10	6.20	6.40	6.60	6.80	
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Content Filtering & Monitoring	0.01	0	7.90	8.10	8.20	8.40	8.70	9.00	
Outsourced/Managed Services	Cyber Services	5.92	49	18.30	18.80	19.00	19.30	19.60	19.80	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.01	0	5.90	6.00	6.20	6.40	6.60	6.80	
Outsourced/Managed Services	Firewalls	0.01	0	3.30	3.40	3.50	3.60	3.80	3.80	
Outsourced/Managed Services	Identity Management	0.10	0	6.00	6.20	6.40	6.50	6.70	6.90	
Outsourced/Managed Services	Intrusion Detection	0.01	0	5.50	5.60	5.70	5.80	5.90	6.00	
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Messaging Security	0.09	0	5.70	5.90	6.10	6.20	6.50	6.60	
Outsourced/Managed Services	Mobile Security/Device management	0.07	0	5.20	5.30	5.50	5.60	5.70	5.90	
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	7.90	8.00	8.30	8.60	8.90	9.20	
Outsourced/Managed Services	Vulnerability Assessment	0.05	0	7.00	7.30	7.50	7.80	8.00	8.20	
Outsourced/Managed Services	Wireless Security	0.01	0	5.10	5.30	5.40	5.50	5.70	5.90	
Situational Awareness	Darkweb	0.49	4	6.20	6.30	6.40	6.50	6.60	6.70	
Situational Awareness	External Cyber Threat Intelligence	34.02	112	16.90	17.40	17.70	18.00	18.30	18.60	
Situational Awareness	High Level Situational Awareness	27.31	85	12.10	12.50	12.90	13.20	13.60	14.00	
Situational Awareness	Internal Cyber Threat Intelligence	6.33	23	19.00	19.60	19.90	20.20	20.50	20.90	
Situational Awareness	Low Level Situational Awareness	6.25	17	16.00	16.50	16.90	17.40	18.10	18.60	
Situational Awareness	Media Monitoring	2.47	18	6.40	6.60	6.70	6.70	6.90	6.90	
Situational Awareness	Proactive Cyber Surveillance	13.06	43	14.20	14.60	14.80	15.00	15.10	15.40	
System Recovery & Data Cleansing	Data Recovery Services	23.10	94	17.90	18.50	18.70	19.00	19.20	19.40	
System Recovery & Data Cleansing	Manual Data Cleansing	9.94	26	15.60	16.00	16.20	16.30	16.50	16.80	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	44.27	121	16.50	17.10	17.30	17.50	17.70	18.00	
Training & Education	Access Management	0.02	0	4.60	4.70	4.80	5.00	5.10	5.30	
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.01	0	4.30	4.40	4.50	4.70	4.80	5.00	
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0	
Training & Education	Identity Management	0.07	0	2.90	3.00	3.10	3.20	3.30	3.40	
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Training & Education	Malware	0.00	0	0	0	0	0	0	0	
Training & Education	Messaging Security	0.01	0	5.00	5.10	5.20	5.40	5.60	5.70	
Training & Education	Mobile Security/Device management	0.01	0	5.10	5.20	5.30	5.50	5.70	5.90	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.02	0	6.50	6.70	6.80	7.00	7.30	7.40	
Training & Education	Vulnerability Assessment	0.01	0	6.80	6.90	7.10	7.40	7.60	7.80	
Training & Education	Wireless Security	0.02	0	4.80	5.00	5.20	5.40	5.60	5.70	

1.1.48 Cyprus

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	0.33	2	4.50	4.60	4.70	4.90	5.10	5.20	
Anti Malware	Anti Virus/Worm	1.46	10	6.50	6.70	6.90	7.10	7.30	7.50	
Anti Malware	Malware	0.39	0	4.30	4.40	4.60	4.80	4.90	5.10	
Anti Malware	Specialist Anti Malware	13.85	37	20.20	20.90	21.60	22.30	22.80	23.60	
Application Security	Application Code Security	0.33	1	5.80	5.90	6.10	6.30	6.50	6.70	
Application Security	Content Filtering & Monitoring	0.33	2	7.00	7.20	7.50	7.70	8.00	8.20	
Application Security	Patch Management	0.22	0	4.60	4.70	4.90	5.00	5.10	5.30	
Application Security	Vulnerability Assessment	35.70	86	17.80	18.40	18.90	19.50	20.10	20.70	
Business Continuity	Business Continuity/Recovery	1.79	5	18.50	19.00	19.60	20.20	20.80	21.50	
Business Continuity	Computer Forensics	0.60	4	11.90	12.30	12.50	12.70	12.90	13.10	
Business Continuity	IT/Cyber Forensics	14.39	58	14.60	15.00	15.50	15.90	16.40	16.90	
Cyber Consultancy	Access Management	0.04	0	4.60	4.70	4.80	4.90	5.10	5.30	
Cyber Consultancy	Anti Spam Solutions	0.01	0	5.10	5.20	5.40	5.50	5.70	5.90	
Cyber Consultancy	Anti Virus/Worm	0.01	0	5.00	5.20	5.30	5.50	5.70	5.80	
Cyber Consultancy	Application Code Security	0.01	0	5.80	5.90	6.10	6.40	6.50	6.70	
Cyber Consultancy	Business Continuity/Recovery	0.01	0	2.20	2.30	2.40	2.50	2.60		
Cyber Consultancy	Computer Forensics	0.02	0	6.80	7.10	7.30	7.40	7.60	7.90	
Cyber Consultancy	Content Filtering & Monitoring	0.01	0	4.80	4.90	5.00	5.20	5.40	5.60	
Cyber Consultancy	Corporate Services	1.48	11	12.70	13.10	13.30	13.50	13.70	13.90	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.01	0	4.50	4.60	4.70	4.90	5.00	5.10	
Cyber Consultancy	Firewalls	0.01	0	5.30	5.50	5.60	5.90	6.10	6.30	
Cyber Consultancy	Identity Management	0.05	0	4.60	4.70	4.80	4.90	5.10	5.20	
Cyber Consultancy	Intrusion Detection	0.01	0	4.30	4.40	4.60	4.70	4.80	4.90	
Cyber Consultancy	Malware	0.02	0	4.00	4.20	4.30	4.50	4.60	4.80	
Cyber Consultancy	Messaging Security	0.07	0	5.50	5.70	5.90	6.00	6.20	6.50	
Cyber Consultancy	Mobile Security/Device management	0.04	0	7.60	7.80	8.10	8.40	8.60	8.90	
Cyber Consultancy	Patch Management	0.01	0	3.60	3.70	3.90	3.90	4.10	4.20	
Cyber Consultancy	PC/Mobile/End Point Security	0.01	0	8.20	8.50	8.70	9.00	9.20	9.50	
Cyber Consultancy	Vulnerability Assessment	0.01	0	6.30	6.50	6.70	6.90	7.10	7.30	
Cyber Consultancy	Wireless Security	0.00	0	0	0	0	0	0	0	
Cyber Security Insurance	Business Interruption from Network Downtime	0.73	5	10.90	11.20	11.60	11.90	12.20	12.70	
Cyber Security Insurance	Cyber Extortion	0.70	5	11.00	11.30	11.60	11.90	12.20	12.60	
Cyber Security Insurance	Investigation of Privacy Breach	0.18	1	11.90	12.20	12.60	12.90	13.30	13.80	
Cyber Security Insurance	Loss of Third Party Data	0.93	6	10.60	10.90	11.30	11.60	12.00	12.30	
Cyber Security Insurance	Loss or Damage to Digital Assets	0.59	4	10.00	10.30	10.60	10.90	11.20	11.50	
Cyber Security Insurance	Multi-Media Liability	0.58	4	11.00	11.40	11.80	12.10	12.40	12.80	
Cyber Security Insurance	Reputational Damage	0.36	2	11.10	11.40	11.70	12.10	12.50	12.90	
Cyber Security Insurance	Security and Privacy Breaches	0.91	6	10.80	11.10	11.50	11.80	12.20	12.50	
Cyber Security Insurance	Theft of Money and Digital Assets	0.49	3	10.70	11.00	11.40	11.70	12.00	12.40	
Cyber Security Insurance	Third Party Breach Notification	0.34	2	10.20	10.50	10.80	11.20	11.50	11.80	
Encryption	Digital Signatures	0.49	3	17.00	17.40	17.60	17.80	18.00	18.20	
Encryption	Encryption/PKI/Digital Certificates	0.49	3	9.80	10.20	10.30	10.50	10.70	10.90	
Encryption	Storage Security, including Cloud	1.00	7	15.20	15.70	15.80	16.00	16.20	16.40	
Identity & Access	Access Management	1.25	8	9.00	9.30	9.60	9.80	10.10	10.40	
Identity & Access	Authentication	1.15	8	17.00	17.50	17.70	18.00	18.20	18.50	
Identity & Access	Identity Management	3.46	23	14.10	14.50	14.60	14.90	15.10	15.20	
Identity & Access	Intrusion & Anomaly Prevention	0.65	4	15.30	15.70	16.00	16.20	16.40	16.60	
Identity & Access	Messaging Security	1.31	5	11.30	11.60	11.70	11.90	12.10	12.30	
Infrastructure	Data Management	1.10	7	11.80	12.20	12.30	12.50	12.60	12.80	
Infrastructure	Firewalls	0.59	2	5.30	5.40	5.60	5.80	5.90	6.10	
Infrastructure	Infrastructure Monitoring	0.61	4	15.60	16.10	16.30	16.50	16.70	16.80	
Infrastructure	Infrastructure Resilience	0.47	3	16.20	16.80	17.00	17.30	17.50	17.70	
Infrastructure	Intrusion Detection	31.85	55	16.20	16.70	17.00	17.30	17.50	17.90	
Infrastructure	Outsourced/Managed Services	0.54	5	15.20	15.60	15.80	16.00	16.30	16.50	
Infrastructure	Storage Security, including Cloud	1.79	11	16.30	16.70	16.90	17.20	17.40	17.60	
Mobile	Mobile Security/Device management	1.10	5	7.80	8.10	8.20	8.50	8.70	9.00	
Mobile	PC/Mobile/End Point Security	0.82	4	7.60	7.80	8.10	8.30	8.60	8.80	
Mobile	VPN	0.51	5	16.00	16.40	16.70	16.80	17.10	17.30	
Mobile	Wireless Security	0.84	8	5.20	5.40	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Access Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Application Code Security	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Cyber Services	1.76	15	15.40	15.90	16.20	16.40	16.60	16.90	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Firewalls	0.01	0	7.30	7.50	7.80	7.90	8.10	8.30	
Outsourced/Managed Services	Identity Management	0.01	0	5.00	5.10	5.30	5.40	5.60	5.70	
Outsourced/Managed Services	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Messaging Security	0.01	0	4.40	4.50	4.70	4.80	4.90	5.10	
Outsourced/Managed Services	Mobile Security/Device management	0.01	0	8.20	8.40	8.70	8.90	9.20	9.40	
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Wireless Security	0.00	0	0	0	0	0	0	0	
Situational Awareness	Darkweb	0.14	1	4.80	5.00	5.10	5.20	5.30	5.30	
Situational Awareness	External Cyber Threat Intelligence	11.30	34	16.40	16.90	17.20	17.50	17.80	18.10	
Situational Awareness	High Level Situational Awareness	8.81	24	12.40	12.80	13.20	13.70	14.10	14.50	
Situational Awareness	Internal Cyber Threat Intelligence	1.85	6	17.50	18.00	18.30	18.60	18.90	19.30	
Situational Awareness	Low Level Situational Awareness	9.06	36	17.50	18.10	18.60	19.10	19.70	20.20	
Situational Awareness	Media Monitoring	0.70	5	5.20	5.40	5.40	5.60	5.60	5.70	
Situational Awareness	Proactive Cyber Surveillance	4.43	16	14.00	14.40	14.60	14.80	15.00	15.20	
System Recovery & Data Cleansing	Data Recovery Services	7.60	28	17.80	18.40	18.60	18.90	19.20	19.40	
System Recovery & Data Cleansing	Manual Data Cleansing	3.00	6	16.00	16.60	16.80	17.00	17.20	17.40	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	12.46	52	17.20	17.70	17.90	18.10	18.40	18.60	
Training & Education	Access Management	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.00	0	0	0	0	0	0	0	
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0	
Training & Education	Identity Management	0.01	0	5.70	5.80	5.90	6.10	6.30	6.50	
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Training & Education	Malware	0.00	0	0	0	0	0	0	0	
Training & Education	Messaging Security	0.00	0	0	0	0	0	0	0	
Training & Education	Mobile Security/Device management	0.00	0	0	0	0	0	0	0	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0	
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Training & Education	Wireless Security	0.00	0	0	0	0	0	0	0	

1.1.49 Czech Republic

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	4.10	32	4.70	4.90	5.00	5.20	5.30	5.50	
Anti Malware	Anti Virus/Worm	11.58	83	7.40	7.60	7.80	8.00	8.30	8.50	
Anti Malware	Malware	2.02	6	6.20	6.30	6.50	6.80	7.00	7.20	
Anti Malware	Specialist Anti Malware	25.75	147	21.40	22.20	22.80	23.50	24.20	25.00	
Application Security	Application Code Security	3.26	17	4.80	4.90	5.00	5.20	5.40	5.50	
Application Security	Content Filtering & Monitoring	3.57	22	5.80	6.00	6.20	6.40	6.60	6.80	
Application Security	Patch Management	1.42	6	4.90	5.10	5.20	5.40	5.60	5.70	
Application Security	Vulnerability Assessment	88.67	524	16.90	17.40	17.90	18.50	19.00	19.60	
Business Continuity	Business Continuity/Recovery	13.68	74	14.10	14.50	15.00	15.40	15.80	16.30	
Business Continuity	Computer Forensics	7.01	48	13.30	13.70	14.00	14.20	14.40	14.60	
Business Continuity	IT/Cyber Forensics	57.40	259	15.30	15.80	16.30	16.80	17.30	17.90	
Cyber Consultancy	Access Management	0.39	1	4.90	5.00	5.20	5.40	5.50	5.70	
Cyber Consultancy	Anti Spam Solutions	0.28	0	6.60	6.80	7.00	7.20	7.40	7.60	
Cyber Consultancy	Anti Virus/Worm	0.38	1	4.40	4.50	4.60	4.80	4.90	5.00	
Cyber Consultancy	Application Code Security	0.36	0	6.30	6.50	6.70	6.90	7.10	7.30	
Cyber Consultancy	Business Continuity/Recovery	0.36	0	5.40	5.60	5.80	5.90	6.10	6.20	
Cyber Consultancy	Computer Forensics	0.42	1	5.50	5.70	5.80	6.00	6.20	6.40	
Cyber Consultancy	Content Filtering & Monitoring	0.23	0	6.00	6.20	6.40	6.60	6.80	7.00	
Cyber Consultancy	Corporate Services	17.68	133	14.20	14.60	14.80	15.00	15.20	15.40	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.48	1	4.70	4.80	4.90	5.00	5.20	5.30	
Cyber Consultancy	Firewalls	0.22	0	5.20	5.30	5.50	5.60	5.80	5.90	
Cyber Consultancy	Identity Management	0.60	2	4.70	4.80	5.00	5.10	5.30	5.50	
Cyber Consultancy	Intrusion Detection	0.29	0	3.90	4.00	4.10	4.20	4.30	4.50	
Cyber Consultancy	Malware	0.42	0	3.70	3.80	4.00	4.10	4.20	4.30	
Cyber Consultancy	Messaging Security	0.49	1	5.50	5.70	5.80	5.90	6.10	6.30	
Cyber Consultancy	Mobile Security/Device management	0.49	0	5.20	5.30	5.50	5.70	5.90	6.10	
Cyber Consultancy	Patch Management	0.37	0	6.80	7.00	7.20	7.50	7.80	8.00	
Cyber Consultancy	PC/Mobile/End Point Security	0.31	0	5.70	5.90	6.00	6.20	6.40	6.60	
Cyber Consultancy	Vulnerability Assessment	0.26	0	5.90	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	Wireless Security	0.23	0	4.10	4.20	4.30	4.40	4.60	4.70	
Cyber Security Insurance	Business Interruption from Network Downtime	7.99	55	10.40	10.70	11.00	11.30	11.60	12.00	
Cyber Security Insurance	Cyber Extortion	7.71	55	10.70	11.00	11.30	11.60	11.90	12.30	
Cyber Security Insurance	Investigation of Privacy Breach	1.95	14	11.40	11.70	12.10	12.40	12.80	13.30	
Cyber Security Insurance	Loss of Third Party Data	9.78	72	10.50	10.90	11.20	11.50	11.90	12.20	
Cyber Security Insurance	Loss or Damage to Digital Assets	7.05	45	11.30	11.60	12.00	12.30	12.70	13.10	
Cyber Security Insurance	Multi-Media Liability	6.35	45	10.90	11.30	11.60	12.00	12.30	12.70	
Cyber Security Insurance	Reputational Damage	3.63	24	11.50	11.90	12.30	12.70	13.00	13.50	
Cyber Security Insurance	Security and Privacy Breaches	10.59	68	11.30	11.60	11.90	12.30	12.60	13.00	
Cyber Security Insurance	Theft of Money and Digital Assets	5.67	36	11.60	12.00	12.30	12.70	13.10	13.50	
Cyber Security Insurance	Third Party Breach Notification	3.79	26	11.40	11.70	12.00	12.40	12.70	13.10	
Encryption	Digital Signatures	6.13	50	17.10	17.60	17.90	18.10	18.40	18.60	
Encryption	Encryption/PKI/Digital Certificates	6.18	34	10.30	10.60	10.80	11.00	11.10	11.30	
Encryption	Storage Security, including Cloud	11.30	77	16.80	17.30	17.50	17.70	18.00	18.20	
Identity & Access	Access Management	4.11	25	6.30	6.50	6.70	6.90	7.10	7.30	
Identity & Access	Authentication	13.69	91	18.70	19.20	19.50	19.70	20.00	20.20	
Identity & Access	Identity Management	40.14	299	16.80	17.30	17.50	17.80	18.00	18.20	
Identity & Access	Intrusion & Anomaly Prevention	7.38	53	18.00	18.50	18.70	19.00	19.20	19.50	
Identity & Access	Messaging Security	11.72	74	9.50	9.80	10.00	10.10	10.30	10.50	
Infrastructure	Data Management	12.79	95	12.40	12.70	12.80	13.00	13.20	13.30	
Infrastructure	Firewalls	2.90	17	5.90	6.10	6.20	6.40	6.60	6.80	
Infrastructure	Infrastructure Monitoring	6.03	43	17.70	18.30	18.50	18.70	18.90	19.20	
Infrastructure	Infrastructure Resilience	5.94	40	19.50	20.20	20.40	20.80	21.00	21.20	
Infrastructure	Intrusion Detection	104.25	485	18.20	18.80	19.20	19.60	20.00	20.40	
Infrastructure	Outsourced/Managed Services	6.73	45	17.90	18.40	18.70	18.90	19.10	19.30	
Infrastructure	Storage Security, including Cloud	19.85	141	18.10	18.80	19.00	19.20	19.40	19.70	
Mobile	Mobile Security/Device management	4.49	33	5.50	5.70	5.80	6.00	6.20	6.40	
Mobile	PC/Mobile/End Point Security	5.86	33	9.20	9.40	9.70	10.00	10.20	10.60	
Mobile	VPN	6.39	45	17.80	18.20	18.60	18.80	19.00	19.30	
Mobile	Wireless Security	6.90	43	4.10	4.30	4.40	4.50	4.70	4.80	
Outsourced/Managed Services	Access Management	0.10	0	4.90	5.00	5.20	5.40	5.50	5.70	
Outsourced/Managed Services	Anti Spam Solutions	0.07	0	6.00	6.20	6.40	6.60	6.80	6.90	
Outsourced/Managed Services	Anti Virus/Worm	0.12	0	5.50	5.70	5.80	6.00	6.20	6.40	
Outsourced/Managed Services	Application Code Security	0.18	0	4.50	4.60	4.70	4.80	5.00	5.20	
Outsourced/Managed Services	Business Continuity/Recovery	0.07	0	4.40	4.50	4.70	4.80	4.90	5.10	
Outsourced/Managed Services	Content Filtering & Monitoring	0.10	0	6.20	6.30	6.50	6.70	6.90	7.10	
Outsourced/Managed Services	Cyber Services	20.60	154	17.20	17.70	18.00	18.20	18.40	18.70	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.10	0	5.10	5.30	5.50	5.60	5.80	5.90	
Outsourced/Managed Services	Firewalls	0.16	0	6.30	6.40	6.60	6.80	7.00	7.20	
Outsourced/Managed Services	Identity Management	0.34	0	5.30	5.50	5.60	5.80	6.00	6.20	
Outsourced/Managed Services	Intrusion Detection	0.10	0	5.30	5.50	5.60	5.70	5.80	5.90	
Outsourced/Managed Services	Malware	0.01	0	4.10	4.30	4.40	4.60	4.70	4.90	
Outsourced/Managed Services	Messaging Security	0.28	0	6.40	6.70	6.90	7.00	7.30	7.50	
Outsourced/Managed Services	Mobile Security/Device management	0.23	0	6.30	6.50	6.80	7.00	7.10	7.40	
Outsourced/Managed Services	Patch Management	0.07	0	4.90	5.10	5.20	5.40	5.60	5.80	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.09	0	5.80	6.00	6.20	6.40	6.60	6.80	
Outsourced/Managed Services	Vulnerability Assessment	0.16	0	6.90	7.00	7.20	7.40	7.60	7.90	
Outsourced/Managed Services	Wireless Security	0.09	0	4.30	4.40	4.50	4.70	4.80	4.90	
Situational Awareness	Darkweb	1.54	12	5.80	5.90	6.00	6.00	6.10	6.20	
Situational Awareness	External Cyber Threat Intelligence	125.65	635	16.90	17.40	17.70	18.00	18.30	18.60	
Situational Awareness	High Level Situational Awareness	98.35	578	13.00	13.30	13.70	14.20	14.60	15.10	
Situational Awareness	Internal Cyber Threat Intelligence	20.11	112	17.80	18.30	18.70	19.00	19.40	19.70	
Situational Awareness	Low Level Situational Awareness	26.48	144	18.00	18.50	19.10	19.70	20.30	20.90	
Situational Awareness	Media Monitoring	7.07	54	6.20	6.40	6.50	6.60	6.70	6.80	
Situational Awareness	Proactive Cyber Surveillance	53.59	290	18.20	18.80	19.00	19.20	19.50	19.80	
System Recovery & Data Cleansing	Data Recovery Services	78.39	373	17.10	17.60	17.90	18.10	18.30	18.60	
System Recovery & Data Cleansing	Manual Data Cleansing	37.73	201	17.10	17.60	17.80	18.00	18.20	18.40	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	135.37	695	17.70	18.20	18.40	18.60	18.90	19.10	
Training & Education	Access Management	0.14	0	3.90	4.10	4.20	4.30	4.50	4.60	
Training & Education	Anti Spam Solutions	0.04	0	5.40	5.60	5.70	6.00	6.10	6.30	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.10	0	5.90	6.10	6.30	6.50	6.70	6.80	
Training & Education	Business Continuity/Recovery	0.01	0	4.50	4.70	4.80	4.90	5.10	5.20	
Training & Education	Computer Forensics	0.01	0	5.10	5.30	5.40	5.60	5.80	5.90	
Training & Education	Content Filtering & Monitoring	0.02	0	4.50	4.60	4.80	4.90	5.00	5.20	
Training & Education	Encryption/PKI/Digital Certificates	0.07	0	6.20	6.40	6.60	6.70	6.90	7.10	
Training & Education	Firewalls	0.02	0	6.20	6.30	6.50	6.80	7.00	7.30	
Training & Education	Identity Management	0.17	0	5.30	5.40	5.50	5.70	5.90	6.00	
Training & Education	Intrusion Detection	0.05	0	5.70	5.80	6.00	6.10	6.30	6.50	
Training & Education	Malware	0.01	0	5.50	5.60	5.80	6.00	6.20	6.30	
Training & Education	Messaging Security	0.12	0	3.90	4.00	4.10	4.20	4.40	4.50	
Training & Education	Mobile Security/Device management	0.11	0	4.70	4.90	5.00	5.20	5.30	5.40	
Training & Education	Patch Management	0.01	0	6.60	6.80	7.00	7.30	7.40	7.70	
Training & Education	PC/Mobile/End Point Security	0.23	0	7.10	7.30	7.50	7.70	7.90	8.10	
Training & Education	Vulnerability Assessment	0.10	0	8.50	8.70	8.90	9.20	9.50	9.70	
Training & Education	Wireless Security	0.14	0	6.20	6.40	6.60	6.70	7.00	7.10	

1.1.50 Denmark

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	5.51	33	4.70	4.80	5.00	5.10	5.30	5.40
Anti Malware	Anti Virus/Worm	17.74	120	6.20	6.30	6.50	6.80	7.00	7.20
Anti Malware	Malware	6.55	47	6.70	6.90	7.10	7.30	7.60	7.80
Anti Malware	Specialist Anti Malware	79.00	390	15.90	16.40	16.90	17.40	17.90	18.40
Application Security	Application Code Security	3.98	28	3.90	4.00	4.20	4.30	4.40	4.50
Application Security	Content Filtering & Monitoring	3.35	25	6.10	6.30	6.50	6.70	6.90	7.10
Application Security	Patch Management	3.23	23	5.60	5.80	5.90	6.10	6.30	6.50
Application Security	Vulnerability Assessment	361.38	1803	16.10	16.60	17.10	17.60	18.20	18.70
Business Continuity	Business Continuity/Recovery	12.40	58	13.60	14.00	14.40	14.80	15.20	15.70
Business Continuity	Computer Forensics	7.02	51	10.80	11.20	11.30	11.50	11.70	11.90
Business Continuity	IT/Cyber Forensics	152.73	890	15.30	15.70	16.10	16.60	17.10	17.70
Cyber Consultancy	Access Management	0.42	3	6.20	6.30	6.60	6.70	6.90	7.10
Cyber Consultancy	Anti Spam Solutions	0.38	1	5.10	5.30	5.40	5.60	5.80	6.00
Cyber Consultancy	Anti Virus/Worm	0.38	1	4.30	4.40	4.60	4.70	4.80	5.00
Cyber Consultancy	Application Code Security	0.40	1	4.30	4.40	4.60	4.70	4.80	5.00
Cyber Consultancy	Business Continuity/Recovery	0.36	2	6.30	6.50	6.60	6.80	7.00	7.30
Cyber Consultancy	Computer Forensics	0.43	4	5.80	6.00	6.10	6.30	6.40	6.60
Cyber Consultancy	Content Filtering & Monitoring	0.34	1	7.10	7.20	7.40	7.70	7.90	8.20
Cyber Consultancy	Corporate Services	16.51	128	11.90	12.30	12.40	12.60	12.80	12.90
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.45	1	5.50	5.70	5.90	6.10	6.30	6.40
Cyber Consultancy	Firewalls	0.16	0	5.60	5.80	5.90	6.10	6.30	6.40
Cyber Consultancy	Identity Management	0.89	7	5.60	5.80	5.90	6.10	6.30	6.40
Cyber Consultancy	Intrusion Detection	0.32	1	5.70	5.90	6.10	6.30	6.50	6.70
Cyber Consultancy	Malware	0.44	3	3.50	3.60	3.70	3.80	3.90	4.00
Cyber Consultancy	Messaging Security	0.64	4	6.60	6.80	7.00	7.20	7.40	7.60
Cyber Consultancy	Mobile Security/Device management	0.47	1	7.50	7.70	7.90	8.20	8.40	8.70
Cyber Consultancy	Patch Management	0.22	0	7.30	7.50	7.70	8.00	8.20	8.40
Cyber Consultancy	PC/Mobile/End Point Security	0.33	0	6.20	6.40	6.50	6.80	6.90	7.10
Cyber Consultancy	Vulnerability Assessment	0.40	1	5.00	5.20	5.30	5.50	5.60	5.80
Cyber Consultancy	Wireless Security	0.38	1	7.80	8.00	8.20	8.50	8.70	9.00
Cyber Security Insurance	Business Interruption from Network Downtime	7.98	56	11.00	11.30	11.60	12.00	12.40	12.70
Cyber Security Insurance	Cyber Extortion	7.06	51	10.60	10.90	11.20	11.60	11.90	12.30
Cyber Security Insurance	Investigation of Privacy Breach	1.97	14	10.50	10.80	11.20	11.60	12.00	12.40
Cyber Security Insurance	Loss of Third Party Data	9.85	69	10.80	11.10	11.40	11.70	12.10	12.50
Cyber Security Insurance	Loss or Damage to Digital Assets	6.36	44	10.60	11.00	11.30	11.50	11.90	12.20
Cyber Security Insurance	Multi-Media Liability	6.33	44	10.80	11.10	11.40	11.80	12.10	12.40
Cyber Security Insurance	Reputational Damage	3.22	24	11.00	11.40	11.70	12.10	12.50	12.80
Cyber Security Insurance	Security and Privacy Breaches	10.26	67	11.30	11.60	11.90	12.30	12.70	13.00
Cyber Security Insurance	Theft of Money and Digital Assets	5.46	40	11.80	12.10	12.60	12.90	13.40	13.80
Cyber Security Insurance	Third Party Breach Notification	3.61	24	10.30	10.70	11.10	11.40	11.70	12.10
Encryption	Digital Signatures	6.09	32	13.90	14.30	14.40	14.60	14.80	15.00
Encryption	Encryption/PKI/Digital Certificates	5.26	41	8.60	8.80	9.00	9.20	9.30	9.50
Encryption	Storage Security, including Cloud	9.86	72	13.90	14.30	14.40	14.50	14.70	14.90
Identity & Access	Access Management	7.26	63	6.00	6.20	6.40	6.50	6.80	7.00
Identity & Access	Authentication	12.18	95	16.00	16.60	16.70	16.90	17.10	17.30
Identity & Access	Identity Management	39.46	282	13.70	14.10	14.30	14.40	14.70	14.90
Identity & Access	Intrusion & Anomaly Prevention	5.65	40	14.60	15.10	15.30	15.50	15.60	15.70
Identity & Access	Messaging Security	15.42	89	11.30	11.60	11.70	11.90	12.10	12.30
Infrastructure	Data Management	11.33	80	10.00	10.30	10.40	10.60	10.70	10.80
Infrastructure	Firewalls	5.48	29	3.80	3.90	4.10	4.20	4.30	4.50
Infrastructure	Infrastructure Monitoring	5.46	35	15.30	15.90	16.10	16.20	16.40	16.50
Infrastructure	Infrastructure Resilience	5.47	39	16.00	16.50	16.70	17.00	17.30	17.50
Infrastructure	Intrusion Detection	499.64	2808	19.30	19.80	20.20	20.50	21.00	21.30
Infrastructure	Outsourced/Managed Services	6.29	48	15.30	15.70	15.80	16.00	16.10	16.40
Infrastructure	Storage Security, including Cloud	18.54	146	15.10	15.50	15.70	15.90	16.20	16.40
Mobile	Mobile Security/Device management	10.34	69	5.00	5.10	5.30	5.50	5.60	5.80
Mobile	PC/Mobile/End Point Security	7.86	56	7.40	7.60	7.80	8.00	8.30	8.50
Mobile	VPN	5.97	43	14.70	15.10	15.30	15.60	15.70	16.00
Mobile	Wireless Security	10.90	77	6.30	6.50	6.60	6.80	7.00	7.20
Outsourced/Managed Services	Access Management	0.10	0	5.30	5.50	5.70	5.80	6.00	6.20
Outsourced/Managed Services	Anti Spam Solutions	0.10	0	11.90	12.30	12.60	13.00	13.40	13.80
Outsourced/Managed Services	Anti Virus/Worm	0.10	0	4.10	4.20	4.40	4.50	4.70	4.80
Outsourced/Managed Services	Application Code Security	0.31	0	6.10	6.30	6.40	6.60	6.80	7.00
Outsourced/Managed Services	Business Continuity/Recovery	0.07	0	5.10	5.30	5.50	5.60	5.80	6.00
Outsourced/Managed Services	Content Filtering & Monitoring	0.10	0	7.10	7.30	7.60	7.80	8.10	8.30
Outsourced/Managed Services	Cyber Services	17.95	148	14.40	14.90	15.00	15.20	15.40	15.70
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.14	0	4.60	4.70	4.80	5.00	5.20	5.30
Outsourced/Managed Services	Firewalls	0.16	0	4.20	4.30	4.50	4.60	4.70	4.90
Outsourced/Managed Services	Identity Management	0.38	1	6.90	7.10	7.30	7.50	7.70	7.90
Outsourced/Managed Services	Intrusion Detection	0.09	0	3.50	3.60	3.70	3.70	3.80	3.90
Outsourced/Managed Services	Malware	0.01	0	8.00	8.20	8.40	8.70	8.90	9.20
Outsourced/Managed Services	Messaging Security	0.28	0	5.30	5.50	5.70	5.80	6.00	6.20
Outsourced/Managed Services	Mobile Security/Device management	0.25	0	5.50	5.70	5.80	6.00	6.20	6.40
Outsourced/Managed Services	Patch Management	0.09	0	5.60	5.80	5.90	6.10	6.20	6.40
Outsourced/Managed Services	PC/Mobile/End Point Security	0.11	0	6.60	6.80	7.00	7.20	7.40	7.70
Outsourced/Managed Services	Vulnerability Assessment	0.15	0	6.70	6.90	7.10	7.30	7.60	7.70
Outsourced/Managed Services	Wireless Security	0.15	0	6.40	6.60	6.80	7.00	7.20	7.40
Situational Awareness	Darkweb	1.42	9	4.90	5.00	5.10	5.20	5.30	5.30
Situational Awareness	External Cyber Threat Intelligence	101.43	577	17.20	17.70	18.00	18.30	18.60	19.00
Situational Awareness	High Level Situational Awareness	92.11	537	13.00	13.40	13.80	14.20	14.60	15.10
Situational Awareness	Internal Cyber Threat Intelligence	17.49	79	13.90	14.30	14.50	14.80	15.10	15.30
Situational Awareness	Low Level Situational Awareness	117.16	668	17.00	17.50	18.10	18.70	19.20	19.80
Situational Awareness	Media Monitoring	7.04	52	5.20	5.40	5.50	5.60	5.60	5.70
Situational Awareness	Proactive Cyber Surveillance	53.51	307	18.90	19.50	19.70	20.00	20.30	20.50
System Recovery & Data Cleansing	Data Recovery Services	69.74	416	14.60	15.00	15.20	15.50	15.60	15.80
System Recovery & Data Cleansing	Manual Data Cleansing	29.88	146	16.30	16.80	17.00	17.30	17.50	17.70
System Recovery & Data Cleansing	System Recovery & Data Cleansing	136.99	772	17.60	18.20	18.40	18.60	18.80	19.10
Training & Education	Access Management	0.21	0	9.10	9.40	9.60	10.00	10.30	10.60
Training & Education	Anti Spam Solutions	0.05	0	5.60	5.70	5.90	6.10	6.30	6.50
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.11	0	7.40	7.70	7.90	8.10	8.30	8.50
Training & Education	Business Continuity/Recovery	0.02	0	6.90	7.20	7.30	7.50	7.80	8.00
Training & Education	Computer Forensics	0.01	0	9.20	9.40	9.70	9.90	10.20	10.50
Training & Education	Content Filtering & Monitoring	0.07	0	6.70	6.90	7.10	7.30	7.50	7.60
Training & Education	Encryption/PKI/Digital Certificates	0.06	0	4.80	5.00	5.20	5.30	5.50	5.60
Training & Education	Firewalls	0.02	0	4.30	4.30	4.50	4.50	4.80	4.80
Training & Education	Identity Management	0.33	1	5.00	5.10	5.20	5.40	5.60	5.80
Training & Education	Intrusion Detection	0.07	0	3.50	3.60	3.70	3.80	3.90	4.10
Training & Education	Malware	0.01	0	8.10	8.40	8.60	8.90	9.20	9.40
Training & Education	Messaging Security	0.12	0	4.70	4.90	5.00	5.20	5.30	5.50
Training & Education	Mobile Security/Device management	0.18	0	7.20	7.40	7.60	7.90	8.20	8.40
Training & Education	Patch Management	0.01	0	4.60	4.80	5.00	5.10	5.30	5.40
Training & Education	PC/Mobile/End Point Security	0.17	0	6.90	7.10	7.40	7.60	7.80	8.00
Training & Education	Vulnerability Assessment	0.07	0	4.20	4.40	4.50	4.60	4.80	4.90
Training & Education	Wireless Security	0.12	0	5.80	6.00	6.20	6.40	6.60	6.70

1.1.51 Estonia

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	0.50	3	6.40	6.60	6.80	7.10	7.30	7.50
Anti Malware	Anti Virus/Worm	1.73	12	7.60	7.80	8.10	8.30	8.60	8.80
Anti Malware	Malware	1.09	6	9.00	9.30	9.60	9.80	10.20	10.40
Anti Malware	Specialist Anti Malware	16.64	50	19.60	20.10	20.60	21.10	21.70	22.30
Application Security	Application Code Security	0.44	3	6.70	6.90	7.10	7.40	7.60	7.80
Application Security	Content Filtering & Monitoring	0.29	1	4.50	4.60	4.80	4.90	5.10	5.20
Application Security	Patch Management	0.25	0	4.90	5.00	5.20	5.30	5.50	5.70
Application Security	Vulnerability Assessment	52.06	150	18.20	18.80	19.40	20.00	20.60	21.20
Business Continuity	Business Continuity/Recovery	2.29	8	19.30	19.90	20.50	21.10	21.80	22.40
Business Continuity	Computer Forensics	0.93	8	15.20	15.60	16.00	16.20	16.50	16.80
Business Continuity	IT/Cyber Forensics	17.49	85	14.20	14.70	15.10	15.50	16.00	16.50
Cyber Consultancy	Access Management	0.09	0	5.60	5.80	6.00	6.20	6.30	6.60
Cyber Consultancy	Anti Spam Solutions	0.05	0	12.00	12.30	12.70	13.00	13.40	13.80
Cyber Consultancy	Anti Virus/Worm	0.02	0	5.80	6.00	6.20	6.30	6.60	6.80
Cyber Consultancy	Application Code Security	0.02	0	7.40	7.60	8.00	8.20	8.50	8.70
Cyber Consultancy	Business Continuity/Recovery	0.02	0	4.30	4.30	4.50	4.60	4.80	4.90
Cyber Consultancy	Computer Forensics	0.05	0	4.10	4.20	4.20	4.40	4.50	4.70
Cyber Consultancy	Content Filtering & Monitoring	0.01	0	5.30	5.50	5.60	5.80	6.00	6.20
Cyber Consultancy	Corporate Services	2.00	14	15.90	16.40	16.60	16.80	17.00	17.30
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.05	0	3.10	3.20	3.30	3.40	3.50	3.60
Cyber Consultancy	Firewalls	0.01	0	6.40	6.50	6.70	6.90	7.00	7.30
Cyber Consultancy	Identity Management	0.02	0	2.60	2.80	2.90	2.90	3.00	3.10
Cyber Consultancy	Intrusion Detection	0.01	0	6.30	6.50	6.70	7.00	7.20	7.40
Cyber Consultancy	Malware	0.05	0	4.80	4.90	5.00	5.20	5.30	5.50
Cyber Consultancy	Messaging Security	0.07	0	6.50	6.70	6.90	7.10	7.30	7.50
Cyber Consultancy	Mobile Security/Device management	0.02	0	4.30	4.50	4.60	4.80	4.90	5.00
Cyber Consultancy	Patch Management	0.02	0	5.80	6.00	6.20	6.40	6.60	6.80
Cyber Consultancy	PC/Mobile/End Point Security	0.01	0	3.50	3.60	3.70	3.80	3.90	4.10
Cyber Consultancy	Vulnerability Assessment	0.02	0	7.20	7.40	7.70	7.90	8.20	8.30
Cyber Consultancy	Wireless Security	0.01	0	6.40	6.60	6.80	7.00	7.20	7.50
Cyber Security Insurance	Business Interruption from Network Downtime	0.99	7	10.30	10.60	10.90	11.20	11.60	11.90
Cyber Security Insurance	Cyber Extortion	0.86	6	11.00	11.40	11.70	12.10	12.40	12.80
Cyber Security Insurance	Investigation of Privacy Breach	0.25	2	11.60	12.00	12.30	12.60	13.00	13.30
Cyber Security Insurance	Loss of Third Party Data	1.27	9	10.80	11.20	11.50	11.80	12.20	12.60
Cyber Security Insurance	Loss or Damage to Digital Assets	0.72	5	10.80	11.10	11.50	11.90	12.20	12.60
Cyber Security Insurance	Multi-Media Liability	0.80	5	10.70	11.10	11.40	11.70	12.10	12.40
Cyber Security Insurance	Reputational Damage	0.43	3	10.20	10.50	10.80	11.10	11.40	11.70
Cyber Security Insurance	Security and Privacy Breaches	1.21	9	10.60	10.90	11.20	11.60	11.90	12.30
Cyber Security Insurance	Theft of Money and Digital Assets	0.66	5	12.20	12.60	13.00	13.40	13.80	14.10
Cyber Security Insurance	Third Party Breach Notification	0.43	3	8.80	9.00	9.30	9.60	9.80	10.10
Encryption	Digital Signatures	0.71	4	17.70	18.20	18.40	18.60	18.80	19.10
Encryption	Encryption/PKI/Digital Certificates	0.69	4	12.10	12.50	12.70	12.80	13.00	13.20
Encryption	Storage Security, including Cloud	1.43	11	18.60	19.10	19.40	19.60	19.80	20.10
Identity & Access	Access Management	0.70	2	6.40	6.60	6.80	7.00	7.20	7.40
Identity & Access	Authentication	1.80	13	20.50	21.10	21.30	21.50	21.70	22.00
Identity & Access	Identity Management	4.87	36	18.20	18.70	19.00	19.20	19.40	19.70
Identity & Access	Intrusion & Anomaly Prevention	0.77	6	17.90	18.40	18.70	18.80	19.10	19.50
Identity & Access	Messaging Security	2.28	18	13.40	13.90	14.10	14.40	14.70	15.00
Infrastructure	Data Management	1.52	13	12.30	12.80	12.90	13.00	13.20	13.40
Infrastructure	Firewalls	0.72	4	5.60	5.70	5.90	6.10	6.30	6.50
Infrastructure	Infrastructure Monitoring	0.76	5	22.10	22.90	23.20	23.60	23.80	24.20
Infrastructure	Infrastructure Resilience	0.60	5	23.80	24.50	24.80	25.20	25.40	25.90
Infrastructure	Intrusion Detection	48.74	165	16.20	16.70	17.00	17.30	17.70	18.00
Infrastructure	Outsourced/Managed Services	1.00	8	19.90	20.60	20.80	21.10	21.30	21.50
Infrastructure	Storage Security, including Cloud	2.59	19	19.70	20.30	20.60	20.90	21.10	21.50
Mobile	Mobile Security/Device management	1.21	5	5.60	5.70	5.90	6.00	6.20	6.50
Mobile	PC/Mobile/End Point Security	1.03	4	7.70	8.00	8.20	8.40	8.70	8.90
Mobile	VPN	0.83	5	20.90	21.50	21.80	22.00	22.30	22.40
Mobile	Wireless Security	0.47	2	3.50	3.60	3.70	3.80	3.90	4.00
Outsourced/Managed Services	Access Management	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Anti Virus/Worm	0.01	0	8.00	8.30	8.50	8.80	9.10	9.30
Outsourced/Managed Services	Application Code Security	0.01	0	5.00	5.10	5.30	5.40	5.60	5.80
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Cyber Services	2.50	18	18.60	19.20	19.40	19.60	19.80	20.10
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Firewalls	0.01	0	5.50	5.60	5.70	5.90	6.10	6.30
Outsourced/Managed Services	Identity Management	0.01	0	5.30	5.50	5.60	5.80	6.00	6.10
Outsourced/Managed Services	Intrusion Detection	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Messaging Security	0.01	0	8.20	8.50	8.80	9.10	9.40	9.70
Outsourced/Managed Services	Mobile Security/Device management	0.01	0	8.30	8.50	8.70	8.90	9.20	9.40
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Vulnerability Assessment	0.01	0	10.80	11.10	11.50	11.90	12.30	12.50
Outsourced/Managed Services	Wireless Security	0.00	0	0	0	0	0	0	0
Situational Awareness	Darkweb	0.20	2	5.90	6.10	6.20	6.20	6.30	6.40
Situational Awareness	External Cyber Threat Intelligence	13.50	50	16.70	17.30	17.50	17.80	18.10	18.40
Situational Awareness	High Level Situational Awareness	11.59	43	12.50	12.80	13.20	13.60	14.10	14.50
Situational Awareness	Internal Cyber Threat Intelligence	2.59	10	18.20	18.80	19.10	19.40	19.80	20.10
Situational Awareness	Low Level Situational Awareness	16.63	60	16.70	17.10	17.60	18.20	18.70	19.30
Situational Awareness	Media Monitoring	0.89	6	6.70	6.80	6.90	7.10	7.10	7.20
Situational Awareness	Proactive Cyber Surveillance	5.79	15	14.60	15.00	15.20	15.40	15.60	15.80
System Recovery & Data Cleansing	Data Recovery Services	9.61	34	18.00	18.60	18.80	19.10	19.30	19.50
System Recovery & Data Cleansing	Manual Data Cleansing	4.05	13	16.30	16.70	16.90	17.10	17.40	17.50
System Recovery & Data Cleansing	System Recovery & Data Cleansing	18.76	48	16.90	17.40	17.60	17.80	18.10	18.30
Training & Education	Access Management	0.00	0	0	0	0	0	0	0
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.00	0	0	0	0	0	0	0
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0
Training & Education	Identity Management	0.01	0	4.00	4.10	4.30	4.40	4.50	4.60
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0
Training & Education	Malware	0.00	0	0	0	0	0	0	0
Training & Education	Messaging Security	0.00	0	0	0	0	0	0	0
Training & Education	Mobile Security/Device management	0.00	0	0	0	0	0	0	0
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0
Training & Education	PC/Mobile/End Point Security	0.01	0	5.20	5.40	5.60	5.80	6.00	6.20
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0
Training & Education	Wireless Security	0.00	0	0	0	0	0	0	0

1.1.52 Finland

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	4.25	22	6.00	6.20	6.40	6.60	6.80	7.00	
Anti Malware	Anti Virus/Worm	17.45	97	8.30	8.50	8.80	9.10	9.40	9.70	
Anti Malware	Malware	6.45	31	7.30	7.50	7.70	8.00	8.20	8.40	
Anti Malware	Specialist Anti Malware	47.69	313	11.30	11.70	12.00	12.40	12.70	13.10	
Application Security	Application Code Security	3.46	19	5.80	5.70	5.90	6.10	6.30	6.50	
Application Security	Content Filtering & Monitoring	2.96	13	5.80	6.00	6.20	6.40	6.60	6.70	
Application Security	Patch Management	3.68	4	6.80	7.00	7.20	7.40	7.60	7.80	
Application Security	Vulnerability Assessment	373.80	1784	17.80	18.30	18.80	19.40	20.00	20.60	
Business Continuity	Business Continuity/Recovery	12.91	61	16.00	16.50	17.00	17.50	18.00	18.60	
Business Continuity	Computer Forensics	7.11	44	20.40	21.00	21.20	21.60	21.90	22.20	
Business Continuity	IT/Cyber Forensics	190.07	942	16.30	16.90	17.30	17.80	18.40	18.90	
Cyber Consultancy	Access Management	0.48	1	5.10	5.30	5.50	5.60	5.80	6.00	
Cyber Consultancy	Anti Spam Solutions	0.27	1	5.40	5.60	5.80	5.90	6.10	6.30	
Cyber Consultancy	Anti Virus/Worm	0.32	1	4.70	4.90	5.00	5.10	5.30	5.50	
Cyber Consultancy	Application Code Security	0.34	1	5.00	5.20	5.30	5.50	5.70	5.90	
Cyber Consultancy	Business Continuity/Recovery	0.32	1	4.70	4.80	5.00	5.10	5.30	5.40	
Cyber Consultancy	Computer Forensics	0.47	1	6.80	7.00	7.30	7.50	7.80	8.00	
Cyber Consultancy	Content Filtering & Monitoring	0.27	1	6.20	6.40	6.60	6.80	7.00	7.30	
Cyber Consultancy	Corporate Services	17.83	137	21.50	22.20	22.50	22.80	23.10	23.40	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.47	1	5.50	5.70	5.90	6.00	6.20	6.40	
Cyber Consultancy	Firewalls	0.12	0	3.90	4.00	4.10	4.20	4.30	4.50	
Cyber Consultancy	Identity Management	0.50	1	5.10	5.30	5.40	5.60	5.70	5.90	
Cyber Consultancy	Intrusion Detection	0.29	0	3.30	3.40	3.50	3.60	3.80	3.90	
Cyber Consultancy	Malware	0.44	1	5.30	5.50	5.70	5.80	6.00	6.20	
Cyber Consultancy	Messaging Security	0.59	1	4.90	5.10	5.30	5.50	5.60	5.80	
Cyber Consultancy	Mobile Security/Device management	0.45	1	5.30	5.50	5.60	5.80	6.00	6.20	
Cyber Consultancy	Patch Management	0.27	0	6.70	7.00	7.20	7.40	7.60	7.80	
Cyber Consultancy	PC/Mobile/End Point Security	0.26	1	5.20	5.40	5.50	5.70	5.90	6.00	
Cyber Consultancy	Vulnerability Assessment	0.37	1	6.00	6.20	6.40	6.60	6.80	7.00	
Cyber Consultancy	Wireless Security	0.42	1	8.30	8.60	8.80	9.00	9.30	9.60	
Cyber Security Insurance	Business Interruption from Network Downtime	6.93	47	11.10	11.40	11.80	12.10	12.50	12.90	
Cyber Security Insurance	Cyber Extortion	6.31	43	10.50	10.80	11.20	11.50	11.80	12.20	
Cyber Security Insurance	Investigation of Privacy Breach	1.73	13	12.00	12.40	12.80	13.20	13.60	14.00	
Cyber Security Insurance	Loss of Third Party Data	8.90	60	10.90	11.30	11.60	11.90	12.30	12.70	
Cyber Security Insurance	Loss or Damage to Digital Assets	6.06	41	10.70	11.00	11.30	11.60	12.00	12.30	
Cyber Security Insurance	Multi-Media Liability	5.80	39	10.90	11.30	11.60	12.00	12.40	12.80	
Cyber Security Insurance	Reputational Damage	3.11	18	9.90	10.10	10.50	10.80	11.20	11.50	
Cyber Security Insurance	Security and Privacy Breaches	8.66	61	10.40	10.70	11.00	11.30	11.70	12.00	
Cyber Security Insurance	Theft of Money and Digital Assets	4.58	32	10.80	11.10	11.40	11.70	12.10	12.50	
Cyber Security Insurance	Third Party Breach Notification	3.10	20	9.80	10.10	10.40	10.80	11.10	11.40	
Encryption	Digital Signatures	6.54	47	25.50	26.30	26.50	26.80	27.10	27.50	
Encryption	Encryption/PKI/Digital Certificates	5.73	37	14.40	14.80	15.10	15.40	15.70	16.10	
Encryption	Storage Security, including Cloud	11.34	87	25.10	25.80	26.20	26.50	26.80	27.10	
Identity & Access	Access Management	5.98	27	5.10	5.30	5.40	5.60	5.80	6.00	
Identity & Access	Authentication	14.05	109	27.60	28.50	28.70	29.10	29.50	29.80	
Identity & Access	Identity Management	46.76	303	23.50	24.10	24.40	24.70	25.00	25.30	
Identity & Access	Intrusion & Anomaly Prevention	7.35	45	27.20	28.00	28.30	28.60	29.10	29.60	
Identity & Access	Messaging Security	16.12	77	11.60	12.00	12.20	12.50	12.70	13.00	
Infrastructure	Data Management	13.13	86	18.00	18.60	18.80	19.00	19.30	19.50	
Infrastructure	Firewalls	4.69	22	4.30	4.40	4.50	4.60	4.80	4.90	
Infrastructure	Infrastructure Monitoring	6.85	47	26.50	27.40	27.70	28.10	28.30	28.50	
Infrastructure	Infrastructure Resilience	6.58	41	28.00	28.70	29.00	29.30	29.80	30.30	
Infrastructure	Intrusion Detection	297.79	1370	17.50	18.00	18.30	18.70	19.00	19.30	
Infrastructure	Outsourced/Managed Services	6.96	52	26.10	27.00	27.40	27.80	28.30	28.70	
Infrastructure	Storage Security, including Cloud	20.71	160	26.80	27.50	27.80	28.20	28.50	28.90	
Mobile	Mobile Security/Device management	9.90	36	5.90	6.00	6.20	6.40	6.60	6.90	
Mobile	PC/Mobile/End Point Security	7.77	36	9.00	9.30	9.50	9.80	10.10	10.40	
Mobile	VPN	7.95	52	27.30	28.00	28.40	28.70	29.10	29.30	
Mobile	Wireless Security	12.69	67	7.00	7.20	7.40	7.60	7.80	8.00	
Outsourced/Managed Services	Access Management	0.10	0	7.20	7.40	7.70	7.90	8.10	8.40	
Outsourced/Managed Services	Anti Spam Solutions	0.07	0	6.70	6.90	7.00	7.30	7.50	7.70	
Outsourced/Managed Services	Anti Virus/Worm	0.11	0	6.90	7.10	7.40	7.60	7.80	8.10	
Outsourced/Managed Services	Application Code Security	0.27	0	7.10	7.40	7.60	7.80	8.00	8.30	
Outsourced/Managed Services	Business Continuity/Recovery	0.02	0	5.70	5.80	6.00	6.20	6.40	6.50	
Outsourced/Managed Services	Content Filtering & Monitoring	0.10	0	5.40	5.60	5.70	5.90	6.10	6.30	
Outsourced/Managed Services	Cyber Services	21.75	160	26.10	26.80	27.10	27.50	27.80	28.20	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.16	0	5.70	5.80	6.00	6.20	6.30	6.50	
Outsourced/Managed Services	Firewalls	0.16	0	4.40	4.60	4.70	4.80	4.90	5.10	
Outsourced/Managed Services	Identity Management	0.37	1	5.50	5.70	5.90	6.00	6.20	6.40	
Outsourced/Managed Services	Intrusion Detection	0.10	0	4.20	4.30	4.40	4.50	4.50	4.60	
Outsourced/Managed Services	Malware	0.02	0	5.50	5.60	5.80	6.00	6.30	6.50	
Outsourced/Managed Services	Messaging Security	0.27	0	5.70	5.90	6.10	6.30	6.40	6.70	
Outsourced/Managed Services	Mobile Security/Device management	0.20	0	4.50	4.60	4.80	4.90	5.00	5.20	
Outsourced/Managed Services	Patch Management	0.07	0	7.20	7.40	7.60	7.80	8.10	8.30	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.07	0	5.30	5.50	5.60	5.80	6.00	6.20	
Outsourced/Managed Services	Vulnerability Assessment	0.17	0	7.10	7.30	7.50	7.80	8.00	8.20	
Outsourced/Managed Services	Wireless Security	0.10	0	6.90	7.00	7.30	7.50	7.70	8.00	
Situational Awareness	Darkweb	1.43	11	8.80	9.00	9.20	9.30	9.50	9.60	
Situational Awareness	External Cyber Threat Intelligence	93.09	506	16.10	16.60	16.90	17.20	17.50	17.80	
Situational Awareness	High Level Situational Awareness	86.38	439	12.70	13.10	13.50	13.90	14.30	14.70	
Situational Awareness	Internal Cyber Threat Intelligence	18.71	102	17.70	18.20	18.60	18.90	19.20	19.60	
Situational Awareness	Low Level Situational Awareness	105.76	483	15.00	15.40	15.90	16.40	16.90	17.50	
Situational Awareness	Media Monitoring	6.98	51	9.10	9.40	9.50	9.50	9.70	9.80	
Situational Awareness	Proactive Cyber Surveillance	47.77	256	16.00	16.40	16.60	16.80	17.00	17.20	
System Recovery & Data Cleansing	Data Recovery Services	61.90	335	15.20	15.70	15.90	16.10	16.30	16.50	
System Recovery & Data Cleansing	Manual Data Cleansing	34.14	186	17.30	17.80	18.00	18.20	18.50	18.70	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	123.79	729	16.70	17.10	17.30	17.50	17.80	18.00	
Training & Education	Access Management	0.15	0	5.90	6.00	6.20	6.30	6.60	6.80	
Training & Education	Anti Spam Solutions	0.05	0	8.00	8.20	8.50	8.80	9.00	9.30	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.11	0	5.00	5.20	5.40	5.60	5.70	5.90	
Training & Education	Business Continuity/Recovery	0.02	0	5.50	5.60	5.90	6.00	6.20	6.30	
Training & Education	Computer Forensics	0.01	0	8.90	9.20	9.40	9.70	9.90	10.30	
Training & Education	Content Filtering & Monitoring	0.02	0	7.00	7.20	7.50	7.70	7.80	8.10	
Training & Education	Encryption/PKI/Digital Certificates	0.07	0	6.30	6.40	6.60	6.80	7.00	7.20	
Training & Education	Firewalls	0.02	0	5.80	5.90	6.20	6.30	6.50	6.70	
Training & Education	Identity Management	0.28	1	4.70	4.90	5.00	5.10	5.30	5.50	
Training & Education	Intrusion Detection	0.07	0	4.30	4.50	4.60	4.80	4.90	5.00	
Training & Education	Malware	0.02	0	5.50	5.80	5.90	6.20	6.30	6.50	
Training & Education	Messaging Security	0.12	0	5.60	5.70	5.90	6.10	6.20	6.40	
Training & Education	Mobile Security/Device management	0.11	0	6.70	6.90	7.10	7.30	7.50	7.70	
Training & Education	Patch Management	0.01	0	5.70	5.90	6.10	6.30	6.40	6.60	
Training & Education	PC/Mobile/End Point Security	0.17	0	5.80	6.00	6.10	6.30	6.50	6.80	
Training & Education	Vulnerability Assessment	0.05	0	6.70	6.80	7.00	7.20	7.40	7.70	
Training & Education	Wireless Security	0.12	0	7.80	8.00	8.30	8.50	8.80	9.10	

1.1.53 France

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	47.20	339	5.50	5.60	5.80	6.00	6.20	6.40	
Anti Malware	Anti Virus/Worm	190.92	1313	8.20	8.40	8.60	8.80	9.10	9.40	
Anti Malware	Malware	45.16	308	5.80	5.90	6.10	6.30	6.50	6.70	
Anti Malware	Specialist Anti Malware	555.32	3376	11.60	12.00	12.40	12.80	13.10	13.50	
Application Security	Application Code Security	44.31	320	6.20	6.40	6.60	6.80	7.00	7.20	
Application Security	Content Filtering & Monitoring	32.51	217	6.00	6.20	6.40	6.50	6.80	6.90	
Application Security	Patch Management	35.56	239	5.80	5.80	6.00	6.10	6.30	6.50	
Application Security	Vulnerability Assessment	3600.35	22718	17.50	18.10	18.60	19.20	19.70	20.30	
Business Continuity	Business Continuity/Recovery	143.12	717	13.50	14.00	14.40	14.70	15.20	15.70	
Business Continuity	Computer Forensics	84.58	551	19.30	19.90	20.20	20.50	20.80	21.00	
Business Continuity	IT/Cyber Forensics	2359.01	15966	16.90	17.30	17.90	18.40	19.00	19.60	
Cyber Consultancy	Access Management	5.96	47	7.80	8.00	8.30	8.50	8.80	9.10	
Cyber Consultancy	Anti Spam Solutions	3.23	23	4.90	5.00	5.20	5.30	5.50	5.70	
Cyber Consultancy	Anti Virus/Worm	4.55	26	5.70	5.80	6.00	6.20	6.40	6.60	
Cyber Consultancy	Application Code Security	3.63	22	3.70	3.80	3.90	4.00	4.10	4.30	
Cyber Consultancy	Business Continuity/Recovery	3.16	28	4.50	4.70	4.80	4.90	5.10	5.30	
Cyber Consultancy	Computer Forensics	4.94	34	4.40	4.50	4.70	4.80	4.90	5.10	
Cyber Consultancy	Content Filtering & Monitoring	4.28	26	7.60	7.90	8.10	8.40	8.60	8.90	
Cyber Consultancy	Corporate Services	212.81	1422	21.60	22.20	22.50	22.80	23.10	23.30	
Cyber Consultancy	Encryption/PKI/Digital Certificates	5.37	34	6.40	6.60	6.80	7.10	7.30	7.50	
Cyber Consultancy	Firewalls	2.00	9	5.20	5.40	5.60	5.70	5.90	6.10	
Cyber Consultancy	Identity Management	5.38	43	5.10	5.30	5.50	5.60	5.90	6.00	
Cyber Consultancy	Intrusion Detection	2.85	17	3.10	3.20	3.30	3.40	3.50	3.60	
Cyber Consultancy	Malware	4.69	35	5.00	5.20	5.40	5.50	5.70	5.90	
Cyber Consultancy	Messaging Security	5.05	33	5.00	5.20	5.30	5.50	5.60	5.80	
Cyber Consultancy	Mobile Security/Device management	3.99	26	4.20	4.30	4.50	4.70	4.80	4.90	
Cyber Consultancy	Patch Management	3.19	19	5.90	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	PC/Mobile/End Point Security	3.51	27	5.40	5.60	5.70	5.90	6.10	6.20	
Cyber Consultancy	Vulnerability Assessment	4.76	31	6.40	6.60	6.70	7.00	7.20	7.40	
Cyber Consultancy	Wireless Security	3.83	24	6.40	6.60	6.70	7.00	7.20	7.40	
Cyber Security Insurance	Business Interruption from Network Downtime	77.25	546	11.70	12.00	12.30	12.70	13.00	13.40	
Cyber Security Insurance	Cyber Extortion	73.78	506	11.20	11.50	11.90	12.30	12.70	13.00	
Cyber Security Insurance	Investigation of Privacy Breach	18.50	132	11.40	11.90	12.20	12.60	13.00	13.40	
Cyber Security Insurance	Loss of Third Party Data	100.01	662	10.20	10.40	10.80	11.10	11.40	11.80	
Cyber Security Insurance	Loss or Damage to Digital Assets	67.30	456	10.40	10.70	11.00	11.40	11.70	12.00	
Cyber Security Insurance	Multi-Media Liability	62.24	414	10.60	10.90	11.20	11.50	11.80	12.20	
Cyber Security Insurance	Reputational Damage	38.16	257	11.70	12.10	12.40	12.80	13.20	13.50	
Cyber Security Insurance	Security and Privacy Breaches	98.46	666	10.70	11.10	11.40	11.70	12.10	12.50	
Cyber Security Insurance	Theft of Money and Digital Assets	55.10	378	11.30	11.60	12.00	12.40	12.70	13.10	
Cyber Security Insurance	Third Party Breach Notification	33.18	236	10.00	10.30	10.70	11.00	11.40	11.80	
Encryption	Digital Signatures	72.70	536	25.70	26.40	26.60	27.10	27.40	27.70	
Encryption	Encryption/PKI/Digital Certificates	65.44	431	14.70	15.10	15.40	15.70	16.00	16.20	
Encryption	Storage Security, including Cloud	136.70	943	25.00	25.80	26.10	26.50	26.80	27.20	
Identity & Access	Access Management	83.00	550	6.40	6.60	6.80	7.10	7.30	7.50	
Identity & Access	Authentication	176.48	1160	28.10	28.90	29.10	29.50	29.80	30.10	
Identity & Access	Identity Management	507.04	3787	23.60	24.30	24.60	24.90	25.20	25.50	
Identity & Access	Intrusion & Anomaly Prevention	84.17	573	26.20	27.00	27.50	27.80	28.30	28.70	
Identity & Access	Messaging Security	153.24	1038	8.50	8.80	8.90	9.10	9.30	9.50	
Infrastructure	Data Management	143.54	1057	18.20	18.70	18.90	19.20	19.40	19.70	
Infrastructure	Firewalls	77.20	493	4.80	5.00	5.10	5.30	5.40	5.60	
Infrastructure	Infrastructure Monitoring	66.23	428	26.10	27.00	27.30	27.60	27.90	28.20	
Infrastructure	Infrastructure Resilience	74.89	549	29.60	30.60	30.90	31.30	31.50	32.00	
Infrastructure	Intrusion Detection	4762.65	27014	18.20	18.70	19.10	19.60	19.90	20.40	
Infrastructure	Outsourced/Managed Services	88.44	511	26.20	26.80	27.00	27.40	27.80	28.20	
Infrastructure	Storage Security, including Cloud	248.02	1733	27.00	27.80	28.10	28.50	28.90	29.30	
Mobile	Mobile Security/Device management	134.82	915	6.40	6.60	6.90	7.10	7.30	7.60	
Mobile	PC/Mobile/End Point Security	107.32	730	7.60	7.80	8.10	8.30	8.50	8.90	
Mobile	VPN	77.42	533	26.80	27.80	28.10	28.30	28.80	29.10	
Mobile	Wireless Security	112.26	774	6.50	6.60	6.90	7.10	7.30	7.50	
Outsourced/Managed Services	Access Management	0.95	1	7.60	7.80	8.00	8.30	8.50	8.80	
Outsourced/Managed Services	Anti Spam Solutions	0.61	1	5.10	5.30	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Anti Virus/Worm	0.97	1	4.20	4.30	4.40	4.60	4.70	4.90	
Outsourced/Managed Services	Application Code Security	3.00	21	7.20	7.40	7.60	7.80	8.10	8.40	
Outsourced/Managed Services	Business Continuity/Recovery	0.73	3	5.90	6.10	6.30	6.50	6.70	6.80	
Outsourced/Managed Services	Content Filtering & Monitoring	0.99	1	6.80	7.00	7.30	7.40	7.70	7.90	
Outsourced/Managed Services	Cyber Services	239.53	1749	26.40	27.20	27.60	28.00	28.40	28.70	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	1.66	6	6.00	6.20	6.40	6.60	6.80	7.00	
Outsourced/Managed Services	Firewalls	2.02	11	6.40	6.70	6.90	7.00	7.30	7.50	
Outsourced/Managed Services	Identity Management	3.01	25	5.20	5.30	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Intrusion Detection	1.07	3	4.20	4.30	4.40	4.50	4.60	4.70	
Outsourced/Managed Services	Malware	0.42	1	4.70	4.90	5.10	5.20	5.40	5.50	
Outsourced/Managed Services	Messaging Security	3.11	14	5.10	5.20	5.40	5.50	5.70	5.90	
Outsourced/Managed Services	Mobile Security/Device management	2.77	13	4.60	4.80	4.90	5.10	5.20	5.40	
Outsourced/Managed Services	Patch Management	0.65	1	5.70	5.90	6.00	6.20	6.40	6.60	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.92	1	6.60	6.90	7.10	7.30	7.50	7.70	
Outsourced/Managed Services	Vulnerability Assessment	1.75	6	5.20	5.30	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Wireless Security	1.18	3	7.20	7.50	7.70	8.00	8.20	8.40	
Situational Awareness	Darkweb	16.90	121	8.60	8.80	9.00	9.10	9.20	9.30	
Situational Awareness	External Cyber Threat Intelligence	1209.20	6760	17.50	18.00	18.30	18.70	19.00	19.30	
Situational Awareness	High Level Situational Awareness	1068.43	7222	13.20	13.70	14.10	14.50	15.00	15.40	
Situational Awareness	Internal Cyber Threat Intelligence	212.83	1200	17.00	17.50	17.80	18.00	18.30	18.60	
Situational Awareness	Low Level Situational Awareness	2131.97	13670	19.70	20.30	21.00	21.60	22.10	22.70	
Situational Awareness	Media Monitoring	82.23	704	9.50	9.70	9.90	10.00	10.10	10.20	
Situational Awareness	Proactive Cyber Surveillance	563.31	3590	18.70	19.30	19.50	19.70	20.00	20.30	
System Recovery & Data Cleansing	Data Recovery Services	818.58	4473	17.30	17.80	18.00	18.30	18.50	18.70	
System Recovery & Data Cleansing	Manual Data Cleansing	398.08	2367	17.00	17.50	17.70	18.00	18.20	18.40	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	1297.82	8061	16.60	17.10	17.40	17.60	17.80	18.00	
Training & Education	Access Management	1.52	4	6.60	6.80	7.00	7.20	7.40	7.60	
Training & Education	Anti Spam Solutions	0.53	1	4.30	4.40	4.50	4.60	4.80	5.00	
Training & Education	Anti Virus/Worm	0.12	0	5.60	5.80	5.90	6.10	6.30	6.50	
Training & Education	Application Code Security	0.93	3	4.50	4.60	4.70	4.90	5.00	5.10	
Training & Education	Business Continuity/Recovery	0.45	0	6.80	7.00	7.20	7.40	7.60	7.80	
Training & Education	Computer Forensics	0.25	0	6.70	6.90	7.10	7.30	7.60	7.70	
Training & Education	Content Filtering & Monitoring	0.69	1	4.90	5.00	5.20	5.30	5.40	5.70	
Training & Education	Encryption/PKI/Digital Certificates	0.65	1	6.00	6.20	6.30	6.50	6.70	6.90	
Training & Education	Firewalls	0.42	1	4.60	4.80	4.90	5.10	5.20	5.40	
Training & Education	Identity Management	2.73	15	5.10	5.30	5.40	5.60	5.80	5.90	
Training & Education	Intrusion Detection	0.61	1	4.30	4.40	4.50	4.60	4.80	4.90	
Training & Education	Malware	0.26	0	5.40	5.50	5.70	5.90	6.00	6.20	
Training & Education	Messaging Security	1.16	3	5.00	5.20	5.30	5.50	5.70	5.80	
Training & Education	Mobile Security/Device management	1.46	4	5.10	5.20	5.40	5.50	5.70	5.90	
Training & Education	Patch Management	0.32	1	5.60	5.80	6.00	6.20	6.40	6.60	
Training & Education	PC/Mobile/End Point Security	2.66	14	6.40	6.70	6.80	7.10	7.30	7.50	
Training & Education	Vulnerability Assessment	0.86	1	6.80	7.10	7.30	7.50	7.70	7.90	
Training & Education	Wireless Security	1.19	4	5.30	5.50	5.70	5.80	6.00	6.20	

1.1.54 Germany

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	65.46	546	5.20	5.30	5.50	5.60	5.80	6.00	
Anti Malware	Anti Virus/Worm	263.72	2029	10.20	10.60	10.90	11.20	11.60	11.80	
Anti Malware	Malware	98.21	727	6.60	6.80	7.00	7.20	7.40	7.60	
Anti Malware	Specialist Anti Malware	1255.94	7354	17.30	17.90	18.40	18.90	19.40	19.90	
Application Security	Application Code Security	60.72	437	5.80	5.90	6.10	6.30	6.50	6.60	
Application Security	Content Filtering & Monitoring	41.43	277	6.50	6.70	6.90	7.10	7.20	7.40	
Application Security	Patch Management	61.31	439	6.50	6.70	6.90	7.10	7.30	7.50	
Application Security	Vulnerability Assessment	7435.48	46582	19.90	20.40	21.10	21.70	22.40	23.00	
Business Continuity	Business Continuity/Recovery	196.57	1220	17.10	17.60	18.10	18.60	19.20	19.90	
Business Continuity	Computer Forensics	143.88	1040	27.90	28.70	29.10	29.50	29.80	30.20	
Business Continuity	IT/Cyber Forensics	1897.30	12242	12.90	13.30	13.70	14.20	14.60	15.00	
Cyber Consultancy	Access Management	7.02	43	5.10	5.20	5.30	5.50	5.70	5.80	
Cyber Consultancy	Anti Spam Solutions	5.23	49	8.70	9.00	9.20	9.50	9.70	10.10	
Cyber Consultancy	Anti Virus/Worm	5.23	32	5.90	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	Application Code Security	4.33	30	3.90	4.00	4.10	4.30	4.40	4.50	
Cyber Consultancy	Business Continuity/Recovery	3.41	26	4.40	4.60	4.70	4.90	5.00	5.20	
Cyber Consultancy	Computer Forensics	7.13	39	4.90	5.10	5.30	5.50	5.60	5.80	
Cyber Consultancy	Content Filtering & Monitoring	4.08	27	6.50	6.70	6.90	7.10	7.30	7.50	
Cyber Consultancy	Corporate Services	335.75	2426	30.30	31.30	31.70	32.10	32.50	32.90	
Cyber Consultancy	Encryption/PKI/Digital Certificates	7.71	53	6.50	6.70	6.90	7.10	7.30	7.50	
Cyber Consultancy	Firewalls	1.75	10	3.40	3.50	3.50	3.70	3.80	3.90	
Cyber Consultancy	Identity Management	10.07	75	5.30	5.50	5.60	5.80	6.00	6.10	
Cyber Consultancy	Intrusion Detection	4.71	29	5.60	5.70	5.90	6.10	6.30	6.50	
Cyber Consultancy	Malware	6.99	46	5.80	6.00	6.20	6.30	6.50	6.70	
Cyber Consultancy	Messaging Security	7.82	44	4.00	4.20	4.30	4.50	4.60	4.70	
Cyber Consultancy	Mobile Security/Device management	8.41	57	4.90	5.00	5.20	5.30	5.50	5.60	
Cyber Consultancy	Patch Management	6.24	42	8.90	9.10	9.40	9.70	10.10	10.40	
Cyber Consultancy	PC/Mobile/End Point Security	3.59	23	6.10	6.30	6.50	6.70	6.90	7.20	
Cyber Consultancy	Vulnerability Assessment	5.92	42	6.50	6.70	6.90	7.10	7.30	7.60	
Cyber Consultancy	Wireless Security	3.77	26	4.90	5.10	5.30	5.40	5.60	5.80	
Cyber Security Insurance	Business Interruption from Network Downtime	111.53	790	11.60	12.00	12.40	12.70	13.10	13.50	
Cyber Security Insurance	Cyber Extortion	100.04	708	10.90	11.30	11.60	12.00	12.30	12.70	
Cyber Security Insurance	Investigation of Privacy Breach	22.28	167	9.90	10.10	10.40	10.80	11.10	11.40	
Cyber Security Insurance	Loss of Third Party Data	138.78	961	11.00	11.30	11.60	12.00	12.30	12.70	
Cyber Security Insurance	Loss or Damage to Digital Assets	91.91	614	10.80	11.20	11.60	11.90	12.30	12.60	
Cyber Security Insurance	Multi-Media Liability	85.29	643	11.10	11.50	11.80	12.20	12.60	12.90	
Cyber Security Insurance	Reputational Damage	51.76	336	11.40	11.80	12.10	12.50	12.80	13.20	
Cyber Security Insurance	Security and Privacy Breaches	138.61	942	11.30	11.70	12.00	12.40	12.70	13.10	
Cyber Security Insurance	Theft of Money and Digital Assets	73.01	473	10.80	11.20	11.50	11.90	12.20	12.60	
Cyber Security Insurance	Third Party Breach Notification	46.54	346	10.50	10.70	11.10	11.40	11.70	12.10	
Encryption	Digital Signatures	139.88	1009	37.20	38.50	39.00	39.50	40.00	40.50	
Encryption	Encryption/PKI/Digital Certificates	87.01	688	20.30	21.00	21.40	21.60	21.90	22.30	
Encryption	Storage Security, including Cloud	233.14	1674	35.20	36.10	36.60	37.20	37.60	38.20	
Identity & Access	Access Management	209.08	1653	7.60	7.90	8.20	8.40	8.60	8.90	
Identity & Access	Authentication	288.17	2001	39.10	40.20	40.70	41.20	41.80	42.40	
Identity & Access	Identity Management	870.96	6318	32.90	33.90	34.40	34.80	35.20	35.70	
Identity & Access	Intrusion & Anomaly Prevention	134.53	918	37.70	38.70	39.20	39.90	40.20	40.80	
Identity & Access	Messaging Security	165.07	1129	11.30	11.70	11.80	12.10	12.30	12.50	
Infrastructure	Data Management	258.56	1793	25.10	25.80	26.10	26.50	26.90	27.20	
Infrastructure	Firewalls	122.79	867	6.10	6.30	6.50	6.70	6.90	7.10	
Infrastructure	Infrastructure Monitoring	134.55	982	37.50	38.80	39.30	39.80	40.30	40.70	
Infrastructure	Infrastructure Resilience	133.58	981	40.50	41.50	41.90	42.30	42.80	43.50	
Infrastructure	Intrusion Detection	7285.08	42753	19.10	19.60	20.00	20.40	20.90	21.30	
Infrastructure	Outsourced/Managed Services	125.70	990	36.40	37.70	38.00	38.30	38.80	39.50	
Infrastructure	Storage Security, including Cloud	432.11	2907	37.50	38.80	39.40	39.80	40.30	40.80	
Mobile	Mobile Security/Device management	144.96	1242	6.10	6.30	6.50	6.60	6.80	7.00	
Mobile	PC/Mobile/End Point Security	131.77	952	8.70	8.90	9.20	9.50	9.80	10.10	
Mobile	VPN	150.82	1036	37.90	39.30	39.80	40.20	40.50	40.90	
Mobile	Wireless Security	148.95	1208	6.10	6.30	6.50	6.70	6.90	7.20	
Outsourced/Managed Services	Access Management	1.60	9	8.10	8.30	8.60	8.90	9.10	9.40	
Outsourced/Managed Services	Anti Spam Solutions	0.91	4	4.90	5.00	5.20	5.30	5.40	5.60	
Outsourced/Managed Services	Anti Virus/Worm	1.51	7	5.40	5.50	5.70	5.90	6.00	6.20	
Outsourced/Managed Services	Application Code Security	3.60	23	4.10	4.20	4.30	4.40	4.50	4.70	
Outsourced/Managed Services	Business Continuity/Recovery	0.78	3	6.20	6.50	6.70	6.80	7.00	7.30	
Outsourced/Managed Services	Content Filtering & Monitoring	1.31	8	7.50	7.80	8.00	8.30	8.50	8.70	
Outsourced/Managed Services	Cyber Services	419.99	3074	36.00	37.10	37.60	38.00	38.60	39.00	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	1.73	9	5.20	5.40	5.50	5.70	5.90	6.10	
Outsourced/Managed Services	Firewalls	2.80	19	5.80	5.90	6.10	6.30	6.50	6.70	
Outsourced/Managed Services	Identity Management	4.53	30	6.70	6.90	7.10	7.30	7.60	7.80	
Outsourced/Managed Services	Intrusion Detection	1.14	5	4.10	4.20	4.20	4.40	4.40	4.50	
Outsourced/Managed Services	Malware	0.49	1	5.60	5.70	5.90	6.10	6.20	6.40	
Outsourced/Managed Services	Messaging Security	3.73	23	4.50	4.70	4.80	4.90	5.10	5.20	
Outsourced/Managed Services	Mobile Security/Device management	3.07	16	5.70	5.90	6.10	6.30	6.50	6.70	
Outsourced/Managed Services	Patch Management	1.08	5	5.90	6.10	6.30	6.50	6.70	6.80	
Outsourced/Managed Services	PC/Mobile/End Point Security	1.38	8	5.00	5.20	5.40	5.50	5.70	5.90	
Outsourced/Managed Services	Vulnerability Assessment	2.86	12	6.90	7.10	7.30	7.50	7.80	8.10	
Outsourced/Managed Services	Wireless Security	1.87	12	5.80	6.00	6.10	6.40	6.50	6.70	
Situational Awareness	Darkweb	23.13	182	12.10	12.40	12.60	12.70	12.80	13.00	
Situational Awareness	External Cyber Threat Intelligence	1357.71	7426	14.70	15.10	15.40	15.60	16.00	16.20	
Situational Awareness	High Level Situational Awareness	1224.07	9144	12.70	13.00	13.40	13.80	14.30	14.70	
Situational Awareness	Internal Cyber Threat Intelligence	287.58	1657	18.20	18.70	19.10	19.50	19.80	20.20	
Situational Awareness	Low Level Situational Awareness	2784.30	15940	18.50	19.00	19.50	20.10	20.60	21.20	
Situational Awareness	Media Monitoring	123.68	872	13.10	13.50	13.70	13.90	14.00	14.20	
Situational Awareness	Proactive Cyber Surveillance	634.15	3821	15.60	16.20	16.40	16.60	16.80	17.00	
System Recovery & Data Cleansing	Data Recovery Services	973.10	5361	16.70	17.20	17.40	17.60	17.90	18.10	
System Recovery & Data Cleansing	Manual Data Cleansing	423.91	2719	15.30	15.80	16.00	16.30	16.50	16.70	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	1934.69	11931	17.90	18.40	18.70	19.00	19.20	19.50	
Training & Education	Access Management	2.61	11	8.10	8.30	8.50	8.80	9.00	9.30	
Training & Education	Anti Spam Solutions	0.80	4	4.40	4.50	4.60	4.80	4.90	5.10	
Training & Education	Anti Virus/Worm	0.15	0	5.70	5.90	6.00	6.20	6.40	6.60	
Training & Education	Application Code Security	1.51	7	4.30	4.40	4.50	4.60	4.80	5.00	
Training & Education	Business Continuity/Recovery	0.44	3	5.00	5.20	5.40	5.60	5.80	5.90	
Training & Education	Computer Forensics	0.17	0	5.10	5.20	5.40	5.50	5.70	5.80	
Training & Education	Content Filtering & Monitoring	0.77	1	6.60	6.80	7.00	7.20	7.50	7.70	
Training & Education	Encryption/PKI/Digital Certificates	0.76	1	6.40	6.60	6.80	7.00	7.20	7.50	
Training & Education	Firewalls	0.42	1	3.90	4.00	4.20	4.30	4.40	4.60	
Training & Education	Identity Management	4.41	29	5.90	6.10	6.30	6.50	6.70	6.90	
Training & Education	Intrusion Detection	0.94	4	4.50	4.70	4.80	4.90	5.10	5.20	
Training & Education	Malware	0.39	0	5.80	6.00	6.10	6.30	6.50	6.70	
Training & Education	Messaging Security	1.69	8	6.10	6.30	6.50	6.60	6.80	7.10	
Training & Education	Mobile Security/Device management	1.85	12	5.20	5.30	5.40	5.60	5.80	6.00	
Training & Education	Patch Management	0.48	1	6.30	6.50	6.70	7.00	7.10	7.40	
Training & Education	PC/Mobile/End Point Security	2.19	12	5.90	6.10	6.30	6.50	6.70	6.90	
Training & Education	Vulnerability Assessment	0.98	4	5.90	6.10	6.20	6.40	6.60	6.80	
Training & Education	Wireless Security	2.11	12	5.90	6.10	6.30	6.40	6.60	6.90	

1.1.55 Greece

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	7.51	46	7.90	8.10	8.40	8.70	8.90	9.20	
Anti Malware	Anti Virus/Worm	15.64	118	7.10	7.30	7.50	7.70	7.90	8.10	
Anti Malware	Malware	3.63	23	6.80	7.00	7.20	7.40	7.60	7.90	
Anti Malware	Specialist Anti Malware	30.81	132	23.00	23.70	24.50	25.30	26.00	26.80	
Application Security	Application Code Security	4.75	38	4.50	4.70	4.80	5.00	5.20	5.30	
Application Security	Content Filtering & Monitoring	4.37	30	6.90	7.10	7.30	7.50	7.80	8.00	
Application Security	Patch Management	2.42	14	6.20	6.40	6.60	6.80	7.00	7.20	
Application Security	Vulnerability Assessment	124.30	661	18.00	18.60	19.20	19.70	20.40	20.90	
Business Continuity	Business Continuity/Recovery	18.45	102	13.10	13.60	14.00	14.40	14.90	15.30	
Business Continuity	Computer Forensics	10.29	71	11.10	11.50	11.70	11.90	12.10	12.30	
Business Continuity	IT/Cyber Forensics	78.76	404	15.80	16.20	16.70	17.30	17.80	18.30	
Cyber Consultancy	Access Management	0.59	0	5.90	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	Anti Spam Solutions	0.44	0	5.20	5.40	5.60	5.70	5.90	6.10	
Cyber Consultancy	Anti Virus/Worm	0.45	0	4.80	4.90	5.10	5.20	5.40	5.60	
Cyber Consultancy	Application Code Security	0.53	0	5.20	5.40	5.60	5.70	5.90	6.10	
Cyber Consultancy	Business Continuity/Recovery	0.49	0	5.30	5.50	5.60	5.80	6.00	6.20	
Cyber Consultancy	Computer Forensics	0.47	0	5.40	5.50	5.70	5.90	6.10	6.20	
Cyber Consultancy	Content Filtering & Monitoring	0.34	0	4.30	4.40	4.60	4.70	4.90	5.00	
Cyber Consultancy	Corporate Services	22.01	159	12.70	13.00	13.20	13.40	13.50	13.70	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.61	0	7.30	7.50	7.70	7.90	8.10	8.40	
Cyber Consultancy	Firewalls	0.28	0	3.70	3.80	3.90	4.00	4.10	4.20	
Cyber Consultancy	Identity Management	0.89	3	4.60	4.70	4.90	5.00	5.10	5.30	
Cyber Consultancy	Intrusion Detection	0.43	0	3.80	3.90	4.00	4.10	4.30	4.40	
Cyber Consultancy	Malware	0.72	0	5.00	5.20	5.40	5.50	5.70	5.90	
Cyber Consultancy	Messaging Security	0.67	1	5.70	5.90	6.00	6.20	6.40	6.60	
Cyber Consultancy	Mobile Security/Device management	0.72	0	5.90	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	Patch Management	0.36	0	6.00	6.10	6.40	6.50	6.80	7.00	
Cyber Consultancy	PC/Mobile/End Point Security	0.33	0	6.20	6.40	6.60	6.70	7.00	7.20	
Cyber Consultancy	Vulnerability Assessment	0.59	0	7.30	7.50	7.70	8.00	8.20	8.50	
Cyber Consultancy	Wireless Security	0.36	0	6.60	6.80	7.10	7.30	7.50	7.70	
Cyber Security Insurance	Business Interruption from Network Downtime	10.10	73	10.50	10.80	11.20	11.50	11.90	12.20	
Cyber Security Insurance	Cyber Extortion	9.39	64	10.50	10.80	11.10	11.40	11.80	12.20	
Cyber Security Insurance	Investigation of Privacy Breach	2.59	16	11.60	11.90	12.30	12.70	13.00	13.40	
Cyber Security Insurance	Loss of Third Party Data	14.09	98	10.80	11.10	11.40	11.80	12.20	12.50	
Cyber Security Insurance	Loss or Damage to Digital Assets	8.95	64	10.60	10.90	11.20	11.50	11.80	12.20	
Cyber Security Insurance	Multi-Media Liability	8.52	61	10.20	10.50	10.80	11.10	11.40	11.80	
Cyber Security Insurance	Reputational Damage	4.45	31	9.90	10.20	10.50	10.80	11.10	11.50	
Cyber Security Insurance	Security and Privacy Breaches	13.53	94	11.10	11.50	11.80	12.10	12.50	12.90	
Cyber Security Insurance	Theft of Money and Digital Assets	7.00	47	10.50	10.80	11.20	11.50	11.90	12.20	
Cyber Security Insurance	Third Party Breach Notification	4.86	32	10.60	10.90	11.20	11.60	11.90	12.30	
Encryption	Digital Signatures	7.49	63	15.20	15.70	15.90	16.10	16.30	16.50	
Encryption	Encryption/PKI/Digital Certificates	6.93	42	9.90	10.20	10.40	10.60	10.80	11.00	
Encryption	Storage Security, including Cloud	13.96	99	14.80	15.30	15.50	15.70	15.90	16.00	
Identity & Access	Access Management	5.59	30	8.70	9.00	9.30	9.50	9.80	10.10	
Identity & Access	Authentication	16.47	124	16.70	17.30	17.50	17.80	18.00	18.20	
Identity & Access	Identity Management	53.06	369	15.10	15.60	15.80	16.00	16.20	16.40	
Identity & Access	Intrusion & Anomaly Prevention	7.78	59	15.80	16.40	16.50	16.70	16.90	17.10	
Identity & Access	Messaging Security	14.29	88	8.60	8.80	9.00	9.10	9.30	9.40	
Infrastructure	Data Management	16.43	114	11.00	11.30	11.50	11.60	11.70	11.90	
Infrastructure	Firewalls	4.92	28	4.80	5.00	5.10	5.30	5.40	5.60	
Infrastructure	Infrastructure Monitoring	7.22	52	16.50	17.00	17.20	17.50	17.70	18.00	
Infrastructure	Infrastructure Resilience	7.47	58	17.00	17.50	17.90	18.10	18.30	18.50	
Infrastructure	Intrusion Detection	122.70	732	15.10	15.60	15.90	16.20	16.60	17.00	
Infrastructure	Outsourced/Managed Services	9.12	57	15.90	16.30	16.50	16.70	16.90	17.20	
Infrastructure	Storage Security, including Cloud	24.21	175	16.40	16.90	17.10	17.30	17.50	17.70	
Mobile	Mobile Security/Device management	7.69	53	6.40	6.70	6.90	7.10	7.30	7.50	
Mobile	PC/Mobile/End Point Security	7.34	39	8.20	8.50	8.80	9.00	9.30	9.50	
Mobile	VPN	8.77	54	16.40	16.90	17.10	17.20	17.50	17.80	
Mobile	Wireless Security	13.91	100	5.60	5.80	6.00	6.10	6.30	6.50	
Outsourced/Managed Services	Access Management	0.15	0	6.30	6.50	6.70	6.90	7.20	7.30	
Outsourced/Managed Services	Anti Spam Solutions	0.09	0	6.30	6.50	6.70	6.90	7.20	7.40	
Outsourced/Managed Services	Anti Virus/Worm	0.20	0	5.70	5.80	6.00	6.20	6.40	6.60	
Outsourced/Managed Services	Application Code Security	0.34	0	4.80	4.90	5.00	5.20	5.30	5.50	
Outsourced/Managed Services	Business Continuity/Recovery	0.09	0	6.10	6.30	6.50	6.70	6.90	7.10	
Outsourced/Managed Services	Content Filtering & Monitoring	0.17	0	6.60	6.80	7.00	7.20	7.40	7.50	
Outsourced/Managed Services	Cyber Services	24.60	191	15.50	16.00	16.20	16.40	16.60	16.80	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.17	0	5.50	5.70	5.80	6.10	6.20	6.50	
Outsourced/Managed Services	Firewalls	0.27	0	4.00	4.10	4.30	4.30	4.50	4.70	
Outsourced/Managed Services	Identity Management	0.45	0	5.50	5.60	5.80	6.00	6.10	6.30	
Outsourced/Managed Services	Intrusion Detection	0.12	0	5.70	5.90	6.00	6.20	6.30	6.40	
Outsourced/Managed Services	Malware	0.05	0	4.90	5.00	5.20	5.30	5.50	5.60	
Outsourced/Managed Services	Messaging Security	0.39	0	4.40	4.60	4.70	4.90	5.00	5.20	
Outsourced/Managed Services	Mobile Security/Device management	0.28	0	6.70	6.90	7.20	7.40	7.50	7.80	
Outsourced/Managed Services	Patch Management	0.10	0	6.00	6.20	6.30	6.60	6.80	7.00	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.14	0	7.30	7.50	7.80	7.90	8.20	8.40	
Outsourced/Managed Services	Vulnerability Assessment	0.22	0	5.80	6.00	6.10	6.30	6.50	6.80	
Outsourced/Managed Services	Wireless Security	0.17	0	7.30	7.50	7.70	7.90	8.10	8.30	
Situational Awareness	Darkweb	1.88	13	5.20	5.30	5.40	5.50	5.50	5.60	
Situational Awareness	External Cyber Threat Intelligence	163.85	904	15.80	16.30	16.60	16.90	17.20	17.50	
Situational Awareness	High Level Situational Awareness	124.28	672	11.90	12.20	12.60	13.00	13.40	13.80	
Situational Awareness	Internal Cyber Threat Intelligence	19.93	111	14.10	14.50	14.70	15.00	15.20	15.50	
Situational Awareness	Low Level Situational Awareness	22.81	121	14.40	14.80	15.30	15.70	16.20	16.70	
Situational Awareness	Media Monitoring	8.96	70	5.50	5.60	5.70	5.80	5.90	5.90	
Situational Awareness	Proactive Cyber Surveillance	72.13	395	16.20	16.70	16.90	17.10	17.30	17.60	
System Recovery & Data Cleansing	Data Recovery Services	99.16	549	15.90	16.40	16.60	16.80	17.00	17.20	
System Recovery & Data Cleansing	Manual Data Cleansing	45.42	251	15.30	15.80	16.00	16.20	16.40	16.60	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	186.87	1064	15.70	16.10	16.40	16.60	16.80	17.00	
Training & Education	Access Management	0.17	0	5.50	5.60	5.80	6.00	6.10	6.30	
Training & Education	Anti Spam Solutions	0.10	0	8.40	8.70	9.00	9.30	9.50	9.80	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.15	0	4.90	5.10	5.20	5.40	5.60	5.70	
Training & Education	Business Continuity/Recovery	0.04	0	5.90	6.00	6.20	6.30	6.50	6.80	
Training & Education	Computer Forensics	0.01	0	5.40	5.60	5.80	6.00	6.10	6.30	
Training & Education	Content Filtering & Monitoring	0.09	0	4.30	4.40	4.60	4.70	4.90	5.00	
Training & Education	Encryption/PKI/Digital Certificates	0.10	0	6.00	6.20	6.40	6.60	6.80	7.00	
Training & Education	Firewalls	0.05	0	6.90	7.10	7.30	7.40	7.60	7.80	
Training & Education	Identity Management	0.38	0	4.90	5.00	5.10	5.30	5.40	5.60	
Training & Education	Intrusion Detection	0.07	0	4.40	4.50	4.70	4.80	4.90	5.00	
Training & Education	Malware	0.05	0	8.10	8.30	8.60	8.80	9.10	9.40	
Training & Education	Messaging Security	0.16	0	4.30	4.40	4.60	4.70	4.80	5.00	
Training & Education	Mobile Security/Device management	0.22	0	6.00	6.10	6.30	6.50	6.70	7.00	
Training & Education	Patch Management	0.04	0	7.50	7.70	8.00	8.20	8.50	8.80	
Training & Education	PC/Mobile/End Point Security	0.25	0	5.10	5.20	5.40	5.50	5.70	5.80	
Training & Education	Vulnerability Assessment	0.10	0	5.20	5.30	5.50	5.60	5.80	6.00	
Training & Education	Wireless Security	0.18	0	5.90	6.10	6.30	6.50	6.70	6.90	

1.1.56 Hungary

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	3.76	26	4.20	4.30	4.50	4.60	4.80	4.90	
Anti Malware	Anti Virus/Worm	9.84	70	6.20	6.40	6.60	6.90	7.10	7.30	
Anti Malware	Malware	2.17	12	6.10	6.30	6.50	6.70	6.90	7.10	
Anti Malware	Specialist Anti Malware	12.57	73	13.50	13.90	14.30	14.80	15.30	15.80	
Application Security	Application Code Security	3.73	23	5.50	5.60	5.80	6.00	6.10	6.30	
Application Security	Content Filtering & Monitoring	2.73	18	6.40	6.50	6.70	6.90	7.20	7.40	
Application Security	Patch Management	1.42	8	5.10	5.20	5.40	5.60	5.70	5.90	
Application Security	Vulnerability Assessment	72.74	434	15.20	15.70	16.10	16.60	17.10	17.60	
Business Continuity	Business Continuity/Recovery	13.75	68	14.70	15.20	15.60	16.10	16.60	17.10	
Business Continuity	Computer Forensics	6.24	45	9.60	9.90	10.10	10.20	10.30	10.50	
Business Continuity	IT/Cyber Forensics	48.75	243	13.40	13.80	14.20	14.60	15.10	15.50	
Cyber Consultancy	Access Management	0.47	1	6.30	6.50	6.70	6.90	7.10	7.30	
Cyber Consultancy	Anti Spam Solutions	0.33	1	6.30	6.50	6.70	6.90	7.10	7.30	
Cyber Consultancy	Anti Virus/Worm	0.33	1	4.50	4.70	4.80	5.00	5.10	5.30	
Cyber Consultancy	Application Code Security	0.32	0	6.40	6.60	6.80	7.00	7.20	7.40	
Cyber Consultancy	Business Continuity/Recovery	0.22	1	4.10	4.30	4.30	4.50	4.60	4.80	
Cyber Consultancy	Computer Forensics	0.40	1	4.20	4.30	4.50	4.60	4.70	4.90	
Cyber Consultancy	Content Filtering & Monitoring	0.31	1	6.10	6.30	6.50	6.70	6.90	7.20	
Cyber Consultancy	Corporate Services	14.00	100	10.20	10.40	10.50	10.70	10.80	10.90	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.54	1	5.30	5.50	5.60	5.70	5.90	6.10	
Cyber Consultancy	Firewalls	0.18	0	4.30	4.50	4.60	4.70	4.90	5.00	
Cyber Consultancy	Identity Management	0.39	1	4.10	4.20	4.40	4.50	4.60	4.70	
Cyber Consultancy	Intrusion Detection	0.32	1	5.80	6.00	6.20	6.30	6.50	6.70	
Cyber Consultancy	Malware	0.43	1	5.50	5.70	5.90	6.10	6.20	6.40	
Cyber Consultancy	Messaging Security	0.55	1	4.20	4.30	4.50	4.60	4.80	4.90	
Cyber Consultancy	Mobile Security/Device management	0.40	1	5.30	5.40	5.60	5.80	6.00	6.10	
Cyber Consultancy	Patch Management	0.22	1	4.50	4.60	4.70	4.90	5.10	5.20	
Cyber Consultancy	PC/Mobile/End Point Security	0.28	1	6.60	6.80	7.00	7.20	7.40	7.70	
Cyber Consultancy	Vulnerability Assessment	0.37	1	6.10	6.30	6.50	6.70	6.90	7.10	
Cyber Consultancy	Wireless Security	0.21	1	3.60	3.80	3.90	4.00	4.10	4.20	
Cyber Security Insurance	Business Interruption from Network Downtime	6.42	47	10.70	11.00	11.30	11.70	12.00	12.40	
Cyber Security Insurance	Cyber Extortion	6.27	41	10.20	10.50	10.80	11.10	11.40	11.70	
Cyber Security Insurance	Investigation of Privacy Breach	1.60	11	10.00	10.30	10.60	11.00	11.30	11.60	
Cyber Security Insurance	Loss of Third Party Data	8.82	62	11.70	12.00	12.40	12.80	13.10	13.50	
Cyber Security Insurance	Loss or Damage to Digital Assets	5.57	39	10.40	10.80	11.10	11.40	11.70	12.00	
Cyber Security Insurance	Multi-Media Liability	5.32	37	10.90	11.20	11.60	11.90	12.30	12.60	
Cyber Security Insurance	Reputational Damage	3.26	24	11.00	11.40	11.70	12.10	12.50	12.90	
Cyber Security Insurance	Security and Privacy Breaches	8.97	61	11.20	11.50	11.90	12.20	12.60	13.10	
Cyber Security Insurance	Theft of Money and Digital Assets	4.86	33	10.50	10.80	11.10	11.40	11.80	12.20	
Cyber Security Insurance	Third Party Breach Notification	3.33	23	11.50	11.80	12.20	12.60	13.00	13.40	
Encryption	Digital Signatures	4.37	30	12.50	12.90	13.10	13.20	13.40	13.60	
Encryption	Encryption/PKI/Digital Certificates	4.37	28	8.30	8.60	8.70	8.80	9.00	9.10	
Encryption	Storage Security, including Cloud	8.68	61	12.10	12.50	12.60	12.80	12.90	13.10	
Identity & Access	Access Management	2.74	14	4.80	4.90	5.10	5.20	5.40	5.60	
Identity & Access	Authentication	10.03	76	14.10	14.50	14.70	14.80	15.00	15.20	
Identity & Access	Identity Management	31.27	223	12.10	12.50	12.70	12.80	13.00	13.10	
Identity & Access	Intrusion & Anomaly Prevention	5.10	34	12.80	13.20	13.40	13.60	13.80	14.00	
Identity & Access	Messaging Security	7.93	63	9.60	9.90	10.10	10.30	10.50	10.70	
Infrastructure	Data Management	9.33	68	8.70	9.00	9.00	9.20	9.30	9.40	
Infrastructure	Firewalls	2.44	15	5.20	5.40	5.60	5.70	5.90	6.10	
Infrastructure	Infrastructure Monitoring	4.64	36	13.90	14.30	14.50	14.70	14.90	15.10	
Infrastructure	Infrastructure Resilience	4.42	36	13.60	14.00	14.10	14.40	14.50	14.70	
Infrastructure	Intrusion Detection	82.09	449	14.50	15.00	15.30	15.70	16.00	16.30	
Infrastructure	Outsourced/Managed Services	5.89	47	12.50	12.80	12.90	13.10	13.30	13.40	
Infrastructure	Storage Security, including Cloud	15.84	129	13.10	13.50	13.70	13.90	14.00	14.20	
Mobile	Mobile Security/Device management	3.87	25	5.70	5.80	6.00	6.20	6.40	6.60	
Mobile	PC/Mobile/End Point Security	5.72	28	12.20	12.50	12.90	13.20	13.60	13.90	
Mobile	VPN	4.93	36	12.90	13.20	13.40	13.70	13.90	14.10	
Mobile	Wireless Security	7.10	54	5.00	5.10	5.30	5.50	5.60	5.80	
Outsourced/Managed Services	Access Management	0.10	0	4.30	4.40	4.50	4.60	4.80	4.90	
Outsourced/Managed Services	Anti Spam Solutions	0.07	0	5.60	5.70	5.90	6.10	6.30	6.50	
Outsourced/Managed Services	Anti Virus/Worm	0.10	0	6.20	6.40	6.60	6.80	7.00	7.20	
Outsourced/Managed Services	Application Code Security	0.21	0	5.80	5.90	6.10	6.30	6.50	6.70	
Outsourced/Managed Services	Business Continuity/Recovery	0.04	0	3.90	4.00	4.10	4.30	4.40	4.50	
Outsourced/Managed Services	Content Filtering & Monitoring	0.09	0	5.70	5.90	6.10	6.30	6.40	6.60	
Outsourced/Managed Services	Cyber Services	15.66	117	12.30	12.60	12.80	13.00	13.20	13.30	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.07	0	6.20	6.40	6.70	6.80	7.00	7.30	
Outsourced/Managed Services	Firewalls	0.17	1	5.70	5.80	6.00	6.20	6.40	6.60	
Outsourced/Managed Services	Identity Management	0.26	1	5.40	5.60	5.80	6.00	6.20	6.30	
Outsourced/Managed Services	Intrusion Detection	0.07	0	6.20	6.50	6.60	6.70	6.80	6.90	
Outsourced/Managed Services	Malware	0.01	0	4.20	4.30	4.40	4.60	4.70	4.80	
Outsourced/Managed Services	Messaging Security	0.17	0	6.10	6.30	6.50	6.70	7.00	7.10	
Outsourced/Managed Services	Mobile Security/Device management	0.21	0	5.10	5.30	5.40	5.60	5.70	5.90	
Outsourced/Managed Services	Patch Management	0.07	0	4.90	5.00	5.20	5.30	5.50	5.60	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.09	0	6.10	6.30	6.50	6.70	6.90	7.10	
Outsourced/Managed Services	Vulnerability Assessment	0.16	0	8.20	8.40	8.60	8.90	9.20	9.50	
Outsourced/Managed Services	Wireless Security	0.07	0	5.00	5.10	5.30	5.50	5.60	5.80	
Situational Awareness	Darkweb	1.29	8	4.40	4.50	4.60	4.70	4.70	4.80	
Situational Awareness	External Cyber Threat Intelligence	99.44	632	17.70	18.20	18.50	18.80	19.10	19.40	
Situational Awareness	High Level Situational Awareness	83.66	570	12.90	13.20	13.60	14.00	14.40	14.90	
Situational Awareness	Internal Cyber Threat Intelligence	19.56	92	17.80	18.40	18.70	19.10	19.40	19.70	
Situational Awareness	Low Level Situational Awareness	17.56	101	13.50	13.90	14.40	14.90	15.30	15.70	
Situational Awareness	Media Monitoring	6.41	46	4.60	4.70	4.80	4.80	4.90	4.90	
Situational Awareness	Proactive Cyber Surveillance	50.12	267	18.80	19.20	19.50	19.70	20.00	20.20	
System Recovery & Data Cleansing	Data Recovery Services	72.19	360	16.80	17.40	17.60	17.80	18.00	18.30	
System Recovery & Data Cleansing	Manual Data Cleansing	35.52	162	20.10	20.70	21.00	21.30	21.50	21.80	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	145.05	765	19.50	20.10	20.40	20.60	20.80	21.10	
Training & Education	Access Management	0.11	0	4.20	4.30	4.40	4.50	4.70	4.80	
Training & Education	Anti Spam Solutions	0.01	0	3.90	4.10	4.10	4.20	4.40	4.50	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.06	0	5.20	5.40	5.60	5.70	5.90	6.10	
Training & Education	Business Continuity/Recovery	0.01	0	6.60	6.80	7.00	7.30	7.50	7.70	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.02	0	5.20	5.40	5.50	5.70	5.90	6.00	
Training & Education	Encryption/PKI/Digital Certificates	0.04	0	4.20	4.40	4.50	4.70	4.80	4.90	
Training & Education	Firewalls	0.02	0	4.00	4.10	4.30	4.40	4.50	4.60	
Training & Education	Identity Management	0.17	0	4.60	4.70	4.90	5.00	5.20	5.30	
Training & Education	Intrusion Detection	0.04	0	6.00	6.20	6.40	6.60	6.80	7.00	
Training & Education	Malware	0.01	0	4.40	4.60	4.80	4.90	5.00	5.10	
Training & Education	Messaging Security	0.10	0	5.10	5.30	5.40	5.60	5.70	5.90	
Training & Education	Mobile Security/Device management	0.11	0	4.80	4.90	5.10	5.20	5.40	5.50	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.12	0	4.90	5.00	5.20	5.30	5.50	5.60	
Training & Education	Vulnerability Assessment	0.06	0	7.30	7.50	7.70	8.00	8.20	8.50	
Training & Education	Wireless Security	0.10	0	5.50	5.60	5.80	6.00	6.10	6.30	

1.1.57 Ireland

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	3.22	13	5.80	6.00	6.20	6.30	6.50	6.80	
Anti Malware	Anti Virus/Worm	11.78	69	10.20	10.50	10.90	11.30	11.60	12.00	
Anti Malware	Malware	2.95	18	5.10	5.30	5.40	5.50	5.70	5.90	
Anti Malware	Specialist Anti Malware	68.89	548	19.20	19.60	20.20	20.90	21.50	22.00	
Application Security	Application Code Security	2.39	12	7.70	7.90	8.20	8.50	8.70	9.00	
Application Security	Content Filtering & Monitoring	2.01	12	4.20	4.30	4.50	4.60	4.80	4.90	
Application Security	Patch Management	1.10	6	2.70	2.80	2.90	3.00	3.10	3.20	
Application Security	Vulnerability Assessment	385.38	2683	17.60	18.10	18.60	19.20	19.80	20.40	
Business Continuity	Business Continuity/Recovery	13.73	96	18.30	18.80	19.40	20.00	20.60	21.20	
Business Continuity	Computer Forensics	6.22	48	22.00	22.70	23.00	23.30	23.80	24.20	
Business Continuity	IT/Cyber Forensics	126.00	883	14.50	14.90	15.40	15.90	16.30	16.80	
Cyber Consultancy	Access Management	0.28	2	3.70	3.80	3.90	4.00	4.10	4.30	
Cyber Consultancy	Anti Spam Solutions	0.27	1	6.80	6.90	7.20	7.30	7.60	7.80	
Cyber Consultancy	Anti Virus/Worm	0.31	2	4.50	4.60	4.70	4.90	5.00	5.20	
Cyber Consultancy	Application Code Security	0.26	1	5.50	5.70	5.90	6.00	6.20	6.40	
Cyber Consultancy	Business Continuity/Recovery	0.23	1	6.20	6.50	6.70	6.90	7.10	7.30	
Cyber Consultancy	Computer Forensics	0.26	1	3.40	3.40	3.50	3.70	3.80	3.90	
Cyber Consultancy	Content Filtering & Monitoring	0.17	1	4.80	5.00	5.10	5.30	5.40	5.60	
Cyber Consultancy	Corporate Services	17.77	127	25.90	26.70	27.00	27.40	27.70	28.10	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.33	2	7.50	7.80	8.00	8.20	8.50	8.70	
Cyber Consultancy	Firewalls	0.17	1	6.80	7.00	7.20	7.40	7.60	7.90	
Cyber Consultancy	Identity Management	0.36	3	3.40	3.50	3.60	3.80	3.90	4.00	
Cyber Consultancy	Intrusion Detection	0.20	1	6.50	6.80	6.90	7.20	7.40	7.60	
Cyber Consultancy	Malware	0.32	1	5.40	5.60	5.80	5.90	6.10	6.20	
Cyber Consultancy	Messaging Security	0.39	2	5.80	6.00	6.20	6.40	6.60	6.80	
Cyber Consultancy	Mobile Security/Device management	0.31	1	5.60	5.80	6.00	6.10	6.30	6.40	
Cyber Consultancy	Patch Management	0.16	2	6.20	6.40	6.60	6.70	6.90	7.10	
Cyber Consultancy	PC/Mobile/End Point Security	0.20	1	6.30	6.50	6.70	6.80	7.00	7.20	
Cyber Consultancy	Vulnerability Assessment	0.25	1	6.60	6.80	7.00	7.20	7.40	7.70	
Cyber Consultancy	Wireless Security	0.21	1	4.40	4.50	4.70	4.80	4.90	5.10	
Cyber Security Insurance	Business Interruption from Network Downtime	5.69	43	11.30	11.60	12.00	12.30	12.70	13.10	
Cyber Security Insurance	Cyber Extortion	5.70	40	11.10	11.50	11.90	12.20	12.60	12.90	
Cyber Security Insurance	Investigation of Privacy Breach	1.42	10	11.00	11.30	11.60	11.90	12.20	12.50	
Cyber Security Insurance	Loss of Third Party Data	7.94	55	10.80	11.10	11.40	11.80	12.10	12.50	
Cyber Security Insurance	Loss or Damage to Digital Assets	5.01	33	9.80	10.10	10.40	10.70	11.00	11.30	
Cyber Security Insurance	Multi-Media Liability	4.92	32	10.60	10.90	11.30	11.60	12.00	12.30	
Cyber Security Insurance	Reputational Damage	2.59	21	11.20	11.50	11.90	12.20	12.50	12.90	
Cyber Security Insurance	Security and Privacy Breaches	7.32	52	10.90	11.20	11.60	11.90	12.20	12.60	
Cyber Security Insurance	Theft of Money and Digital Assets	4.08	28	10.50	10.80	11.10	11.50	11.80	12.10	
Cyber Security Insurance	Third Party Breach Notification	2.46	17	9.50	9.80	10.10	10.30	10.70	11.00	
Encryption	Digital Signatures	6.06	44	30.80	31.70	32.20	32.50	33.10	33.50	
Encryption	Encryption/PKI/Digital Certificates	5.08	33	15.40	15.80	16.10	16.40	16.70	16.90	
Encryption	Storage Security, including Cloud	11.34	76	30.20	31.10	31.40	31.90	32.30	32.70	
Identity & Access	Access Management	3.93	33	4.00	4.10	4.20	4.40	4.50	4.70	
Identity & Access	Authentication	14.86	97	32.80	33.90	34.40	34.90	35.30	35.70	
Identity & Access	Identity Management	37.38	276	26.70	27.40	27.70	28.10	28.50	28.80	
Identity & Access	Intrusion & Anomaly Prevention	6.79	44	30.50	31.30	31.70	32.20	32.60	33.00	
Identity & Access	Messaging Security	12.46	106	11.50	11.90	12.10	12.30	12.50	12.70	
Infrastructure	Data Management	11.30	73	21.30	21.90	22.20	22.50	22.80	23.10	
Infrastructure	Firewalls	4.69	25	5.70	5.90	6.10	6.30	6.50	6.70	
Infrastructure	Infrastructure Monitoring	5.38	39	28.20	29.20	29.40	29.80	30.00	30.30	
Infrastructure	Infrastructure Resilience	5.84	41	33.70	34.80	35.40	35.90	36.40	36.80	
Infrastructure	Intrusion Detection	289.38	2503	15.50	16.00	16.30	16.60	16.90	17.20	
Infrastructure	Outsourced/Managed Services	5.91	55	30.90	31.80	32.00	32.40	32.90	33.30	
Infrastructure	Storage Security, including Cloud	22.53	163	32.00	32.90	33.20	33.60	34.00	34.50	
Mobile	Mobile Security/Device management	7.37	45	7.10	7.40	7.60	7.80	8.10	8.30	
Mobile	PC/Mobile/End Point Security	6.29	36	7.70	7.90	8.20	8.40	8.70	8.90	
Mobile	VPN	7.62	53	32.20	33.20	33.60	34.00	34.40	34.90	
Mobile	Wireless Security	5.69	52	5.20	5.40	5.60	5.70	5.90	6.10	
Outsourced/Managed Services	Access Management	0.09	0	7.30	7.50	7.60	7.90	8.10	8.40	
Outsourced/Managed Services	Anti Spam Solutions	0.05	0	2.60	2.70	2.80	2.90	3.00	3.10	
Outsourced/Managed Services	Anti Virus/Worm	0.07	0	3.10	3.20	3.20	3.30	3.50	3.60	
Outsourced/Managed Services	Application Code Security	0.17	1	7.60	7.90	8.10	8.40	8.60	8.90	
Outsourced/Managed Services	Business Continuity/Recovery	0.04	0	7.10	7.30	7.60	7.80	8.10	8.30	
Outsourced/Managed Services	Content Filtering & Monitoring	0.07	0	6.50	6.70	6.90	7.10	7.30	7.50	
Outsourced/Managed Services	Cyber Services	18.67	139	27.80	28.70	29.10	29.40	29.70	30.10	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.07	0	5.20	5.30	5.50	5.60	5.90	6.00	
Outsourced/Managed Services	Firewalls	0.14	0	5.60	5.70	5.90	6.10	6.20	6.50	
Outsourced/Managed Services	Identity Management	0.21	1	5.60	5.80	5.90	6.10	6.30	6.50	
Outsourced/Managed Services	Intrusion Detection	0.07	0	6.90	7.10	7.20	7.30	7.50	7.70	
Outsourced/Managed Services	Malware	0.01	0	4.80	4.90	5.00	5.20	5.30	5.50	
Outsourced/Managed Services	Messaging Security	0.21	1	5.60	5.80	6.00	6.20	6.40	6.50	
Outsourced/Managed Services	Mobile Security/Device management	0.15	1	5.50	5.70	5.80	6.00	6.20	6.40	
Outsourced/Managed Services	Patch Management	0.01	0	4.30	4.40	4.50	4.60	4.80	4.90	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.07	0	7.50	7.70	8.00	8.20	8.40	8.70	
Outsourced/Managed Services	Vulnerability Assessment	0.09	0	6.60	6.70	6.90	7.10	7.30	7.50	
Outsourced/Managed Services	Wireless Security	0.07	0	4.70	4.80	4.90	5.10	5.30	5.40	
Situational Awareness	Darkweb	1.15	10	9.90	10.10	10.30	10.50	10.50	10.70	
Situational Awareness	External Cyber Threat Intelligence	80.01	703	16.40	16.90	17.20	17.50	17.80	18.10	
Situational Awareness	High Level Situational Awareness	71.71	470	12.20	12.60	13.00	13.40	13.80	14.20	
Situational Awareness	Internal Cyber Threat Intelligence	16.81	131	18.10	18.70	19.00	19.30	19.60	19.90	
Situational Awareness	Low Level Situational Awareness	96.12	858	17.00	17.50	18.00	18.50	19.10	19.70	
Situational Awareness	Media Monitoring	6.03	41	11.80	12.20	12.30	12.40	12.60	12.70	
Situational Awareness	Proactive Cyber Surveillance	37.41	244	13.80	14.30	14.40	14.60	14.80	15.00	
System Recovery & Data Cleansing	Data Recovery Services	62.45	310	18.10	18.70	18.90	19.10	19.30	19.60	
System Recovery & Data Cleansing	Manual Data Cleansing	29.60	236	16.00	16.50	16.70	16.90	17.10	17.40	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	110.50	735	17.00	17.50	17.70	18.00	18.20	18.40	
Training & Education	Access Management	0.10	1	4.90	5.10	5.20	5.40	5.60	5.70	
Training & Education	Anti Spam Solutions	0.01	0	4.80	4.90	4.90	5.10	5.30	5.40	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.07	0	5.00	5.20	5.40	5.50	5.70	5.80	
Training & Education	Business Continuity/Recovery	0.01	0	8.50	8.70	9.00	9.30	9.50	9.70	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.02	0	9.50	9.80	10.10	10.30	10.80	11.20	
Training & Education	Encryption/PKI/Digital Certificates	0.05	0	5.10	5.30	5.50	5.60	5.80	6.00	
Training & Education	Firewalls	0.01	0	5.90	6.20	6.40	6.60	6.80	7.00	
Training & Education	Identity Management	0.21	1	7.10	7.30	7.50	7.70	7.90	8.20	
Training & Education	Intrusion Detection	0.04	0	7.10	7.30	7.50	7.70	7.90	8.10	
Training & Education	Malware	0.01	0	4.00	4.10	4.20	4.40	4.50	4.70	
Training & Education	Messaging Security	0.09	0	6.60	6.80	7.00	7.30	7.50	7.70	
Training & Education	Mobile Security/Device management	0.07	0	5.10	5.20	5.30	5.50	5.70	5.90	
Training & Education	Patch Management	0.01	0	4.30	4.40	4.50	4.60	4.80	4.90	
Training & Education	PC/Mobile/End Point Security	0.11	0	4.80	5.00	5.10	5.30	5.40	5.60	
Training & Education	Vulnerability Assessment	0.04	0	8.20	8.40	8.70	9.00	9.20	9.50	
Training & Education	Wireless Security	0.07	0	3.90	4.00	4.20	4.30	4.40	4.50	

1.1.58 Italy

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	45.25	341	5.40	5.60	5.70	5.90	6.10	6.30	
Anti Malware	Anti Virus/Worm	157.05	1137	7.60	7.80	8.00	8.20	8.50	8.70	
Anti Malware	Malware	45.53	320	5.40	5.60	5.70	5.90	6.00	6.20	
Anti Malware	Specialist Anti Malware	1560.77	9136	21.80	22.50	23.10	23.70	24.40	25.00	
Application Security	Application Code Security	38.74	263	5.10	5.30	5.40	5.60	5.80	6.00	
Application Security	Content Filtering & Monitoring	33.70	228	5.30	5.40	5.60	5.70	5.90	6.10	
Application Security	Patch Management	51.47	295	6.50	6.70	6.90	7.10	7.30	7.60	
Application Security	Vulnerability Assessment	3076.50	18502	16.30	16.80	17.30	17.80	18.40	18.90	
Business Continuity	Business Continuity/Recovery	129.96	709	14.60	15.00	15.50	15.90	16.40	16.90	
Business Continuity	Computer Forensics	75.71	519	13.80	14.30	14.50	14.80	15.00	15.20	
Business Continuity	IT/Cyber Forensics	1476.59	9043	16.70	17.20	17.70	18.20	18.70	19.30	
Cyber Consultancy	Access Management	3.65	22	4.30	4.50	4.60	4.70	4.90	5.00	
Cyber Consultancy	Anti Spam Solutions	3.10	19	9.80	10.10	10.30	10.70	11.00	11.20	
Cyber Consultancy	Anti Virus/Worm	4.14	21	6.50	6.70	6.90	7.10	7.30	7.60	
Cyber Consultancy	Application Code Security	3.90	31	7.80	8.00	8.20	8.50	8.70	9.00	
Cyber Consultancy	Business Continuity/Recovery	2.95	17	4.70	4.90	5.00	5.20	5.30	5.40	
Cyber Consultancy	Computer Forensics	4.66	27	4.70	4.80	4.90	5.10	5.20	5.40	
Cyber Consultancy	Content Filtering & Monitoring	3.08	17	5.50	5.70	5.90	6.10	6.30	6.50	
Cyber Consultancy	Corporate Services	159.67	1122	15.90	16.40	16.60	16.80	17.00	17.10	
Cyber Consultancy	Encryption/PKI/Digital Certificates	5.09	44	6.50	6.70	6.90	7.10	7.30	7.50	
Cyber Consultancy	Firewalls	1.68	9	5.00	5.20	5.30	5.50	5.60	5.80	
Cyber Consultancy	Identity Management	7.31	52	5.60	5.80	6.00	6.10	6.30	6.60	
Cyber Consultancy	Intrusion Detection	2.51	13	3.50	3.60	3.70	3.80	3.90	4.00	
Cyber Consultancy	Malware	4.12	28	4.80	5.00	5.10	5.30	5.40	5.60	
Cyber Consultancy	Messaging Security	5.03	32	5.40	5.50	5.70	5.90	6.10	6.30	
Cyber Consultancy	Mobile Security/Device management	5.21	34	4.20	4.30	4.50	4.60	4.70	4.90	
Cyber Consultancy	Patch Management	2.11	12	3.80	4.00	4.10	4.20	4.30	4.40	
Cyber Consultancy	PC/Mobile/End Point Security	2.31	14	5.30	5.40	5.60	5.80	6.00	6.20	
Cyber Consultancy	Vulnerability Assessment	3.50	24	4.40	4.60	4.70	4.90	5.00	5.20	
Cyber Consultancy	Wireless Security	3.51	18	7.50	7.70	7.90	8.10	8.40	8.70	
Cyber Security Insurance	Business Interruption from Network Downtime	74.96	457	10.70	11.10	11.40	11.70	12.10	12.40	
Cyber Security Insurance	Cyber Extortion	66.97	457	10.80	11.20	11.50	11.80	12.30	12.60	
Cyber Security Insurance	Investigation of Privacy Breach	18.23	130	12.10	12.50	12.90	13.30	13.70	14.20	
Cyber Security Insurance	Loss of Third Party Data	92.57	635	10.90	11.30	11.60	11.90	12.20	12.60	
Cyber Security Insurance	Loss or Damage to Digital Assets	62.01	422	10.90	11.30	11.60	11.90	12.30	12.60	
Cyber Security Insurance	Multi-Media Liability	59.88	394	10.90	11.20	11.60	12.00	12.40	12.70	
Cyber Security Insurance	Reputational Damage	34.04	226	10.90	11.20	11.50	11.80	12.10	12.50	
Cyber Security Insurance	Security and Privacy Breaches	86.57	602	10.20	10.50	10.80	11.20	11.50	11.90	
Cyber Security Insurance	Theft of Money and Digital Assets	50.03	347	12.20	12.60	12.90	13.30	13.70	14.10	
Cyber Security Insurance	Third Party Breach Notification	31.93	219	10.00	10.20	10.50	10.80	11.10	11.40	
Encryption	Digital Signatures	57.32	394	18.90	19.40	19.60	19.70	19.90	20.20	
Encryption	Encryption/PKI/Digital Certificates	55.32	403	11.30	11.60	11.80	12.00	12.30	12.40	
Encryption	Storage Security, including Cloud	103.82	717	19.00	19.50	19.80	20.00	20.30	20.50	
Identity & Access	Access Management	101.62	820	7.00	7.20	7.40	7.60	7.90	8.20	
Identity & Access	Authentication	131.44	934	21.10	21.70	21.90	22.30	22.60	22.90	
Identity & Access	Identity Management	400.93	2834	18.10	18.60	18.90	19.20	19.40	19.70	
Identity & Access	Intrusion & Anomaly Prevention	61.66	439	20.50	21.10	21.40	21.70	22.00	22.20	
Identity & Access	Messaging Security	150.88	1091	11.40	11.80	12.00	12.30	12.50	12.70	
Infrastructure	Data Management	115.92	853	13.80	14.30	14.40	14.60	14.80	15.00	
Infrastructure	Firewalls	51.13	367	4.60	4.80	4.90	5.10	5.20	5.30	
Infrastructure	Infrastructure Monitoring	60.41	398	20.70	21.30	21.50	21.80	22.00	22.30	
Infrastructure	Infrastructure Resilience	57.72	459	21.00	21.60	22.00	22.30	22.60	22.80	
Infrastructure	Intrusion Detection	4337.49	26650	19.70	20.30	20.80	21.30	21.80	22.30	
Infrastructure	Outsourced/Managed Services	69.20	454	20.50	21.10	21.40	21.60	21.90	22.10	
Infrastructure	Storage Security, including Cloud	193.97	1432	20.90	21.60	21.90	22.20	22.40	22.70	
Mobile	Mobile Security/Device management	101.81	763	5.70	5.80	6.00	6.20	6.30	6.60	
Mobile	PC/Mobile/End Point Security	85.87	611	6.70	6.90	7.10	7.30	7.50	7.70	
Mobile	VPN	61.48	473	19.40	20.00	20.30	20.50	20.70	20.90	
Mobile	Wireless Security	111.48	799	6.40	6.50	6.70	7.00	7.20	7.40	
Outsourced/Managed Services	Access Management	1.02	1	6.70	7.00	7.10	7.40	7.60	7.80	
Outsourced/Managed Services	Anti Spam Solutions	0.58	1	5.10	5.30	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Anti Virus/Worm	1.18	7	5.60	5.70	5.90	6.00	6.20	6.40	
Outsourced/Managed Services	Application Code Security	3.15	20	5.30	5.40	5.60	5.70	5.90	6.10	
Outsourced/Managed Services	Business Continuity/Recovery	0.48	1	5.00	5.10	5.30	5.40	5.60	5.80	
Outsourced/Managed Services	Content Filtering & Monitoring	0.99	4	6.90	7.10	7.30	7.50	7.70	7.90	
Outsourced/Managed Services	Cyber Services	185.31	1376	19.20	19.80	20.10	20.30	20.60	20.90	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	1.26	3	6.00	6.20	6.40	6.50	6.70	6.90	
Outsourced/Managed Services	Firewalls	1.88	12	5.30	5.50	5.60	5.80	5.90	6.10	
Outsourced/Managed Services	Identity Management	2.24	13	5.30	5.50	5.60	5.80	6.00	6.10	
Outsourced/Managed Services	Intrusion Detection	0.80	3	6.20	6.40	6.50	6.70	6.80	6.90	
Outsourced/Managed Services	Malware	0.32	0	5.30	5.50	5.60	5.80	6.00	6.10	
Outsourced/Managed Services	Messaging Security	2.83	14	6.90	7.00	7.20	7.40	7.60	7.90	
Outsourced/Managed Services	Mobile Security/Device management	2.29	13	5.30	5.40	5.50	5.70	5.80	6.00	
Outsourced/Managed Services	Patch Management	0.76	1	6.10	6.20	6.40	6.60	6.80	7.10	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.95	2	5.80	5.90	6.10	6.30	6.50	6.70	
Outsourced/Managed Services	Vulnerability Assessment	1.71	11	5.50	5.70	5.90	6.10	6.30	6.50	
Outsourced/Managed Services	Wireless Security	1.08	3	7.90	8.10	8.40	8.50	8.90	9.10	
Situational Awareness	Darkweb	13.49	92	6.50	6.70	6.70	6.90	6.90	7.00	
Situational Awareness	External Cyber Threat Intelligence	1007.42	6336	16.10	16.60	16.90	17.10	17.50	17.80	
Situational Awareness	High Level Situational Awareness	831.54	4682	10.60	11.00	11.30	11.60	12.00	12.30	
Situational Awareness	Internal Cyber Threat Intelligence	181.92	952	16.50	17.00	17.30	17.70	18.00	18.30	
Situational Awareness	Low Level Situational Awareness	1063.40	7326	19.10	19.70	20.30	20.80	21.50	22.20	
Situational Awareness	Media Monitoring	64.13	505	7.00	7.20	7.30	7.30	7.50	7.60	
Situational Awareness	Proactive Cyber Surveillance	484.98	2825	19.60	20.10	20.40	20.60	20.90	21.10	
System Recovery & Data Cleansing	Data Recovery Services	584.92	3285	16.40	16.90	17.10	17.30	17.50	17.80	
System Recovery & Data Cleansing	Manual Data Cleansing	362.74	2092	18.20	18.70	18.90	19.20	19.50	19.70	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	1286.08	8067	19.80	20.30	20.50	20.80	21.10	21.30	
Training & Education	Access Management	1.62	10	4.10	4.10	4.30	4.40	4.50	4.70	
Training & Education	Anti Spam Solutions	0.50	0	8.30	8.50	8.80	9.00	9.30	9.60	
Training & Education	Anti Virus/Worm	0.09	0	5.60	5.80	5.90	6.10	6.30	6.50	
Training & Education	Application Code Security	0.80	1	5.70	5.80	6.00	6.20	6.30	6.50	
Training & Education	Business Continuity/Recovery	0.25	0	5.30	5.50	5.70	5.80	6.00	6.20	
Training & Education	Computer Forensics	0.16	0	6.60	6.90	7.00	7.20	7.40	7.60	
Training & Education	Content Filtering & Monitoring	0.43	1	5.40	5.60	5.80	5.90	6.10	6.30	
Training & Education	Encryption/PKI/Digital Certificates	0.59	1	7.90	8.10	8.40	8.70	8.90	9.20	
Training & Education	Firewalls	0.34	0	6.00	6.20	6.30	6.50	6.70	6.90	
Training & Education	Identity Management	2.64	13	4.10	4.20	4.30	4.40	4.60	4.70	
Training & Education	Intrusion Detection	0.51	0	4.70	4.80	5.00	5.10	5.20	5.40	
Training & Education	Malware	0.25	0	7.00	7.20	7.40	7.60	7.90	8.10	
Training & Education	Messaging Security	1.44	10	7.70	7.90	8.20	8.40	8.70	8.90	
Training & Education	Mobile Security/Device management	1.52	9	5.80	6.00	6.20	6.40	6.60	6.80	
Training & Education	Patch Management	0.22	0	5.80	6.00	6.20	6.40	6.60	6.80	
Training & Education	PC/Mobile/End Point Security	1.90	10	6.20	6.30	6.60	6.70	6.90	7.10	
Training & Education	Vulnerability Assessment	0.60	1	4.80	4.90	5.10	5.20	5.40	5.50	
Training & Education	Wireless Security	0.99	5	4.40	4.50	4.60	4.80	4.90	5.00	

1.1.59 Latvia

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	0.70	3	5.50	5.60	5.80	6.00	6.20	6.40
Anti Malware	Anti Virus/Worm	2.37	19	5.10	5.30	5.50	5.60	5.80	6.00
Anti Malware	Malware	0.86	3	5.20	5.40	5.50	5.70	5.90	6.10
Anti Malware	Specialist Anti Malware	45.01	132	22.90	23.50	24.20	25.00	25.70	26.60
Application Security	Application Code Security	0.56	4	4.50	4.60	4.70	4.90	5.00	5.20
Application Security	Content Filtering & Monitoring	0.49	2	4.70	4.80	5.00	5.10	5.30	5.40
Application Security	Patch Management	0.61	4	5.40	5.50	5.70	5.80	6.00	6.20
Application Security	Vulnerability Assessment	81.65	374	18.10	18.70	19.30	19.90	20.50	21.10
Business Continuity	Business Continuity/Recovery	2.78	10	17.50	18.00	18.50	19.00	19.60	20.10
Business Continuity	Computer Forensics	1.15	6	10.30	10.60	10.80	11.00	11.20	11.40
Business Continuity	IT/Cyber Forensics	35.99	115	14.30	14.70	15.10	15.60	16.10	16.60
Cyber Consultancy	Access Management	0.10	0	7.40	7.60	7.90	8.10	8.30	8.60
Cyber Consultancy	Anti Spam Solutions	0.07	0	6.50	6.60	6.90	7.10	7.30	7.50
Cyber Consultancy	Anti Virus/Worm	0.06	0	4.50	4.60	4.80	4.90	5.00	5.20
Cyber Consultancy	Application Code Security	0.04	0	4.40	4.50	4.70	4.80	5.00	5.20
Cyber Consultancy	Business Continuity/Recovery	0.04	0	5.50	5.60	5.80	6.00	6.20	6.30
Cyber Consultancy	Computer Forensics	0.07	0	3.50	3.50	3.70	3.80	3.90	4.00
Cyber Consultancy	Content Filtering & Monitoring	0.02	0	5.70	5.80	6.00	6.30	6.50	6.70
Cyber Consultancy	Corporate Services	2.52	20	11.00	11.30	11.40	11.60	11.70	11.80
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.04	0	3.90	4.00	4.10	4.20	4.30	4.50
Cyber Consultancy	Firewalls	0.01	0	4.50	4.70	4.80	5.00	5.20	5.30
Cyber Consultancy	Identity Management	0.09	0	4.70	4.80	5.00	5.10	5.30	5.40
Cyber Consultancy	Intrusion Detection	0.09	0	7.90	8.20	8.40	8.60	8.90	9.10
Cyber Consultancy	Malware	0.10	0	7.20	7.40	7.60	7.90	8.10	8.40
Cyber Consultancy	Messaging Security	0.07	0	5.10	5.20	5.40	5.50	5.60	5.80
Cyber Consultancy	Mobile Security/Device management	0.07	0	5.50	5.70	5.80	6.00	6.10	6.30
Cyber Consultancy	Patch Management	0.02	0	3.10	3.30	3.40	3.40	3.60	3.60
Cyber Consultancy	PC/Mobile/End Point Security	0.02	0	6.80	7.00	7.20	7.40	7.70	7.90
Cyber Consultancy	Vulnerability Assessment	0.07	0	10.00	10.30	10.60	10.90	11.20	11.60
Cyber Consultancy	Wireless Security	0.02	0	5.80	6.00	6.20	6.30	6.50	6.80
Cyber Security Insurance	Business Interruption from Network Downtime	1.35	9	10.50	10.80	11.20	11.50	11.80	12.20
Cyber Security Insurance	Cyber Extortion	1.15	9	11.00	11.40	11.70	12.00	12.40	12.70
Cyber Security Insurance	Investigation of Privacy Breach	0.32	2	10.60	11.00	11.30	11.70	12.10	12.40
Cyber Security Insurance	Loss of Third Party Data	1.64	11	10.70	11.00	11.30	11.60	12.00	12.30
Cyber Security Insurance	Loss or Damage to Digital Assets	1.10	8	10.40	10.70	11.00	11.40	11.70	12.10
Cyber Security Insurance	Multi-Media Liability	1.10	7	10.90	11.20	11.60	11.90	12.20	12.60
Cyber Security Insurance	Reputational Damage	0.50	4	9.80	10.10	10.40	10.70	11.00	11.30
Cyber Security Insurance	Security and Privacy Breaches	1.68	12	11.20	11.60	11.90	12.30	12.70	13.00
Cyber Security Insurance	Theft of Money and Digital Assets	0.89	6	11.40	11.70	12.00	12.30	12.60	13.00
Cyber Security Insurance	Third Party Breach Notification	0.58	4	9.30	9.50	9.80	10.00	10.40	10.70
Encryption	Digital Signatures	0.82	6	13.60	14.00	14.20	14.40	14.60	14.80
Encryption	Encryption/PKI/Digital Certificates	0.87	6	9.50	9.80	10.00	10.20	10.40	10.70
Encryption	Storage Security, including Cloud	1.63	13	13.20	13.60	13.70	14.00	14.10	14.30
Identity & Access	Access Management	0.80	7	4.20	4.30	4.40	4.50	4.70	4.80
Identity & Access	Authentication	1.98	17	13.80	14.20	14.30	14.50	14.70	14.80
Identity & Access	Identity Management	6.02	51	11.50	11.90	12.00	12.20	12.30	12.50
Identity & Access	Intrusion & Anomaly Prevention	0.99	6	13.30	13.70	13.90	14.00	14.20	14.30
Identity & Access	Messaging Security	3.35	18	12.30	12.70	13.00	13.20	13.40	13.60
Infrastructure	Data Management	1.69	15	8.50	8.70	8.80	8.90	9.00	9.10
Infrastructure	Firewalls	1.70	9	7.50	7.70	8.00	8.30	8.50	8.70
Infrastructure	Infrastructure Monitoring	0.88	10	14.00	14.40	14.60	14.80	14.90	15.10
Infrastructure	Infrastructure Resilience	0.89	6	14.30	14.60	14.70	14.90	15.10	15.30
Infrastructure	Intrusion Detection	61.93	180	16.60	17.10	17.50	17.80	18.10	18.40
Infrastructure	Outsourced/Managed Services	0.98	8	13.40	13.70	13.90	14.10	14.30	14.60
Infrastructure	Storage Security, including Cloud	2.93	21	13.80	14.30	14.40	14.60	14.80	14.90
Mobile	Mobile Security/Device management	2.35	15	6.80	7.00	7.20	7.40	7.60	7.80
Mobile	PC/Mobile/End Point Security	1.63	12	8.60	8.80	9.10	9.40	9.70	10.00
Mobile	VPN	0.92	6	11.70	12.10	12.30	12.40	12.50	12.70
Mobile	Wireless Security	0.98	6	3.30	3.50	3.50	3.60	3.80	3.90
Outsourced/Managed Services	Access Management	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Anti Virus/Worm	0.01	0	7.40	7.50	7.80	8.00	8.20	8.40
Outsourced/Managed Services	Application Code Security	0.04	0	5.80	6.00	6.10	6.30	6.60	6.80
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Content Filtering & Monitoring	0.01	0	4.30	4.40	4.60	4.70	4.80	5.00
Outsourced/Managed Services	Cyber Services	2.61	24	12.40	12.80	13.00	13.10	13.30	13.40
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.01	0	3.50	3.60	3.70	3.80	3.90	4.00
Outsourced/Managed Services	Firewalls	0.01	0	8.10	8.40	8.70	8.90	9.20	9.50
Outsourced/Managed Services	Identity Management	0.04	0	7.00	7.20	7.40	7.60	7.80	8.00
Outsourced/Managed Services	Intrusion Detection	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Messaging Security	0.01	0	3.80	3.90	4.00	4.10	4.30	4.40
Outsourced/Managed Services	Mobile Security/Device management	0.01	0	4.30	4.50	4.50	4.70	4.80	4.90
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Vulnerability Assessment	0.01	0	7.80	8.10	8.40	8.70	9.00	9.30
Outsourced/Managed Services	Wireless Security	0.00	0	0	0	0	0	0	0
Situational Awareness	Darkweb	0.23	1	4.20	4.30	4.30	4.40	4.40	4.50
Situational Awareness	External Cyber Threat Intelligence	18.06	46	16.00	16.60	16.80	17.10	17.40	17.70
Situational Awareness	High Level Situational Awareness	14.70	55	12.20	12.60	13.00	13.40	13.70	14.10
Situational Awareness	Internal Cyber Threat Intelligence	3.37	11	18.40	19.00	19.20	19.50	19.90	20.10
Situational Awareness	Low Level Situational Awareness	15.28	41	16.30	16.80	17.30	17.80	18.30	19.00
Situational Awareness	Media Monitoring	1.22	7	4.60	4.70	4.80	4.80	4.90	5.00
Situational Awareness	Proactive Cyber Surveillance	7.38	28	14.30	14.70	14.90	15.10	15.30	15.50
System Recovery & Data Cleansing	Data Recovery Services	12.60	48	17.70	18.30	18.50	18.70	18.90	19.20
System Recovery & Data Cleansing	Manual Data Cleansing	6.07	20	15.70	16.20	16.40	16.60	16.80	17.00
System Recovery & Data Cleansing	System Recovery & Data Cleansing	23.31	72	16.90	17.40	17.60	17.90	18.10	18.30
Training & Education	Access Management	0.01	0	3.80	4.00	4.10	4.20	4.30	4.40
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.00	0	0	0	0	0	0	0
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0
Training & Education	Identity Management	0.02	0	4.90	5.10	5.30	5.40	5.60	5.80
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0
Training & Education	Malware	0.00	0	0	0	0	0	0	0
Training & Education	Messaging Security	0.01	0	7.40	7.60	7.80	8.00	8.20	8.50
Training & Education	Mobile Security/Device management	0.00	0	0	0	0	0	0	0
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0
Training & Education	PC/Mobile/End Point Security	0.02	0	11.20	11.60	12.00	12.30	12.70	13.10
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0
Training & Education	Wireless Security	0.01	0	4.10	4.20	4.40	4.50	4.60	4.80

1.1.60 Lithuania

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	1.21	4	4.40	4.50	4.60	4.80	4.90	5.10
Anti Malware	Anti Virus/Worm	3.05	23	9.50	9.80	10.10	10.40	10.60	10.90
Anti Malware	Malware	0.50	1	5.20	5.30	5.50	5.70	5.90	6.10
Anti Malware	Specialist Anti Malware	4.22	11	19.30	19.70	20.50	21.10	21.80	22.50
Application Security	Application Code Security	0.78	5	3.80	3.90	4.00	4.10	4.20	4.40
Application Security	Content Filtering & Monitoring	0.77	5	4.60	4.80	4.90	5.10	5.20	5.40
Application Security	Patch Management	0.28	1	4.20	4.40	4.50	4.60	4.80	4.90
Application Security	Vulnerability Assessment	26.96	89	17.10	17.60	18.10	18.60	19.20	19.80
Business Continuity	Business Continuity/Recovery	4.76	22	18.70	19.30	19.80	20.40	21.10	21.80
Business Continuity	Computer Forensics	2.02	19	16.80	17.20	17.50	17.70	18.00	18.20
Business Continuity	IT/Cyber Forensics	12.18	60	13.00	13.40	13.80	14.20	14.60	15.00
Cyber Consultancy	Access Management	0.09	1	2.70	2.80	2.90	3.00	3.10	3.20
Cyber Consultancy	Anti Spam Solutions	0.10	0	5.30	5.50	5.70	5.80	6.00	6.20
Cyber Consultancy	Anti Virus/Worm	0.09	0	4.30	4.40	4.50	4.60	4.80	4.90
Cyber Consultancy	Application Code Security	0.10	1	4.50	4.60	4.80	4.90	5.10	5.20
Cyber Consultancy	Business Continuity/Recovery	0.10	0	4.80	4.90	5.00	5.20	5.40	5.50
Cyber Consultancy	Computer Forensics	0.10	1	3.10	3.20	3.30	3.40	3.50	3.60
Cyber Consultancy	Content Filtering & Monitoring	0.07	0	4.10	4.30	4.40	4.50	4.60	4.70
Cyber Consultancy	Corporate Services	4.96	34	16.70	17.30	17.50	17.70	18.00	18.20
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.10	0	3.40	3.50	3.60	3.80	3.90	4.00
Cyber Consultancy	Firewalls	0.05	0	7.00	7.20	7.40	7.60	7.80	8.00
Cyber Consultancy	Identity Management	0.14	1	5.60	5.80	5.90	6.10	6.20	6.40
Cyber Consultancy	Intrusion Detection	0.10	0	6.50	6.70	6.90	7.10	7.30	7.50
Cyber Consultancy	Malware	0.11	0	3.20	3.30	3.40	3.50	3.70	3.80
Cyber Consultancy	Messaging Security	0.12	2	6.00	6.10	6.30	6.50	6.70	7.00
Cyber Consultancy	Mobile Security/Device management	0.11	1	4.10	4.20	4.30	4.40	4.50	4.70
Cyber Consultancy	Patch Management	0.06	0	5.10	5.20	5.40	5.50	5.70	5.90
Cyber Consultancy	PC/Mobile/End Point Security	0.09	0	4.70	4.90	5.00	5.20	5.30	5.50
Cyber Consultancy	Vulnerability Assessment	0.10	0	3.50	3.60	3.70	3.80	4.00	4.10
Cyber Consultancy	Wireless Security	0.06	0	3.70	3.80	3.90	3.90	4.10	4.20
Cyber Security Insurance	Business Interruption from Network Downtime	2.20	15	11.40	11.80	12.20	12.50	12.90	13.30
Cyber Security Insurance	Cyber Extortion	2.12	14	10.90	11.20	11.60	11.90	12.20	12.50
Cyber Security Insurance	Investigation of Privacy Breach	0.48	4	10.40	10.70	11.00	11.30	11.60	11.90
Cyber Security Insurance	Loss of Third Party Data	2.70	18	10.30	10.70	11.00	11.30	11.70	12.00
Cyber Security Insurance	Loss or Damage to Digital Assets	1.79	13	10.10	10.40	10.70	11.00	11.30	11.70
Cyber Security Insurance	Multi-Media Liability	1.79	12	10.50	10.80	11.10	11.40	11.80	12.10
Cyber Security Insurance	Reputational Damage	0.93	7	10.20	10.50	10.80	11.10	11.40	11.80
Cyber Security Insurance	Security and Privacy Breaches	2.64	19	11.00	11.30	11.70	12.00	12.40	12.70
Cyber Security Insurance	Theft of Money and Digital Assets	1.48	11	11.20	11.60	11.90	12.30	12.60	13.00
Cyber Security Insurance	Third Party Breach Notification	0.94	7	9.30	9.50	9.70	10.00	10.30	10.60
Encryption	Digital Signatures	2.03	11	20.20	20.80	21.10	21.40	21.60	21.80
Encryption	Encryption/PKI/Digital Certificates	1.51	13	14.90	15.40	15.60	15.90	16.10	16.30
Encryption	Storage Security, including Cloud	3.22	24	19.70	20.30	20.60	20.80	21.10	21.30
Identity & Access	Access Management	0.73	4	5.30	5.50	5.70	5.80	6.00	6.20
Identity & Access	Authentication	4.39	35	24.80	25.50	25.70	26.10	26.30	26.70
Identity & Access	Identity Management	12.45	118	21.20	21.90	22.20	22.50	22.70	23.00
Identity & Access	Intrusion & Anomaly Prevention	1.91	17	20.80	21.50	21.80	22.00	22.40	22.70
Identity & Access	Messaging Security	2.83	10	15.50	16.00	16.20	16.40	16.60	16.90
Infrastructure	Data Management	3.93	32	16.10	16.60	16.90	17.10	17.30	17.50
Infrastructure	Firewalls	0.81	5	4.40	4.50	4.70	4.80	5.00	5.10
Infrastructure	Infrastructure Monitoring	2.00	10	22.20	22.90	23.00	23.30	23.60	23.90
Infrastructure	Infrastructure Resilience	1.63	15	22.90	23.70	24.10	24.40	24.70	24.90
Infrastructure	Intrusion Detection	25.71	88	14.80	15.20	15.60	15.90	16.30	16.70
Infrastructure	Outsourced/Managed Services	1.87	14	23.00	23.60	23.80	24.10	24.40	24.70
Infrastructure	Storage Security, including Cloud	6.01	45	23.60	24.30	24.60	25.00	25.30	25.60
Mobile	Mobile Security/Device management	1.36	5	8.00	8.30	8.50	8.80	9.00	9.30
Mobile	PC/Mobile/End Point Security	1.47	5	9.30	9.50	9.80	10.10	10.40	10.70
Mobile	VPN	2.08	21	20.80	21.40	21.70	22.00	22.40	22.60
Mobile	Wireless Security	3.05	12	7.90	8.10	8.40	8.60	8.90	9.20
Outsourced/Managed Services	Access Management	0.01	0	4.40	4.50	4.60	4.80	4.90	5.00
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Anti Virus/Worm	0.01	0	6.90	7.10	7.30	7.50	7.70	7.90
Outsourced/Managed Services	Application Code Security	0.07	0	6.60	6.80	7.00	7.30	7.50	7.70
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Content Filtering & Monitoring	0.01	0	5.50	5.60	5.80	5.90	6.00	6.20
Outsourced/Managed Services	Cyber Services	6.08	52	21.30	21.90	22.10	22.40	22.70	23.10
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.01	0	4.30	4.40	4.50	4.60	4.70	4.90
Outsourced/Managed Services	Firewalls	0.07	0	7.30	7.60	7.80	8.00	8.30	8.60
Outsourced/Managed Services	Identity Management	0.09	0	7.00	7.20	7.50	7.70	8.00	8.20
Outsourced/Managed Services	Intrusion Detection	0.01	0	3.60	3.70	3.80	3.80	3.80	3.90
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Messaging Security	0.06	0	6.10	6.20	6.40	6.60	6.80	7.00
Outsourced/Managed Services	Mobile Security/Device management	0.09	0	10.20	10.50	10.80	11.20	11.50	11.80
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	7.20	7.40	7.60	7.90	8.10	8.50
Outsourced/Managed Services	Vulnerability Assessment	0.05	0	9.00	9.20	9.40	9.80	10.10	10.30
Outsourced/Managed Services	Wireless Security	0.01	0	6.10	6.30	6.40	6.70	6.80	7.00
Situational Awareness	Darkweb	0.48	3	7.30	7.50	7.60	7.60	7.80	7.80
Situational Awareness	External Cyber Threat Intelligence	31.93	111	16.50	17.00	17.30	17.60	17.90	18.20
Situational Awareness	High Level Situational Awareness	26.07	109	12.20	12.60	12.90	13.40	13.80	14.20
Situational Awareness	Internal Cyber Threat Intelligence	5.47	14	17.30	17.80	18.10	18.40	18.70	19.00
Situational Awareness	Low Level Situational Awareness	5.35	21	15.90	16.40	16.80	17.30	17.80	18.40
Situational Awareness	Media Monitoring	2.07	13	7.40	7.70	7.80	7.90	8.00	8.10
Situational Awareness	Proactive Cyber Surveillance	12.15	49	14.30	14.80	15.00	15.10	15.30	15.50
System Recovery & Data Cleansing	Data Recovery Services	19.96	50	17.90	18.50	18.70	19.00	19.20	19.40
System Recovery & Data Cleansing	Manual Data Cleansing	9.74	26	15.80	16.30	16.50	16.70	16.90	17.10
System Recovery & Data Cleansing	System Recovery & Data Cleansing	36.70	107	17.00	17.50	17.70	18.00	18.20	18.40
Training & Education	Access Management	0.02	0	8.30	8.50	8.80	9.00	9.30	9.60
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.01	0	3.60	3.70	3.80	3.90	4.00	4.00
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0
Training & Education	Identity Management	0.09	0	6.60	6.80	7.10	7.30	7.50	7.70
Training & Education	Intrusion Detection	0.01	0	6.90	7.20	7.40	7.60	7.80	8.00
Training & Education	Malware	0.00	0	0	0	0	0	0	0
Training & Education	Messaging Security	0.02	0	10.00	10.20	10.50	10.80	11.30	11.60
Training & Education	Mobile Security/Device management	0.02	0	5.80	5.90	6.10	6.30	6.40	6.60
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0
Training & Education	PC/Mobile/End Point Security	0.04	0	3.70	3.80	3.90	4.00	4.20	4.30
Training & Education	Vulnerability Assessment	0.01	0	11.30	11.70	12.10	12.40	12.80	13.10
Training & Education	Wireless Security	0.02	0	6.80	7.10	7.30	7.40	7.60	7.80

1.1.61 Luxembourg

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	2022
Anti Malware	Anti Spam Solutions	0.65	2	5.00	5.20	5.30	5.50	5.70	5.90	
Anti Malware	Anti Virus/Worm	2.68	20	11.20	11.60	11.90	12.20	12.70	13.10	
Anti Malware	Malware	1.07	4	7.50	7.70	8.00	8.20	8.50	8.80	
Anti Malware	Specialist Anti Malware	28.21	308	20.30	20.90	21.50	22.20	22.70	23.50	
Application Security	Application Code Security	0.47	1	5.90	6.10	6.30	6.40	6.60	6.80	
Application Security	Content Filtering & Monitoring	0.47	2	5.00	5.20	5.30	5.50	5.60	5.80	
Application Security	Patch Management	0.31	2	3.60	3.70	3.80	3.90	4.10	4.20	
Application Security	Vulnerability Assessment	69.56	479	18.60	19.20	19.70	20.40	21.00	21.60	
Business Continuity	Business Continuity/Recovery	2.88	27	18.40	18.90	19.40	20.00	20.60	21.20	
Business Continuity	Computer Forensics	1.41	8	20.70	21.30	21.60	22.00	22.30	22.60	
Business Continuity	IT/Cyber Forensics	23.19	156	13.20	13.60	14.00	14.40	14.90	15.30	
Cyber Consultancy	Access Management	0.10	0	7.00	7.20	7.40	7.60	7.90	8.10	
Cyber Consultancy	Anti Spam Solutions	0.06	0	8.70	9.00	9.20	9.50	9.80	10.00	
Cyber Consultancy	Anti Virus/Worm	0.06	0	5.40	5.60	5.80	6.00	6.10	6.30	
Cyber Consultancy	Application Code Security	0.04	0	6.80	7.10	7.30	7.50	7.70	8.00	
Cyber Consultancy	Business Continuity/Recovery	0.05	0	7.60	7.90	8.10	8.30	8.50	8.80	
Cyber Consultancy	Computer Forensics	0.07	0	6.20	6.40	6.50	6.80	7.00	7.20	
Cyber Consultancy	Content Filtering & Monitoring	0.02	0	5.00	5.10	5.30	5.50	5.50	5.70	
Cyber Consultancy	Corporate Services	3.57	24	26.00	26.70	27.00	27.30	27.60	28.00	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.09	0	4.20	4.40	4.50	4.60	4.80	4.90	
Cyber Consultancy	Firewalls	0.01	0	4.10	4.20	4.30	4.40	4.60	4.70	
Cyber Consultancy	Identity Management	0.09	0	5.60	5.80	6.00	6.10	6.30	6.50	
Cyber Consultancy	Intrusion Detection	0.07	0	8.30	8.60	8.90	9.20	9.50	9.70	
Cyber Consultancy	Malware	0.06	0	4.70	4.80	5.00	5.10	5.30	5.50	
Cyber Consultancy	Messaging Security	0.09	1	3.40	3.50	3.60	3.70	3.80	4.00	
Cyber Consultancy	Mobile Security/Device management	0.09	0	6.60	6.80	7.00	7.30	7.50	7.70	
Cyber Consultancy	Patch Management	0.04	0	6.00	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	PC/Mobile/End Point Security	0.06	0	8.70	9.10	9.40	9.60	9.90	10.20	
Cyber Consultancy	Vulnerability Assessment	0.07	0	8.60	8.90	9.20	9.40	9.70	9.90	
Cyber Consultancy	Wireless Security	0.05	0	5.90	6.00	6.30	6.50	6.60	6.80	
Cyber Security Insurance	Business Interruption from Network Downtime	1.29	9	10.60	10.90	11.20	11.50	11.90	12.20	
Cyber Security Insurance	Cyber Extortion	1.18	8	10.80	11.10	11.50	11.80	12.10	12.50	
Cyber Security Insurance	Investigation of Privacy Breach	0.32	2	10.10	10.40	10.70	11.00	11.30	11.60	
Cyber Security Insurance	Loss of Third Party Data	1.66	11	10.50	10.80	11.20	11.50	11.80	12.20	
Cyber Security Insurance	Loss or Damage to Digital Assets	1.08	8	10.30	10.60	10.90	11.20	11.60	11.90	
Cyber Security Insurance	Multi-Media Liability	0.98	7	11.10	11.40	11.70	12.10	12.50	12.80	
Cyber Security Insurance	Reputational Damage	0.60	4	10.60	10.90	11.30	11.50	11.80	12.20	
Cyber Security Insurance	Security and Privacy Breaches	1.66	12	12.10	12.40	12.80	13.20	13.60	14.00	
Cyber Security Insurance	Theft of Money and Digital Assets	0.82	6	11.30	11.60	12.00	12.30	12.70	13.00	
Cyber Security Insurance	Third Party Breach Notification	0.58	4	10.30	10.70	11.00	11.30	11.70	12.00	
Encryption	Digital Signatures	1.54	9	33.00	33.70	34.20	34.50	34.80	35.20	
Encryption	Encryption/PKI/Digital Certificates	1.04	8	20.00	20.50	20.90	21.20	21.60	21.90	
Encryption	Storage Security, including Cloud	2.31	17	29.80	30.70	31.00	31.40	31.80	32.30	
Identity & Access	Access Management	1.21	8	6.50	6.70	6.90	7.10	7.30	7.50	
Identity & Access	Authentication	3.06	19	34.10	35.20	35.60	36.10	36.60	36.90	
Identity & Access	Identity Management	8.75	56	26.10	26.80	27.10	27.50	27.80	28.20	
Identity & Access	Intrusion & Anomaly Prevention	1.46	10	29.40	30.30	30.80	31.20	31.40	31.90	
Identity & Access	Messaging Security	2.52	28	12.00	12.40	12.60	12.80	13.00	13.20	
Infrastructure	Data Management	2.39	20	20.80	21.50	21.70	22.00	22.30	22.60	
Infrastructure	Firewalls	1.38	7	5.20	5.40	5.60	5.70	5.90	6.10	
Infrastructure	Infrastructure Monitoring	1.21	12	33.60	34.70	35.00	35.50	35.70	36.20	
Infrastructure	Infrastructure Resilience	1.31	10	36.00	36.90	37.40	38.00	38.20	38.70	
Infrastructure	Intrusion Detection	47.64	243	15.90	16.40	16.60	16.90	17.20	17.50	
Infrastructure	Outsourced/Managed Services	1.51	11	28.80	29.60	30.10	30.40	30.80	31.20	
Infrastructure	Storage Security, including Cloud	5.02	34	30.90	31.80	32.30	32.80	33.30	33.70	
Mobile	Mobile Security/Device management	1.55	9	5.00	5.20	5.30	5.50	5.70	5.80	
Mobile	PC/Mobile/End Point Security	1.96	8	9.10	9.40	9.60	9.90	10.30	10.60	
Mobile	VPN	1.53	11	32.50	33.40	33.80	34.10	34.60	35.10	
Mobile	Wireless Security	1.15	9	5.10	5.30	5.40	5.60	5.70	5.90	
Outsourced/Managed Services	Access Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Virus/Worm	0.01	0	6.40	6.70	6.90	7.10	7.30	7.50	
Outsourced/Managed Services	Application Code Security	0.01	0	7.30	7.60	7.80	8.10	8.30	8.50	
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Cyber Services	4.65	37	32.00	32.90	33.30	33.70	34.20	34.60	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.01	0	7.10	7.30	7.60	7.70	8.00	8.20	
Outsourced/Managed Services	Firewalls	0.01	0	5.40	5.60	5.70	5.80	6.00	6.20	
Outsourced/Managed Services	Identity Management	0.02	0	4.80	4.80	5.00	5.10	5.30	5.30	
Outsourced/Managed Services	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Messaging Security	0.01	0	4.00	4.10	4.20	4.30	4.50	4.60	
Outsourced/Managed Services	Mobile Security/Device management	0.04	0	7.70	7.90	8.20	8.40	8.70	8.90	
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	12.90	13.20	13.60	14.10	14.60	14.90	
Outsourced/Managed Services	Vulnerability Assessment	0.01	0	9.10	9.30	9.50	9.80	10.00	10.40	
Outsourced/Managed Services	Wireless Security	0.00	0	0	0	0	0	0	0	
Situational Awareness	Darkweb	0.26	2	10.20	10.50	10.70	10.80	10.90	11.10	
Situational Awareness	External Cyber Threat Intelligence	17.43	86	16.40	16.90	17.10	17.40	17.70	18.00	
Situational Awareness	High Level Situational Awareness	15.79	112	12.30	12.70	13.10	13.50	13.90	14.30	
Situational Awareness	Internal Cyber Threat Intelligence	3.52	22	18.70	19.20	19.50	19.90	20.20	20.50	
Situational Awareness	Low Level Situational Awareness	22.11	159	15.70	16.20	16.80	17.30	17.80	18.30	
Situational Awareness	Media Monitoring	1.29	8	10.90	11.20	11.30	11.40	11.50	11.70	
Situational Awareness	Proactive Cyber Surveillance	7.62	37	14.60	15.00	15.20	15.40	15.50	15.70	
System Recovery & Data Cleansing	Data Recovery Services	12.85	86	17.70	18.20	18.40	18.70	18.90	19.10	
System Recovery & Data Cleansing	Manual Data Cleansing	5.90	40	16.00	16.50	16.70	17.00	17.20	17.50	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	23.56	134	17.30	17.80	18.00	18.20	18.40	18.70	
Training & Education	Access Management	0.01	0	5.60	5.70	5.90	6.00	6.20	6.40	
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.00	0	0	0	0	0	0	0	
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0	
Training & Education	Identity Management	0.02	0	7.50	7.70	7.90	8.20	8.40	8.70	
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Training & Education	Malware	0.00	0	0	0	0	0	0	0	
Training & Education	Messaging Security	0.01	0	4.90	5.10	5.20	5.40	5.50	5.70	
Training & Education	Mobile Security/Device management	0.00	0	0	0	0	0	0	0	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.02	0	8.30	8.60	8.90	9.00	9.30	9.50	
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Training & Education	Wireless Security	0.01	0	2.80	2.90	3.00	3.10	3.10	3.20	

1.1.62 Malta

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	2022
Anti Malware	Anti Spam Solutions	0.16	0	5.90	6.10	6.30	6.50	6.70	6.90	
Anti Malware	Anti Virus/Worm	0.69	3	10.10	10.40	10.60	10.90	11.20	11.50	
Anti Malware	Malware	0.22	0	6.50	6.70	6.90	7.10	7.30	7.50	
Anti Malware	Specialist Anti Malware	10.89	33	20.60	21.30	21.90	22.40	23.20	23.90	
Application Security	Application Code Security	0.11	1	4.80	5.00	5.10	5.30	5.40	5.50	
Application Security	Content Filtering & Monitoring	0.14	0	6.30	6.50	6.70	6.90	7.10	7.30	
Application Security	Patch Management	0.11	0	5.70	5.90	6.00	6.20	6.40	6.60	
Application Security	Vulnerability Assessment	15.92	62	17.10	17.60	18.10	18.60	19.20	19.80	
Business Continuity	Business Continuity/Recovery	0.66	2	18.10	18.70	19.30	19.80	20.40	21.00	
Business Continuity	Computer Forensics	0.36	2	23.00	23.60	23.90	24.20	24.60	25.00	
Business Continuity	IT/Cyber Forensics	4.99	15	13.60	14.10	14.50	14.90	15.30	15.80	
Cyber Consultancy	Access Management	0.01	0	4.30	4.50	4.60	4.70	4.90	5.10	
Cyber Consultancy	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Anti Virus/Worm	0.01	0	5.80	6.00	6.10	6.30	6.50	6.70	
Cyber Consultancy	Application Code Security	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Computer Forensics	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Corporate Services	0.82	7	24.00	24.70	25.10	25.40	25.80	26.20	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Firewalls	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Identity Management	0.01	0	3.70	3.70	3.90	4.00	4.10	4.20	
Cyber Consultancy	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Malware	0.01	0	8.30	8.60	8.90	9.20	9.40	9.70	
Cyber Consultancy	Messaging Security	0.01	0	4.80	4.90	5.10	5.20	5.40	5.50	
Cyber Consultancy	Mobile Security/Device management	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Patch Management	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Cyber Consultancy	Wireless Security	0.00	0	0	0	0	0	0	0	
Cyber Security Insurance	Business Interruption from Network Downtime	0.33	2	11.10	11.40	11.70	12.10	12.40	12.80	
Cyber Security Insurance	Cyber Extortion	0.29	2	11.50	11.90	12.30	12.70	13.00	13.50	
Cyber Security Insurance	Investigation of Privacy Breach	0.09	1	12.00	12.30	12.60	13.00	13.40	13.80	
Cyber Security Insurance	Loss of Third Party Data	0.40	3	11.60	11.90	12.30	12.70	13.10	13.50	
Cyber Security Insurance	Loss or Damage to Digital Assets	0.28	2	10.80	11.10	11.40	11.80	12.20	12.60	
Cyber Security Insurance	Multi-Media Liability	0.26	2	9.90	10.20	10.60	10.90	11.20	11.50	
Cyber Security Insurance	Reputational Damage	0.15	1	9.40	9.70	10.00	10.30	10.60	10.90	
Cyber Security Insurance	Security and Privacy Breaches	0.40	3	11.10	11.50	11.80	12.20	12.60	13.00	
Cyber Security Insurance	Theft of Money and Digital Assets	0.21	1	10.40	10.70	11.00	11.20	11.60	12.00	
Cyber Security Insurance	Third Party Breach Notification	0.15	1	11.00	11.30	11.60	12.00	12.20	12.60	
Encryption	Digital Signatures	0.28	2	32.10	33.20	33.80	34.20	34.70	35.00	
Encryption	Encryption/PKI/Digital Certificates	0.22	1	19.10	19.80	20.00	20.20	20.60	20.90	
Encryption	Storage Security, including Cloud	0.61	4	28.40	29.20	29.50	29.90	30.30	30.60	
Identity & Access	Access Management	0.31	3	5.10	5.20	5.30	5.50	5.60	5.80	
Identity & Access	Authentication	0.77	7	32.90	33.90	34.40	34.80	35.30	35.80	
Identity & Access	Identity Management	2.31	15	29.20	30.10	30.50	30.90	31.20	31.60	
Identity & Access	Intrusion & Anomaly Prevention	0.38	2	29.20	30.00	30.40	30.70	31.10	31.50	
Identity & Access	Messaging Security	0.55	1	14.90	15.40	15.60	15.80	16.00	16.20	
Infrastructure	Data Management	0.64	5	20.00	20.50	20.80	21.10	21.40	21.50	
Infrastructure	Firewalls	0.27	0	4.80	4.90	5.00	5.20	5.30	5.50	
Infrastructure	Infrastructure Monitoring	0.34	2	31.40	32.40	32.80	33.20	33.40	33.90	
Infrastructure	Infrastructure Resilience	0.38	2	33.20	34.30	34.90	35.30	35.70	36.10	
Infrastructure	Intrusion Detection	18.53	34	16.30	16.70	17.10	17.40	17.60	18.00	
Infrastructure	Outsourced/Managed Services	0.39	3	24.90	25.70	25.90	26.30	26.50	26.90	
Infrastructure	Storage Security, including Cloud	1.18	8	30.10	31.00	31.40	31.90	32.30	32.70	
Mobile	Mobile Security/Device management	0.44	0	5.70	5.90	6.00	6.20	6.40	6.60	
Mobile	PC/Mobile/End Point Security	0.53	0	9.30	9.60	10.00	10.30	10.60	10.90	
Mobile	VPN	0.34	2	32.00	32.90	33.40	33.70	34.10	34.60	
Mobile	Wireless Security	0.23	0	4.10	4.20	4.30	4.50	4.60	4.70	
Outsourced/Managed Services	Access Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Application Code Security	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Cyber Services	1.14	7	31.30	32.40	32.80	33.20	33.70	34.20	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Firewalls	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Identity Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Messaging Security	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Mobile Security/Device management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Wireless Security	0.00	0	0	0	0	0	0	0	
Situational Awareness	Darkweb	0.07	0	10.30	10.60	10.80	10.90	11.10	11.20	
Situational Awareness	External Cyber Threat Intelligence	4.74	12	16.00	16.50	16.70	17.00	17.30	17.60	
Situational Awareness	High Level Situational Awareness	4.54	17	12.40	12.80	13.20	13.50	14.00	14.40	
Situational Awareness	Internal Cyber Threat Intelligence	0.98	4	17.90	18.50	18.80	19.10	19.40	19.70	
Situational Awareness	Low Level Situational Awareness	6.71	14	16.10	16.60	17.00	17.50	18.10	18.60	
Situational Awareness	Media Monitoring	0.33	3	10.80	11.20	11.40	11.50	11.60	11.80	
Situational Awareness	Proactive Cyber Surveillance	1.92	5	14.50	15.00	15.10	15.40	15.50	15.70	
System Recovery & Data Cleansing	Data Recovery Services	3.46	11	17.90	18.50	18.70	19.00	19.20	19.50	
System Recovery & Data Cleansing	Manual Data Cleansing	1.52	5	16.80	17.30	17.50	17.80	18.00	18.20	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	5.86	14	16.80	17.30	17.50	17.70	18.00	18.20	
Training & Education	Access Management	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.00	0	0	0	0	0	0	0	
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0	
Training & Education	Identity Management	0.00	0	0	0	0	0	0	0	
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Training & Education	Malware	0.00	0	0	0	0	0	0	0	
Training & Education	Messaging Security	0.00	0	0	0	0	0	0	0	
Training & Education	Mobile Security/Device management	0.00	0	0	0	0	0	0	0	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.00	0	0	0	0	0	0	0	
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Training & Education	Wireless Security	0.00	0	0	0	0	0	0	0	

1.1.63 Netherlands

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	12.64	99	6.10	6.30	6.50	6.70	6.90	7.10	
Anti Malware	Anti Virus/Worm	50.54	372	8.50	8.70	9.10	9.40	9.60	9.90	
Anti Malware	Malware	15.04	112	4.70	4.80	5.00	5.20	5.30	5.50	
Anti Malware	Specialist Anti Malware	612.95	3288	20.90	21.50	22.00	22.60	23.30	24.00	
Application Security	Application Code Security	12.29	115	6.70	7.00	7.10	7.30	7.50	7.80	
Application Security	Content Filtering & Monitoring	10.84	85	6.30	6.50	6.70	6.90	7.10	7.20	
Application Security	Patch Management	14.53	107	8.80	9.00	9.30	9.60	9.90	10.20	
Application Security	Vulnerability Assessment	1474.56	8036	18.20	18.80	19.30	19.90	20.50	21.10	
Business Continuity	Business Continuity/Recovery	48.84	281	18.10	18.70	19.20	19.80	20.40	21.00	
Business Continuity	Computer Forensics	23.43	161	19.80	20.30	20.60	20.90	21.20	21.50	
Business Continuity	IT/Cyber Forensics	419.02	2076	13.70	14.10	14.60	15.00	15.40	16.00	
Cyber Consultancy	Access Management	1.64	8	6.50	6.80	6.90	7.10	7.30	7.60	
Cyber Consultancy	Anti Spam Solutions	1.22	8	6.30	6.40	6.60	6.80	7.00	7.20	
Cyber Consultancy	Anti Virus/Worm	1.11	9	5.30	5.50	5.60	5.80	6.00	6.20	
Cyber Consultancy	Application Code Security	0.99	6	4.70	4.80	4.90	5.10	5.30	5.40	
Cyber Consultancy	Business Continuity/Recovery	0.76	5	5.10	5.30	5.50	5.60	5.80	5.90	
Cyber Consultancy	Computer Forensics	1.64	10	6.10	6.30	6.50	6.70	6.80	7.10	
Cyber Consultancy	Content Filtering & Monitoring	1.15	7	7.80	8.10	8.40	8.60	8.80	9.10	
Cyber Consultancy	Corporate Services	55.31	356	20.40	21.00	21.30	21.50	21.80	22.00	
Cyber Consultancy	Encryption/PKI/Digital Certificates	1.40	10	5.80	6.00	6.20	6.40	6.50	6.70	
Cyber Consultancy	Firewalls	0.40	1	5.40	5.60	5.80	6.00	6.20	6.30	
Cyber Consultancy	Identity Management	1.84	16	5.30	5.50	5.70	5.80	6.00	6.20	
Cyber Consultancy	Intrusion Detection	0.64	5	3.60	3.70	3.80	3.90	4.00	4.10	
Cyber Consultancy	Malware	1.76	12	8.60	8.90	9.10	9.40	9.70	10.10	
Cyber Consultancy	Messaging Security	1.35	9	4.10	4.30	4.40	4.50	4.70	4.80	
Cyber Consultancy	Mobile Security/Device management	1.48	10	5.50	5.70	5.90	6.10	6.30	6.50	
Cyber Consultancy	Patch Management	1.02	7	6.70	6.90	7.20	7.40	7.70	7.90	
Cyber Consultancy	PC/Mobile/End Point Security	0.76	5	4.30	4.40	4.60	4.70	4.80	5.00	
Cyber Consultancy	Vulnerability Assessment	1.11	9	4.40	4.60	4.70	4.80	4.90	5.10	
Cyber Consultancy	Wireless Security	0.92	7	6.00	6.20	6.40	6.70	6.90	7.10	
Cyber Security Insurance	Business Interruption from Network Downtime	21.40	140	10.30	10.60	10.90	11.20	11.50	11.90	
Cyber Security Insurance	Cyber Extortion	19.40	139	9.90	10.20	10.50	10.90	11.20	11.60	
Cyber Security Insurance	Investigation of Privacy Breach	4.79	32	10.00	10.30	10.60	11.00	11.30	11.60	
Cyber Security Insurance	Loss of Third Party Data	27.91	193	10.70	11.00	11.30	11.70	12.00	12.40	
Cyber Security Insurance	Loss or Damage to Digital Assets	17.87	117	10.80	11.10	11.40	11.80	12.10	12.50	
Cyber Security Insurance	Multi-Media Liability	17.41	115	10.50	10.80	11.10	11.50	11.80	12.20	
Cyber Security Insurance	Reputational Damage	9.81	76	11.10	11.40	11.70	12.10	12.40	12.90	
Cyber Security Insurance	Security and Privacy Breaches	27.28	188	10.60	10.80	11.10	11.50	11.90	12.20	
Cyber Security Insurance	Theft of Money and Digital Assets	15.09	102	11.20	11.60	11.90	12.30	12.60	13.00	
Cyber Security Insurance	Third Party Breach Notification	9.64	65	9.60	9.90	10.10	10.40	10.70	11.00	
Encryption	Digital Signatures	18.28	132	23.90	24.70	25.10	25.30	25.50	25.90	
Encryption	Encryption/PKI/Digital Certificates	16.78	119	13.30	13.70	14.00	14.10	14.40	14.60	
Encryption	Storage Security, including Cloud	36.65	294	24.90	25.60	25.90	26.30	26.70	27.00	
Identity & Access	Access Management	20.50	177	4.90	5.00	5.20	5.40	5.50	5.70	
Identity & Access	Authentication	46.46	331	27.40	28.20	28.60	28.90	29.20	29.50	
Identity & Access	Identity Management	153.97	1074	22.80	23.40	23.70	24.00	24.30	24.60	
Identity & Access	Intrusion & Anomaly Prevention	20.73	152	26.20	26.90	27.20	27.70	27.90	28.40	
Identity & Access	Messaging Security	48.64	329	11.40	11.70	11.90	12.20	12.40	12.60	
Infrastructure	Data Management	37.96	266	17.40	18.00	18.10	18.40	18.60	18.90	
Infrastructure	Firewalls	25.11	186	6.20	6.40	6.60	6.80	7.00	7.20	
Infrastructure	Infrastructure Monitoring	18.28	119	25.30	25.90	26.30	26.70	27.00	27.40	
Infrastructure	Infrastructure Resilience	19.21	125	27.80	28.80	29.20	29.40	29.80	30.30	
Infrastructure	Intrusion Detection	1074.10	6639	16.50	16.90	17.20	17.50	17.90	18.20	
Infrastructure	Outsourced/Managed Services	23.18	173	24.70	25.40	25.70	26.00	26.40	26.70	
Infrastructure	Storage Security, including Cloud	68.55	516	26.00	26.80	27.10	27.40	27.70	28.00	
Mobile	Mobile Security/Device management	36.16	265	6.10	6.30	6.50	6.60	6.80	7.00	
Mobile	PC/Mobile/End Point Security	27.42	219	8.50	8.80	9.00	9.30	9.60	9.90	
Mobile	VPN	22.72	141	26.40	27.10	27.50	27.70	28.20	28.50	
Mobile	Wireless Security	27.22	212	5.30	5.50	5.60	5.80	6.00	6.10	
Outsourced/Managed Services	Access Management	0.37	1	8.00	8.20	8.50	8.80	9.10	9.40	
Outsourced/Managed Services	Anti Spam Solutions	0.17	0	6.20	6.40	6.60	6.80	7.00	7.20	
Outsourced/Managed Services	Anti Virus/Worm	0.34	1	6.80	7.10	7.30	7.40	7.70	8.00	
Outsourced/Managed Services	Application Code Security	0.73	4	4.20	4.40	4.50	4.60	4.70	4.90	
Outsourced/Managed Services	Business Continuity/Recovery	0.18	0	5.50	5.70	5.80	6.00	6.20	6.30	
Outsourced/Managed Services	Content Filtering & Monitoring	0.23	0	7.20	7.40	7.60	7.90	8.10	8.40	
Outsourced/Managed Services	Cyber Services	68.97	494	25.40	26.20	26.50	26.80	27.20	27.50	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.38	1	4.70	4.80	5.00	5.10	5.30	5.40	
Outsourced/Managed Services	Firewalls	0.59	3	6.40	6.50	6.70	6.90	7.10	7.30	
Outsourced/Managed Services	Identity Management	1.00	5	4.90	5.10	5.20	5.30	5.50	5.60	
Outsourced/Managed Services	Intrusion Detection	0.23	1	5.30	5.50	5.60	5.70	5.80	5.90	
Outsourced/Managed Services	Malware	0.17	0	8.00	8.30	8.50	8.70	9.00	9.30	
Outsourced/Managed Services	Messaging Security	0.56	4	4.50	4.60	4.80	4.90	5.10	5.20	
Outsourced/Managed Services	Mobile Security/Device management	0.59	2	4.70	4.90	5.10	5.20	5.40	5.60	
Outsourced/Managed Services	Patch Management	0.23	1	6.50	6.70	6.90	7.10	7.30	7.60	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.23	1	5.10	5.30	5.40	5.50	5.70	5.80	
Outsourced/Managed Services	Vulnerability Assessment	0.53	4	4.60	4.70	4.90	5.10	5.20	5.40	
Outsourced/Managed Services	Wireless Security	0.27	3	5.80	6.00	6.20	6.40	6.60	6.80	
Situational Awareness	Darkweb	3.77	29	8.50	8.70	8.80	8.90	9.00	9.10	
Situational Awareness	External Cyber Threat Intelligence	303.77	1894	16.40	16.90	17.20	17.40	17.70	18.10	
Situational Awareness	High Level Situational Awareness	247.16	1354	12.70	13.10	13.50	14.00	14.40	14.80	
Situational Awareness	Internal Cyber Threat Intelligence	56.66	302	17.90	18.50	18.90	19.20	19.50	19.90	
Situational Awareness	Low Level Situational Awareness	252.95	1383	16.70	17.30	17.80	18.30	18.90	19.60	
Situational Awareness	Media Monitoring	23.64	178	9.50	9.80	10.00	10.10	10.20	10.30	
Situational Awareness	Proactive Cyber Surveillance	121.37	713	14.10	14.50	14.70	14.90	15.10	15.20	
System Recovery & Data Cleansing	Data Recovery Services	209.63	1370	18.10	18.60	18.90	19.10	19.30	19.60	
System Recovery & Data Cleansing	Manual Data Cleansing	89.22	495	16.10	16.60	16.80	17.00	17.30	17.50	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	412.61	2732	16.70	17.20	17.40	17.70	17.90	18.10	
Training & Education	Access Management	0.48	3	5.90	6.10	6.30	6.50	6.70	6.90	
Training & Education	Anti Spam Solutions	0.11	0	6.20	6.40	6.50	6.70	6.90	7.10	
Training & Education	Anti Virus/Worm	0.02	0	9.10	9.40	9.70	10.00	10.30	10.60	
Training & Education	Application Code Security	0.26	1	5.40	5.60	5.70	5.90	6.10	6.30	
Training & Education	Business Continuity/Recovery	0.10	0	6.20	6.40	6.60	6.80	6.90	7.10	
Training & Education	Computer Forensics	0.04	0	5.40	5.60	5.80	5.90	6.10	6.30	
Training & Education	Content Filtering & Monitoring	0.14	0	4.90	5.10	5.20	5.40	5.60	5.70	
Training & Education	Encryption/PKI/Digital Certificates	0.20	0	8.80	9.10	9.30	9.60	10.00	10.30	
Training & Education	Firewalls	0.10	0	2.70	2.80	2.90	2.90	3.00	3.10	
Training & Education	Identity Management	0.94	4	5.40	5.60	5.80	5.90	6.10	6.30	
Training & Education	Intrusion Detection	0.12	0	4.10	4.20	4.30	4.40	4.50	4.70	
Training & Education	Malware	0.11	0	5.80	5.90	6.10	6.30	6.50	6.70	
Training & Education	Messaging Security	0.33	1	5.30	5.50	5.70	5.80	6.00	6.20	
Training & Education	Mobile Security/Device management	0.55	3	5.00	5.20	5.40	5.60	5.70	5.90	
Training & Education	Patch Management	0.12	0	7.90	8.10	8.40	8.60	8.90	9.20	
Training & Education	PC/Mobile/End Point Security	0.53	4	5.50	5.60	5.80	6.00	6.20	6.30	
Training & Education	Vulnerability Assessment	0.34	2	8.10	8.30	8.60	8.90	9.10	9.40	
Training & Education	Wireless Security	0.36	3	3.40	3.50	3.60	3.70	3.70	3.90	

1.1.64 Poland

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	11.97	88	5.50	5.60	5.80	6.00	6.20	6.30
Anti Malware	Anti Virus/Worm	26.49	193	6.10	6.20	6.40	6.60	6.80	6.90
Anti Malware	Malware	4.97	37	5.30	5.50	5.60	5.80	6.00	6.20
Anti Malware	Specialist Anti Malware	54.50	283	20.00	20.50	21.20	21.80	22.50	23.10
Application Security	Application Code Security	9.52	59	5.00	5.20	5.30	5.50	5.60	5.80
Application Security	Content Filtering & Monitoring	8.37	58	5.00	5.10	5.30	5.50	5.60	5.80
Application Security	Patch Management	3.19	17	4.40	4.60	4.70	4.80	5.00	5.10
Application Security	Vulnerability Assessment	285.43	1658	17.40	18.00	18.50	19.10	19.60	20.20
Business Continuity	Business Continuity/Recovery	49.79	281	18.10	18.70	19.20	19.80	20.30	20.90
Business Continuity	Computer Forensics	18.99	130	8.80	9.00	9.20	9.30	9.50	9.70
Business Continuity	IT/Cyber Forensics	126.16	899	12.70	13.20	13.60	14.00	14.40	14.90
Cyber Consultancy	Access Management	1.51	9	5.50	5.70	5.90	6.10	6.20	6.40
Cyber Consultancy	Anti Spam Solutions	0.77	2	4.20	4.40	4.50	4.60	4.70	4.90
Cyber Consultancy	Anti Virus/Worm	0.91	4	3.70	3.80	3.90	4.00	4.10	4.30
Cyber Consultancy	Application Code Security	0.93	3	6.10	6.30	6.50	6.70	6.80	7.10
Cyber Consultancy	Business Continuity/Recovery	0.87	1	4.50	4.60	4.80	4.90	5.00	5.20
Cyber Consultancy	Computer Forensics	0.98	4	4.20	4.40	4.50	4.70	4.80	4.90
Cyber Consultancy	Content Filtering & Monitoring	0.75	1	4.80	4.90	5.10	5.20	5.40	5.60
Cyber Consultancy	Corporate Services	39.97	279	9.30	9.60	9.70	9.80	9.90	10.10
Cyber Consultancy	Encryption/PKI/Digital Certificates	1.20	7	5.50	5.70	5.90	6.10	6.30	6.40
Cyber Consultancy	Firewalls	0.69	1	6.60	6.80	7.00	7.20	7.40	7.70
Cyber Consultancy	Identity Management	1.42	9	6.20	6.40	6.60	6.80	7.00	7.20
Cyber Consultancy	Intrusion Detection	0.76	3	5.40	5.50	5.70	5.90	6.10	6.30
Cyber Consultancy	Malware	0.94	3	4.80	4.90	5.10	5.20	5.40	5.60
Cyber Consultancy	Messaging Security	1.62	10	5.70	5.80	6.00	6.20	6.40	6.50
Cyber Consultancy	Mobile Security/Device management	1.53	5	6.60	6.80	6.90	7.20	7.40	7.60
Cyber Consultancy	Patch Management	0.78	1	4.60	4.80	4.90	5.00	5.20	5.40
Cyber Consultancy	PC/Mobile/End Point Security	0.91	4	5.50	5.70	5.90	6.00	6.20	6.40
Cyber Consultancy	Vulnerability Assessment	1.13	4	7.10	7.30	7.60	7.70	8.00	8.20
Cyber Consultancy	Wireless Security	0.84	4	5.50	5.70	5.90	6.10	6.30	6.50
Cyber Security Insurance	Business Interruption from Network Downtime	21.46	141	11.40	11.80	12.20	12.60	13.00	13.30
Cyber Security Insurance	Cyber Extortion	18.92	134	10.70	11.10	11.40	11.70	12.10	12.40
Cyber Security Insurance	Investigation of Privacy Breach	4.71	34	11.00	11.30	11.60	12.00	12.30	12.70
Cyber Security Insurance	Loss of Third Party Data	27.25	185	10.80	11.10	11.40	11.80	12.20	12.50
Cyber Security Insurance	Loss or Damage to Digital Assets	16.85	125	10.40	10.70	11.10	11.40	11.70	12.10
Cyber Security Insurance	Multi-Media Liability	17.21	117	9.80	10.00	10.40	10.70	11.00	11.30
Cyber Security Insurance	Reputational Damage	10.26	63	9.20	9.50	9.80	10.10	10.40	10.70
Cyber Security Insurance	Security and Privacy Breaches	26.84	186	11.40	11.70	12.10	12.50	12.90	13.30
Cyber Security Insurance	Theft of Money and Digital Assets	15.53	110	11.70	12.20	12.50	12.90	13.20	13.60
Cyber Security Insurance	Third Party Breach Notification	9.17	67	10.80	11.10	11.50	11.90	12.20	12.50
Encryption	Digital Signatures	14.75	99	10.80	11.10	11.40	11.50	11.60	11.70
Encryption	Encryption/PKI/Digital Certificates	13.53	102	7.90	8.20	8.40	8.50	8.60	8.80
Encryption	Storage Security, including Cloud	24.25	187	11.20	11.50	11.70	11.90	12.00	12.20
Identity & Access	Access Management	6.89	48	4.70	4.80	5.00	5.20	5.30	5.40
Identity & Access	Authentication	30.42	239	12.60	12.90	13.10	13.30	13.40	13.60
Identity & Access	Identity Management	91.46	694	11.20	11.50	11.70	11.80	12.00	12.10
Identity & Access	Intrusion & Anomaly Prevention	15.91	124	12.10	12.40	12.50	12.70	12.90	13.10
Identity & Access	Messaging Security	37.01	234	17.20	17.70	18.00	18.40	18.70	18.90
Infrastructure	Data Management	28.39	200	7.80	8.00	8.10	8.20	8.40	8.50
Infrastructure	Firewalls	7.56	54	6.40	6.60	6.80	6.90	7.20	7.30
Infrastructure	Infrastructure Monitoring	14.06	89	12.00	12.30	12.50	12.70	12.80	13.00
Infrastructure	Infrastructure Resilience	12.27	82	12.50	12.90	13.10	13.30	13.40	13.60
Infrastructure	Intrusion Detection	224.60	1399	15.30	15.70	16.10	16.50	16.80	17.20
Infrastructure	Outsourced/Managed Services	14.48	94	11.30	11.60	11.70	11.90	12.00	12.20
Infrastructure	Storage Security, including Cloud	44.58	319	11.90	12.20	12.40	12.50	12.70	12.80
Mobile	Mobile Security/Device management	12.43	87	4.80	5.00	5.10	5.30	5.40	5.60
Mobile	PC/Mobile/End Point Security	12.58	71	10.00	10.30	10.60	10.90	11.30	11.60
Mobile	VPN	14.99	105	11.50	11.90	12.00	12.20	12.40	12.60
Mobile	Wireless Security	15.28	125	4.40	4.50	4.70	4.80	4.90	5.10
Outsourced/Managed Services	Access Management	0.23	0	5.60	5.80	6.00	6.10	6.30	6.60
Outsourced/Managed Services	Anti Spam Solutions	0.15	0	5.60	5.80	6.00	6.10	6.30	6.50
Outsourced/Managed Services	Anti Virus/Worm	0.31	0	4.70	4.90	5.10	5.20	5.40	5.50
Outsourced/Managed Services	Application Code Security	0.53	0	4.40	4.50	4.60	4.80	4.90	5.00
Outsourced/Managed Services	Business Continuity/Recovery	0.14	0	5.80	6.00	6.10	6.30	6.50	6.70
Outsourced/Managed Services	Content Filtering & Monitoring	0.20	0	5.90	6.10	6.30	6.50	6.60	6.80
Outsourced/Managed Services	Cyber Services	45.51	329	11.40	11.80	11.90	12.10	12.20	12.40
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.32	0	5.20	5.30	5.50	5.70	5.80	6.00
Outsourced/Managed Services	Firewalls	0.51	1	4.40	4.50	4.60	4.80	4.90	5.10
Outsourced/Managed Services	Identity Management	0.94	3	5.50	5.70	5.90	6.10	6.20	6.50
Outsourced/Managed Services	Intrusion Detection	0.25	0	4.90	5.10	5.20	5.30	5.30	5.50
Outsourced/Managed Services	Malware	0.09	0	4.80	4.90	5.10	5.20	5.40	5.60
Outsourced/Managed Services	Messaging Security	0.58	1	7.10	7.30	7.50	7.70	7.90	8.10
Outsourced/Managed Services	Mobile Security/Device management	0.48	1	5.80	6.00	6.20	6.40	6.60	6.80
Outsourced/Managed Services	Patch Management	0.10	0	4.20	4.30	4.50	4.60	4.80	4.90
Outsourced/Managed Services	PC/Mobile/End Point Security	0.25	0	7.20	7.40	7.60	7.90	8.10	8.30
Outsourced/Managed Services	Vulnerability Assessment	0.43	0	7.70	7.90	8.10	8.40	8.60	8.90
Outsourced/Managed Services	Wireless Security	0.29	0	5.10	5.20	5.40	5.50	5.70	5.90
Situational Awareness	Darkweb	3.73	27	3.80	3.90	4.00	4.00	4.00	4.10
Situational Awareness	External Cyber Threat Intelligence	292.04	1612	16.10	16.60	16.80	17.10	17.40	17.70
Situational Awareness	High Level Situational Awareness	265.15	1606	12.60	13.00	13.40	13.80	14.20	14.60
Situational Awareness	Internal Cyber Threat Intelligence	52.23	235	17.90	18.50	18.80	19.10	19.50	19.80
Situational Awareness	Low Level Situational Awareness	69.93	434	15.80	16.30	16.90	17.30	17.80	18.40
Situational Awareness	Media Monitoring	18.23	128	4.10	4.20	4.30	4.30	4.40	4.50
Situational Awareness	Proactive Cyber Surveillance	134.72	750	14.00	14.50	14.70	14.90	15.00	15.20
System Recovery & Data Cleansing	Data Recovery Services	221.33	1327	17.80	18.40	18.60	18.80	19.00	19.30
System Recovery & Data Cleansing	Manual Data Cleansing	89.16	519	15.90	16.50	16.70	16.90	17.10	17.30
System Recovery & Data Cleansing	System Recovery & Data Cleansing	376.47	2438	16.80	17.30	17.50	17.70	17.90	18.10
Training & Education	Access Management	0.42	0	5.30	5.40	5.60	5.70	5.90	6.10
Training & Education	Anti Spam Solutions	0.11	0	5.00	5.10	5.20	5.40	5.60	5.70
Training & Education	Anti Virus/Worm	0.01	0	5.00	5.20	5.30	5.40	5.60	5.70
Training & Education	Application Code Security	0.25	0	5.60	5.80	6.00	6.10	6.30	6.50
Training & Education	Business Continuity/Recovery	0.11	0	4.70	4.80	5.00	5.10	5.30	5.40
Training & Education	Computer Forensics	0.02	0	4.60	4.80	5.00	5.10	5.40	5.50
Training & Education	Content Filtering & Monitoring	0.11	0	6.70	6.90	7.10	7.30	7.50	7.70
Training & Education	Encryption/PKI/Digital Certificates	0.18	0	5.80	6.00	6.20	6.40	6.50	6.70
Training & Education	Firewalls	0.10	0	4.20	4.30	4.40	4.60	4.80	4.90
Training & Education	Identity Management	0.58	1	4.70	4.80	5.00	5.20	5.30	5.40
Training & Education	Intrusion Detection	0.16	0	6.20	6.30	6.50	6.70	6.80	7.10
Training & Education	Malware	0.10	0	4.30	4.40	4.50	4.70	4.80	4.90
Training & Education	Messaging Security	0.29	0	4.30	4.50	4.60	4.70	4.80	4.90
Training & Education	Mobile Security/Device management	0.33	1	5.30	5.40	5.60	5.70	5.90	6.10
Training & Education	Patch Management	0.10	0	6.00	6.20	6.40	6.50	6.80	6.90
Training & Education	PC/Mobile/End Point Security	0.56	0	7.50	7.70	7.90	8.20	8.40	8.70
Training & Education	Vulnerability Assessment	0.21	0	6.00	6.20	6.40	6.60	6.80	7.00
Training & Education	Wireless Security	0.29	0	4.50	4.70	4.80	5.00	5.10	5.30

1.1.65 Portugal

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	6.00	45	5.10	5.30	5.40	5.60	5.80	5.90	
Anti Malware	Anti Virus/Worm	11.45	86	5.00	5.20	5.30	5.50	5.70	5.80	
Anti Malware	Malware	3.21	24	6.50	6.70	6.90	7.10	7.30	7.60	
Anti Malware	Specialist Anti Malware	20.72	107	20.20	20.70	21.40	22.10	22.70	23.40	
Application Security	Application Code Security	4.99	36	5.50	5.70	5.90	6.00	6.10	6.30	
Application Security	Content Filtering & Monitoring	4.17	24	6.00	6.20	6.40	6.50	6.70	6.90	
Application Security	Patch Management	1.55	11	5.30	5.50	5.70	5.80	6.00	6.20	
Application Security	Vulnerability Assessment	98.63	530	16.60	17.10	17.70	18.20	18.70	19.20	
Business Continuity	Business Continuity/Recovery	17.39	95	17.90	18.40	19.00	19.50	20.10	20.70	
Business Continuity	Computer Forensics	7.98	56	7.80	8.00	8.10	8.30	8.40	8.60	
Business Continuity	IT/Cyber Forensics	54.92	328	13.20	13.60	14.00	14.40	14.90	15.30	
Cyber Consultancy	Access Management	0.88	6	9.90	10.20	10.50	10.80	11.10	11.40	
Cyber Consultancy	Anti Spam Solutions	0.36	0	7.50	7.70	8.00	8.20	8.40	8.60	
Cyber Consultancy	Anti Virus/Worm	0.51	3	6.50	6.70	6.90	7.20	7.30	7.50	
Cyber Consultancy	Application Code Security	0.45	0	5.30	5.50	5.60	5.80	5.90	6.10	
Cyber Consultancy	Business Continuity/Recovery	0.28	0	3.70	3.80	3.90	4.00	4.10	4.30	
Cyber Consultancy	Computer Forensics	0.60	4	6.60	6.80	7.10	7.30	7.50	7.70	
Cyber Consultancy	Content Filtering & Monitoring	0.45	0	6.80	7.00	7.20	7.50	7.70	7.90	
Cyber Consultancy	Corporate Services	15.10	111	7.40	7.60	7.70	7.80	7.90	8.00	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.65	1	6.60	6.80	6.90	7.10	7.40	7.60	
Cyber Consultancy	Firewalls	0.18	0	5.50	5.70	5.90	6.00	6.20	6.40	
Cyber Consultancy	Identity Management	0.88	3	6.80	7.00	7.20	7.40	7.70	7.80	
Cyber Consultancy	Intrusion Detection	0.25	0	3.50	3.60	3.70	3.90	4.00	4.10	
Cyber Consultancy	Malware	0.69	1	7.70	7.90	8.10	8.40	8.60	8.90	
Cyber Consultancy	Messaging Security	0.70	5	5.10	5.20	5.40	5.50	5.70	5.80	
Cyber Consultancy	Mobile Security/Device management	0.72	5	4.60	4.70	4.80	4.90	5.10	5.30	
Cyber Consultancy	Patch Management	0.34	0	4.50	4.70	4.80	4.90	5.00	5.20	
Cyber Consultancy	PC/Mobile/End Point Security	0.38	0	4.70	4.80	4.90	5.10	5.20	5.40	
Cyber Consultancy	Vulnerability Assessment	0.44	1	5.10	5.20	5.30	5.50	5.60	5.80	
Cyber Consultancy	Wireless Security	0.32	0	4.50	4.60	4.80	4.90	5.00	5.20	
Cyber Security Insurance	Business Interruption from Network Downtime	8.85	56	11.40	11.80	12.20	12.50	12.90	13.20	
Cyber Security Insurance	Cyber Extortion	7.82	57	11.20	11.50	11.80	12.20	12.60	12.90	
Cyber Security Insurance	Investigation of Privacy Breach	2.06	15	11.90	12.30	12.70	13.10	13.40	13.90	
Cyber Security Insurance	Loss of Third Party Data	10.46	82	10.90	11.20	11.50	11.90	12.30	12.70	
Cyber Security Insurance	Loss or Damage to Digital Assets	6.98	49	11.40	11.70	12.10	12.50	12.80	13.20	
Cyber Security Insurance	Multi-Media Liability	7.05	45	10.20	10.60	10.90	11.30	11.70	12.00	
Cyber Security Insurance	Reputational Damage	3.97	26	10.90	11.20	11.60	11.90	12.20	12.60	
Cyber Security Insurance	Security and Privacy Breaches	9.88	74	10.70	11.00	11.30	11.80	12.10	12.50	
Cyber Security Insurance	Theft of Money and Digital Assets	6.02	42	10.80	11.20	11.50	11.90	12.30	12.60	
Cyber Security Insurance	Third Party Breach Notification	3.46	27	10.60	11.00	11.20	11.60	11.90	12.20	
Encryption	Digital Signatures	4.86	34	8.40	8.60	8.70	8.80	9.00	9.00	
Encryption	Encryption/PKI/Digital Certificates	5.78	39	6.60	6.90	7.00	7.10	7.30	7.40	
Encryption	Storage Security, including Cloud	9.03	64	8.80	9.10	9.20	9.30	9.40	9.50	
Identity & Access	Access Management	4.59	25	6.70	6.90	7.20	7.40	7.70	7.90	
Identity & Access	Authentication	11.10	85	10.00	10.30	10.50	10.60	10.70	10.80	
Identity & Access	Identity Management	35.98	259	8.70	8.90	9.00	9.20	9.20	9.40	
Identity & Access	Intrusion & Anomaly Prevention	5.38	35	9.20	9.40	9.50	9.60	9.70	9.80	
Identity & Access	Messaging Security	14.93	93	15.10	15.40	15.70	16.00	16.20	16.50	
Infrastructure	Data Management	11.91	76	6.30	6.50	6.60	6.70	6.80	6.90	
Infrastructure	Firewalls	3.24	20	5.30	5.50	5.60	5.80	5.90	6.10	
Infrastructure	Infrastructure Monitoring	5.31	36	9.60	9.90	10.00	10.10	10.30	10.40	
Infrastructure	Infrastructure Resilience	5.01	39	9.60	9.90	9.90	10.10	10.20	10.30	
Infrastructure	Intrusion Detection	90.82	553	15.00	15.50	15.80	16.20	16.60	17.00	
Infrastructure	Outsourced/Managed Services	5.45	40	8.50	8.80	8.90	9.00	9.10	9.20	
Infrastructure	Storage Security, including Cloud	17.44	125	9.30	9.60	9.70	9.80	9.90	10.10	
Mobile	Mobile Security/Device management	4.93	34	6.60	6.80	7.00	7.30	7.50	7.70	
Mobile	PC/Mobile/End Point Security	6.30	41	9.30	9.60	9.90	10.20	10.40	10.80	
Mobile	VPN	5.29	34	9.00	9.30	9.50	9.50	9.60	9.70	
Mobile	Wireless Security	11.32	67	5.90	6.10	6.30	6.50	6.70	6.90	
Outsourced/Managed Services	Access Management	0.12	0	7.80	8.10	8.20	8.50	8.70	9.00	
Outsourced/Managed Services	Anti Spam Solutions	0.09	0	4.70	4.80	5.00	5.20	5.30	5.50	
Outsourced/Managed Services	Anti Virus/Worm	0.11	0	4.20	4.40	4.50	4.70	4.80	4.90	
Outsourced/Managed Services	Application Code Security	0.23	0	6.20	6.40	6.60	6.80	7.00	7.20	
Outsourced/Managed Services	Business Continuity/Recovery	0.06	0	6.80	7.10	7.30	7.50	7.80	8.00	
Outsourced/Managed Services	Content Filtering & Monitoring	0.10	0	4.00	4.10	4.20	4.40	4.50	4.60	
Outsourced/Managed Services	Cyber Services	16.66	127	8.90	9.10	9.30	9.30	9.50	9.60	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.17	0	5.80	6.00	6.10	6.30	6.60	6.70	
Outsourced/Managed Services	Firewalls	0.22	0	4.80	5.00	5.10	5.30	5.40	5.60	
Outsourced/Managed Services	Identity Management	0.43	0	4.90	5.10	5.20	5.40	5.50	5.70	
Outsourced/Managed Services	Intrusion Detection	0.15	0	6.50	6.60	6.80	6.90	7.10	7.20	
Outsourced/Managed Services	Malware	0.01	0	5.00	5.20	5.40	5.50	5.70	5.90	
Outsourced/Managed Services	Messaging Security	0.26	0	6.20	6.40	6.60	6.80	6.90	7.10	
Outsourced/Managed Services	Mobile Security/Device management	0.33	0	9.20	9.50	9.80	10.20	10.50	10.80	
Outsourced/Managed Services	Patch Management	0.10	0	7.10	7.30	7.50	7.70	8.00	8.20	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.11	0	6.30	6.40	6.60	6.70	6.90	7.10	
Outsourced/Managed Services	Vulnerability Assessment	0.18	0	5.00	5.20	5.30	5.50	5.60	5.80	
Outsourced/Managed Services	Wireless Security	0.15	0	8.30	8.50	8.80	9.00	9.30	9.60	
Situational Awareness	Darkweb	1.46	10	3.00	3.10	3.10	3.20	3.20	3.20	
Situational Awareness	External Cyber Threat Intelligence	118.67	741	16.10	16.60	16.90	17.10	17.40	17.80	
Situational Awareness	High Level Situational Awareness	91.80	510	12.40	12.80	13.20	13.60	14.00	14.40	
Situational Awareness	Internal Cyber Threat Intelligence	20.60	96	18.20	18.70	19.00	19.30	19.60	20.00	
Situational Awareness	Low Level Situational Awareness	23.50	144	15.60	16.10	16.60	17.10	17.70	18.30	
Situational Awareness	Media Monitoring	7.01	56	3.20	3.30	3.40	3.40	3.40	3.50	
Situational Awareness	Proactive Cyber Surveillance	53.82	315	14.30	14.80	15.00	15.20	15.40	15.60	
System Recovery & Data Cleansing	Data Recovery Services	77.03	458	17.20	17.80	18.00	18.20	18.50	18.80	
System Recovery & Data Cleansing	Manual Data Cleansing	32.91	176	16.10	16.50	16.80	17.00	17.10	17.40	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	151.67	857	16.90	17.40	17.60	17.80	18.00	18.20	
Training & Education	Access Management	0.21	0	6.10	6.30	6.50	6.60	6.90	7.10	
Training & Education	Anti Spam Solutions	0.07	0	7.00	7.20	7.40	7.60	7.80	8.00	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.11	0	5.90	6.10	6.30	6.40	6.60	6.80	
Training & Education	Business Continuity/Recovery	0.01	0	5.30	5.40	5.70	5.80	6.10	6.20	
Training & Education	Computer Forensics	0.01	0	6.90	7.20	7.50	7.70	8.00	8.20	
Training & Education	Content Filtering & Monitoring	0.02	0	4.80	4.90	5.00	5.30	5.40	5.50	
Training & Education	Encryption/PKI/Digital Certificates	0.06	0	5.00	5.20	5.30	5.40	5.60	5.80	
Training & Education	Firewalls	0.01	0	4.50	4.60	4.70	4.90	5.00	5.10	
Training & Education	Identity Management	0.45	0	5.80	6.00	6.20	6.40	6.60	6.80	
Training & Education	Intrusion Detection	0.07	0	5.30	5.50	5.70	5.90	6.10	6.20	
Training & Education	Malware	0.01	0	4.40	4.50	4.60	4.80	4.90	5.00	
Training & Education	Messaging Security	0.14	0	5.70	5.90	6.10	6.30	6.50	6.70	
Training & Education	Mobile Security/Device management	0.14	0	6.20	6.30	6.50	6.60	6.90	7.00	
Training & Education	Patch Management	0.02	0	6.20	6.30	6.60	6.80	7.00	7.20	
Training & Education	PC/Mobile/End Point Security	0.20	0	5.90	6.10	6.30	6.50	6.70	6.80	
Training & Education	Vulnerability Assessment	0.09	0	6.20	6.40	6.60	6.80	6.90	7.20	
Training & Education	Wireless Security	0.16	0	5.30	5.50	5.70	5.90	6.00	6.30	

1.1.66 Romania

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	4.27	30	5.90	6.00	6.20	6.40	6.60	6.80
Anti Malware	Anti Virus/Worm	10.71	65	5.10	5.20	5.40	5.60	5.70	5.90
Anti Malware	Malware	2.64	15	5.00	5.20	5.30	5.50	5.70	5.80
Anti Malware	Specialist Anti Malware	23.14	122	20.70	21.20	21.70	22.30	23.10	23.90
Application Security	Application Code Security	3.71	28	4.70	4.80	4.90	5.10	5.20	5.40
Application Security	Content Filtering & Monitoring	2.55	15	4.40	4.50	4.70	4.80	5.00	5.10
Application Security	Patch Management	1.48	8	4.80	4.90	5.00	5.20	5.30	5.50
Application Security	Vulnerability Assessment	97.38	557	17.10	17.50	18.10	18.60	19.10	19.70
Business Continuity	Business Continuity/Recovery	17.66	80	18.20	18.80	19.40	19.90	20.60	21.20
Business Continuity	Computer Forensics	6.47	47	8.00	8.20	8.40	8.50	8.60	8.80
Business Continuity	IT/Cyber Forensics	49.40	273	13.00	13.40	13.80	14.20	14.70	15.10
Cyber Consultancy	Access Management	0.53	0	5.10	5.20	5.40	5.60	5.70	5.90
Cyber Consultancy	Anti Spam Solutions	0.37	0	5.10	5.20	5.40	5.50	5.70	5.80
Cyber Consultancy	Anti Virus/Worm	0.47	0	6.60	6.80	7.00	7.20	7.40	7.70
Cyber Consultancy	Application Code Security	0.31	0	5.10	5.20	5.40	5.60	5.70	5.90
Cyber Consultancy	Business Continuity/Recovery	0.36	0	4.70	4.80	5.00	5.20	5.30	5.50
Cyber Consultancy	Computer Forensics	0.33	0	4.60	4.80	5.00	5.10	5.30	5.40
Cyber Consultancy	Content Filtering & Monitoring	0.39	0	6.60	6.80	7.00	7.20	7.40	7.60
Cyber Consultancy	Corporate Services	14.89	108	7.50	7.80	7.90	8.00	8.10	8.20
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.51	0	5.80	6.00	6.10	6.30	6.50	6.70
Cyber Consultancy	Firewalls	0.23	0	6.40	6.60	6.80	7.00	7.30	7.40
Cyber Consultancy	Identity Management	0.48	3	3.90	4.00	4.10	4.30	4.40	4.50
Cyber Consultancy	Intrusion Detection	0.34	0	5.90	6.10	6.30	6.50	6.60	6.80
Cyber Consultancy	Malware	0.50	1	5.50	5.70	5.90	6.00	6.20	6.50
Cyber Consultancy	Messaging Security	0.56	0	5.40	5.50	5.70	5.90	6.00	6.20
Cyber Consultancy	Mobile Security/Device management	0.39	0	4.00	4.10	4.20	4.30	4.50	4.60
Cyber Consultancy	Patch Management	0.29	0	5.30	5.50	5.60	5.80	6.00	6.20
Cyber Consultancy	PC/Mobile/End Point Security	0.27	0	6.40	6.60	6.80	7.00	7.20	7.40
Cyber Consultancy	Vulnerability Assessment	0.38	0	4.80	5.00	5.10	5.20	5.40	5.60
Cyber Consultancy	Wireless Security	0.27	0	6.00	6.20	6.40	6.60	6.80	7.00
Cyber Security Insurance	Business Interruption from Network Downtime	8.21	55	10.70	11.00	11.40	11.70	12.00	12.40
Cyber Security Insurance	Cyber Extortion	7.23	51	11.70	12.10	12.50	12.90	13.30	13.80
Cyber Security Insurance	Investigation of Privacy Breach	2.15	14	11.50	11.90	12.30	12.70	13.00	13.50
Cyber Security Insurance	Loss of Third Party Data	10.33	72	11.30	11.60	12.00	12.30	12.70	13.00
Cyber Security Insurance	Loss or Damage to Digital Assets	6.99	46	9.70	10.00	10.30	10.60	10.90	11.20
Cyber Security Insurance	Multi-Media Liability	6.96	46	10.80	11.10	11.50	11.80	12.20	12.60
Cyber Security Insurance	Reputational Damage	3.48	24	10.60	10.90	11.30	11.60	12.00	12.40
Cyber Security Insurance	Security and Privacy Breaches	10.22	68	10.80	11.10	11.40	11.70	12.10	12.50
Cyber Security Insurance	Theft of Money and Digital Assets	5.97	41	11.60	11.90	12.30	12.70	13.10	13.50
Cyber Security Insurance	Third Party Breach Notification	3.52	28	10.30	10.60	10.90	11.20	11.60	12.00
Encryption	Digital Signatures	5.13	38	9.20	9.50	9.60	9.80	9.90	10.00
Encryption	Encryption/PKI/Digital Certificates	4.90	35	7.10	7.30	7.40	7.60	7.80	7.90
Encryption	Storage Security, including Cloud	9.24	62	9.40	9.60	9.70	9.80	10.00	10.10
Identity & Access	Access Management	3.75	24	6.00	6.20	6.40	6.60	6.70	7.00
Identity & Access	Authentication	10.94	79	10.20	10.60	10.70	10.80	10.90	11.00
Identity & Access	Identity Management	33.90	233	9.10	9.40	9.50	9.60	9.70	9.90
Identity & Access	Intrusion & Anomaly Prevention	5.36	37	9.30	9.60	9.60	9.80	9.90	10.00
Identity & Access	Messaging Security	11.17	66	14.50	15.00	15.20	15.40	15.70	15.90
Infrastructure	Data Management	10.61	84	6.50	6.60	6.70	6.80	6.90	7.00
Infrastructure	Firewalls	3.34	20	5.70	5.90	6.10	6.30	6.50	6.60
Infrastructure	Infrastructure Monitoring	4.28	31	9.90	10.20	10.30	10.40	10.50	10.70
Infrastructure	Infrastructure Resilience	4.61	30	10.40	10.70	10.80	11.00	11.10	11.30
Infrastructure	Intrusion Detection	95.73	537	15.40	15.80	16.20	16.60	16.90	17.40
Infrastructure	Outsourced/Managed Services	5.31	42	9.30	9.60	9.70	9.80	9.90	10.00
Infrastructure	Storage Security, including Cloud	15.95	120	9.50	9.70	9.90	10.00	10.10	10.20
Mobile	Mobile Security/Device management	4.60	33	5.90	6.20	6.30	6.50	6.70	6.90
Mobile	PC/Mobile/End Point Security	4.98	29	9.80	10.10	10.40	10.70	11.00	11.40
Mobile	VPN	5.52	35	9.30	9.60	9.70	9.90	10.10	10.20
Mobile	Wireless Security	5.34	35	4.50	4.70	4.80	4.90	5.10	5.20
Outsourced/Managed Services	Access Management	0.09	0	5.20	5.40	5.50	5.70	5.90	6.10
Outsourced/Managed Services	Anti Spam Solutions	0.07	0	4.60	4.80	5.00	5.10	5.30	5.40
Outsourced/Managed Services	Anti Virus/Worm	0.10	0	5.30	5.40	5.50	5.70	5.90	6.10
Outsourced/Managed Services	Application Code Security	0.23	0	4.50	4.70	4.80	5.00	5.10	5.30
Outsourced/Managed Services	Business Continuity/Recovery	0.07	0	6.80	7.00	7.20	7.50	7.70	7.90
Outsourced/Managed Services	Content Filtering & Monitoring	0.09	0	5.70	5.90	6.10	6.20	6.40	6.60
Outsourced/Managed Services	Cyber Services	17.43	116	9.10	9.30	9.50	9.60	9.70	9.80
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.10	0	5.00	5.20	5.40	5.50	5.70	5.80
Outsourced/Managed Services	Firewalls	0.20	0	3.70	3.80	3.90	4.00	4.20	4.30
Outsourced/Managed Services	Identity Management	0.26	0	4.30	4.40	4.50	4.70	4.80	4.90
Outsourced/Managed Services	Intrusion Detection	0.10	0	6.50	6.70	6.80	6.90	7.10	7.20
Outsourced/Managed Services	Malware	0.01	0	4.90	5.00	5.20	5.40	5.60	5.70
Outsourced/Managed Services	Messaging Security	0.27	0	5.90	6.10	6.20	6.40	6.60	6.80
Outsourced/Managed Services	Mobile Security/Device management	0.22	0	6.30	6.50	6.70	6.90	7.10	7.30
Outsourced/Managed Services	Patch Management	0.05	0	5.20	5.30	5.50	5.60	5.70	6.00
Outsourced/Managed Services	PC/Mobile/End Point Security	0.14	0	8.30	8.40	8.70	9.00	9.20	9.50
Outsourced/Managed Services	Vulnerability Assessment	0.16	0	6.50	6.60	6.90	7.10	7.30	7.50
Outsourced/Managed Services	Wireless Security	0.10	0	4.30	4.50	4.60	4.70	4.90	5.00
Situational Awareness	Darkweb	1.41	10	3.00	3.10	3.10	3.20	3.20	3.20
Situational Awareness	External Cyber Threat Intelligence	105.65	541	16.30	16.80	17.10	17.30	17.70	18.00
Situational Awareness	High Level Situational Awareness	97.14	573	12.30	12.70	13.10	13.50	13.80	14.30
Situational Awareness	Internal Cyber Threat Intelligence	24.58	114	18.00	18.60	18.80	19.10	19.40	19.70
Situational Awareness	Low Level Situational Awareness	23.96	123	15.90	16.40	16.90	17.40	17.90	18.30
Situational Awareness	Media Monitoring	6.56	50	3.30	3.40	3.50	3.50	3.60	3.60
Situational Awareness	Proactive Cyber Surveillance	44.57	256	14.70	15.10	15.30	15.50	15.70	15.90
System Recovery & Data Cleansing	Data Recovery Services	84.62	474	17.80	18.30	18.50	18.70	19.00	19.20
System Recovery & Data Cleansing	Manual Data Cleansing	37.12	189	16.20	16.70	16.80	17.10	17.30	17.50
System Recovery & Data Cleansing	System Recovery & Data Cleansing	142.12	850	16.50	17.00	17.20	17.40	17.70	17.90
Training & Education	Access Management	0.12	0	4.60	4.70	4.80	5.00	5.10	5.30
Training & Education	Anti Spam Solutions	0.04	0	4.80	4.90	5.00	5.20	5.30	5.50
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.11	0	5.80	5.90	6.10	6.30	6.50	6.60
Training & Education	Business Continuity/Recovery	0.02	0	5.00	5.20	5.30	5.50	5.60	5.80
Training & Education	Computer Forensics	0.01	0	4.90	5.10	5.20	5.40	5.60	5.70
Training & Education	Content Filtering & Monitoring	0.02	0	7.50	7.80	8.00	8.30	8.50	8.70
Training & Education	Encryption/PKI/Digital Certificates	0.07	0	4.30	4.50	4.60	4.70	4.90	5.00
Training & Education	Firewalls	0.02	0	5.60	5.70	5.90	6.10	6.30	6.50
Training & Education	Identity Management	0.25	0	5.10	5.20	5.40	5.50	5.70	5.90
Training & Education	Intrusion Detection	0.07	0	4.90	5.00	5.20	5.40	5.50	5.70
Training & Education	Malware	0.02	0	5.90	6.10	6.30	6.40	6.70	6.80
Training & Education	Messaging Security	0.11	0	4.00	4.10	4.30	4.40	4.50	4.60
Training & Education	Mobile Security/Device management	0.11	0	6.00	6.10	6.30	6.50	6.70	6.90
Training & Education	Patch Management	0.02	0	5.50	5.60	5.80	6.00	6.20	6.50
Training & Education	PC/Mobile/End Point Security	0.14	0	5.30	5.50	5.60	5.80	6.00	6.20
Training & Education	Vulnerability Assessment	0.09	0	5.70	6.00	6.10	6.30	6.50	6.70
Training & Education	Wireless Security	0.12	0	4.70	4.80	5.00	5.10	5.30	5.40

1.1.67 Slovakia

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %					
				2016	2017	2018	2019	2020	2021
Anti Malware	Anti Spam Solutions	1.62	11	4.20	4.30	4.40	4.60	4.70	4.90
Anti Malware	Anti Virus/Worm	9.42	49	5.90	6.10	6.30	6.50	6.60	6.90
Anti Malware	Malware	2.00	16	4.70	4.80	5.00	5.10	5.30	5.50
Anti Malware	Specialist Anti Malware	123.41	324	22.10	22.80	23.40	24.20	24.80	25.70
Application Security	Application Code Security	1.69	11	6.60	6.80	7.00	7.20	7.40	7.60
Application Security	Content Filtering & Monitoring	1.16	7	4.30	4.40	4.60	4.70	4.80	5.00
Application Security	Patch Management	1.43	5	6.00	6.20	6.40	6.60	6.80	7.00
Application Security	Vulnerability Assessment	228.49	996	17.80	18.40	18.90	19.50	20.00	20.60
Business Continuity	Business Continuity/Recovery	8.79	28	18.20	18.70	19.20	19.80	20.40	21.00
Business Continuity	Computer Forensics	3.29	29	9.60	9.80	10.00	10.10	10.30	10.50
Business Continuity	IT/Cyber Forensics	90.06	291	14.00	14.40	14.90	15.40	15.80	16.30
Cyber Consultancy	Access Management	0.21	1	4.80	5.00	5.10	5.30	5.40	5.60
Cyber Consultancy	Anti Spam Solutions	0.16	1	6.40	6.50	6.70	6.90	7.10	7.30
Cyber Consultancy	Anti Virus/Worm	0.20	1	4.00	4.10	4.20	4.30	4.50	4.60
Cyber Consultancy	Application Code Security	0.18	1	5.70	5.80	6.00	6.20	6.40	6.60
Cyber Consultancy	Business Continuity/Recovery	0.11	1	2.60	2.70	2.80	2.90	3.00	3.00
Cyber Consultancy	Computer Forensics	0.25	1	7.10	7.30	7.50	7.80	8.00	8.20
Cyber Consultancy	Content Filtering & Monitoring	0.11	0	5.00	5.20	5.30	5.50	5.60	5.80
Cyber Consultancy	Corporate Services	8.14	56	9.40	9.70	9.80	9.90	10.10	10.20
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.12	1	2.60	2.70	2.70	2.80	2.90	3.00
Cyber Consultancy	Firewalls	0.10	0	5.80	6.00	6.20	6.40	6.60	6.80
Cyber Consultancy	Identity Management	0.29	1	3.40	3.50	3.60	3.70	3.80	4.00
Cyber Consultancy	Intrusion Detection	0.14	1	3.90	4.00	4.10	4.20	4.40	4.40
Cyber Consultancy	Malware	0.25	1	4.60	4.80	4.90	5.10	5.20	5.40
Cyber Consultancy	Messaging Security	0.23	1	4.40	4.50	4.70	4.80	5.00	5.10
Cyber Consultancy	Mobile Security/Device management	0.22	1	7.30	7.50	7.80	8.00	8.20	8.40
Cyber Consultancy	Patch Management	0.11	0	3.70	3.80	3.90	4.00	4.20	4.30
Cyber Consultancy	PC/Mobile/End Point Security	0.14	0	4.30	4.40	4.50	4.70	4.80	5.00
Cyber Consultancy	Vulnerability Assessment	0.12	1	6.10	6.30	6.60	6.70	7.00	7.20
Cyber Consultancy	Wireless Security	0.12	1	6.50	6.70	6.90	7.10	7.30	7.50
Cyber Security Insurance	Business Interruption from Network Downtime	3.90	26	11.20	11.60	11.90	12.30	12.60	13.00
Cyber Security Insurance	Cyber Extortion	3.39	23	10.30	10.60	11.00	11.30	11.60	11.90
Cyber Security Insurance	Investigation of Privacy Breach	0.89	6	11.00	11.30	11.70	12.00	12.30	12.70
Cyber Security Insurance	Loss of Third Party Data	4.83	32	10.20	10.50	10.90	11.20	11.60	11.90
Cyber Security Insurance	Loss or Damage to Digital Assets	3.12	21	10.10	10.40	10.70	11.00	11.40	11.70
Cyber Security Insurance	Multi-Media Liability	3.00	21	10.40	10.70	11.00	11.40	11.70	12.10
Cyber Security Insurance	Reputational Damage	1.63	11	10.90	11.20	11.60	12.00	12.30	12.70
Cyber Security Insurance	Security and Privacy Breaches	4.38	32	11.10	11.40	11.80	12.20	12.50	12.90
Cyber Security Insurance	Theft of Money and Digital Assets	2.46	16	10.20	10.60	10.90	11.20	11.50	11.80
Cyber Security Insurance	Third Party Breach Notification	1.70	12	10.20	10.40	10.70	11.00	11.30	11.60
Encryption	Digital Signatures	2.82	19	10.60	10.90	11.10	11.20	11.40	11.60
Encryption	Encryption/PKI/Digital Certificates	2.47	11	7.70	7.90	8.10	8.30	8.40	8.70
Encryption	Storage Security, including Cloud	4.37	25	11.60	11.90	12.10	12.20	12.40	12.50
Identity & Access	Access Management	3.70	15	5.50	5.70	5.80	6.00	6.20	6.40
Identity & Access	Authentication	5.03	36	12.30	12.70	12.90	13.00	13.20	13.30
Identity & Access	Identity Management	16.63	115	10.30	10.60	10.70	10.80	11.00	11.10
Identity & Access	Intrusion & Anomaly Prevention	2.61	17	11.60	12.00	12.10	12.40	12.50	12.70
Identity & Access	Messaging Security	7.91	43	14.40	14.90	15.10	15.30	15.50	15.70
Infrastructure	Data Management	5.16	38	7.90	8.20	8.30	8.40	8.50	8.60
Infrastructure	Firewalls	2.35	13	5.90	6.10	6.20	6.50	6.70	6.90
Infrastructure	Infrastructure Monitoring	2.94	15	11.30	11.70	11.90	12.00	12.10	12.20
Infrastructure	Infrastructure Resilience	2.35	18	11.90	12.30	12.50	12.60	12.80	13.00
Infrastructure	Intrusion Detection	165.02	417	16.00	16.50	16.80	17.10	17.50	17.80
Infrastructure	Outsourced/Managed Services	2.77	17	10.80	11.20	11.40	11.60	11.70	11.90
Infrastructure	Storage Security, including Cloud	8.11	53	11.70	12.10	12.20	12.40	12.50	12.70
Mobile	Mobile Security/Device management	3.50	20	5.40	5.60	5.70	5.90	6.10	6.30
Mobile	PC/Mobile/End Point Security	4.94	19	8.30	8.50	8.80	9.00	9.30	9.60
Mobile	VPN	2.83	26	12.10	12.50	12.70	12.80	13.00	13.00
Mobile	Wireless Security	2.59	14	3.70	3.80	4.00	4.10	4.20	4.30
Outsourced/Managed Services	Access Management	0.04	0	5.40	5.50	5.70	5.90	6.00	6.20
Outsourced/Managed Services	Anti Spam Solutions	0.01	0	3.00	3.10	3.20	3.30	3.40	3.50
Outsourced/Managed Services	Anti Virus/Worm	0.06	0	3.90	4.00	4.10	4.20	4.30	4.40
Outsourced/Managed Services	Application Code Security	0.10	0	4.60	4.70	4.90	5.00	5.10	5.30
Outsourced/Managed Services	Business Continuity/Recovery	0.01	0	5.70	5.90	6.00	6.30	6.50	6.70
Outsourced/Managed Services	Content Filtering & Monitoring	0.04	0	4.70	4.90	5.00	5.20	5.30	5.50
Outsourced/Managed Services	Cyber Services	8.27	54	11.50	11.90	12.00	12.20	12.30	12.50
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.06	0	5.40	5.50	5.70	5.90	6.00	6.20
Outsourced/Managed Services	Firewalls	0.10	1	5.70	5.90	6.10	6.20	6.40	6.60
Outsourced/Managed Services	Identity Management	0.17	1	6.40	6.60	6.80	7.00	7.20	7.40
Outsourced/Managed Services	Intrusion Detection	0.04	0	3.40	3.50	3.50	3.60	3.60	3.70
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0
Outsourced/Managed Services	Messaging Security	0.10	0	4.60	4.70	4.80	5.00	5.20	5.30
Outsourced/Managed Services	Mobile Security/Device management	0.11	0	6.30	6.50	6.70	6.80	7.00	7.30
Outsourced/Managed Services	Patch Management	0.01	0	6.30	6.50	6.70	6.90	7.20	7.30
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	7.70	8.00	8.20	8.40	8.70	8.90
Outsourced/Managed Services	Vulnerability Assessment	0.07	0	6.40	6.50	6.70	6.90	7.10	7.30
Outsourced/Managed Services	Wireless Security	0.02	0	3.00	3.00	3.10	3.30	3.40	3.40
Situational Awareness	Darkweb	0.67	5	3.60	3.80	3.80	3.90	3.90	3.90
Situational Awareness	External Cyber Threat Intelligence	49.79	153	16.00	16.50	16.80	17.10	17.40	17.60
Situational Awareness	High Level Situational Awareness	47.47	183	12.30	12.70	13.10	13.50	13.90	14.30
Situational Awareness	Internal Cyber Threat Intelligence	10.40	35	17.10	17.60	17.90	18.20	18.50	18.80
Situational Awareness	Low Level Situational Awareness	78.77	360	17.50	18.00	18.50	19.10	19.70	20.20
Situational Awareness	Media Monitoring	3.13	31	3.90	4.00	4.10	4.20	4.20	4.30
Situational Awareness	Proactive Cyber Surveillance	21.72	68	14.20	14.60	14.80	15.00	15.20	15.40
System Recovery & Data Cleansing	Data Recovery Services	38.90	150	18.30	18.80	19.00	19.20	19.50	19.70
System Recovery & Data Cleansing	Manual Data Cleansing	17.00	58	16.20	16.70	16.90	17.10	17.30	17.50
System Recovery & Data Cleansing	System Recovery & Data Cleansing	71.39	264	16.90	17.40	17.60	17.80	18.00	18.30
Training & Education	Access Management	0.07	0	3.90	4.00	4.10	4.30	4.30	4.50
Training & Education	Anti Spam Solutions	0.01	0	5.30	5.40	5.60	5.80	6.00	6.20
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0
Training & Education	Application Code Security	0.04	0	5.70	5.90	6.00	6.20	6.40	6.60
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0
Training & Education	Encryption/PKI/Digital Certificates	0.01	0	4.40	4.60	4.70	4.80	4.90	5.10
Training & Education	Firewalls	0.01	0	8.00	8.30	8.50	8.70	8.90	9.20
Training & Education	Identity Management	0.11	1	3.60	3.70	3.80	3.90	4.00	4.10
Training & Education	Intrusion Detection	0.01	0	5.50	5.70	5.90	6.00	6.20	6.30
Training & Education	Malware	0.00	0	0	0	0	0	0	0
Training & Education	Messaging Security	0.06	0	3.70	3.90	4.00	4.10	4.20	4.30
Training & Education	Mobile Security/Device management	0.04	0	6.00	6.20	6.40	6.50	6.70	6.90
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0
Training & Education	PC/Mobile/End Point Security	0.07	0	5.00	5.10	5.30	5.50	5.60	5.80
Training & Education	Vulnerability Assessment	0.01	0	3.20	3.30	3.40	3.50	3.60	3.70
Training & Education	Wireless Security	0.02	0	2.30	2.40	2.40	2.40	2.60	2.60

1.1.68 Slovenia

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	2021
Anti Malware	Anti Spam Solutions	0.97	4	4.60	4.70	4.90	5.00	5.20	5.30	
Anti Malware	Anti Virus/Worm	3.65	20	6.00	6.20	6.40	6.60	6.80	7.00	
Anti Malware	Malware	0.69	4	3.40	3.50	3.60	3.70	3.80	3.90	
Anti Malware	Specialist Anti Malware	38.07	176	20.00	20.70	21.30	21.90	22.60	23.40	
Application Security	Application Code Security	0.88	8	6.60	6.70	6.90	7.10	7.30	7.60	
Application Security	Content Filtering & Monitoring	0.81	6	7.10	7.30	7.60	7.80	8.00	8.20	
Application Security	Patch Management	0.66	3	4.60	4.70	4.90	5.00	5.20	5.40	
Application Security	Vulnerability Assessment	95.53	346	17.50	18.00	18.60	19.10	19.70	20.20	
Business Continuity	Business Continuity/Recovery	4.26	14	18.70	19.30	19.90	20.60	21.10	21.70	
Business Continuity	Computer Forensics	1.59	11	9.30	9.60	9.70	9.90	10.00	10.20	
Business Continuity	IT/Cyber Forensics	27.17	108	13.40	13.80	14.20	14.70	15.20	15.60	
Cyber Consultancy	Access Management	0.12	1	7.10	7.30	7.50	7.80	8.00	8.30	
Cyber Consultancy	Anti Spam Solutions	0.09	0	4.70	4.80	5.00	5.10	5.30	5.50	
Cyber Consultancy	Anti Virus/Worm	0.10	0	4.40	4.50	4.70	4.80	5.00	5.10	
Cyber Consultancy	Application Code Security	0.09	0	5.50	5.70	5.80	6.00	6.20	6.30	
Cyber Consultancy	Business Continuity/Recovery	0.09	0	6.10	6.30	6.40	6.60	6.80	7.00	
Cyber Consultancy	Computer Forensics	0.07	0	4.50	4.70	4.80	4.90	5.10	5.20	
Cyber Consultancy	Content Filtering & Monitoring	0.06	0	5.30	5.50	5.70	5.80	6.00	6.20	
Cyber Consultancy	Corporate Services	3.70	22	10.50	10.90	11.00	11.10	11.30	11.50	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.11	0	4.50	4.60	4.70	4.80	5.00	5.10	
Cyber Consultancy	Firewalls	0.04	0	4.50	4.60	4.80	4.90	5.10	5.20	
Cyber Consultancy	Identity Management	0.16	1	4.90	5.00	5.20	5.30	5.40	5.60	
Cyber Consultancy	Intrusion Detection	0.10	0	6.20	6.40	6.50	6.80	7.00	7.20	
Cyber Consultancy	Malware	0.10	0	3.40	3.50	3.60	3.70	3.80	3.90	
Cyber Consultancy	Messaging Security	0.12	1	6.50	6.60	6.80	7.10	7.30	7.50	
Cyber Consultancy	Mobile Security/Device management	0.12	1	5.60	5.80	6.00	6.20	6.40	6.60	
Cyber Consultancy	Patch Management	0.04	0	5.20	5.40	5.60	5.70	5.90	6.10	
Cyber Consultancy	PC/Mobile/End Point Security	0.09	0	7.90	8.10	8.30	8.60	8.80	9.00	
Cyber Consultancy	Vulnerability Assessment	0.09	0	5.50	5.60	5.80	6.00	6.20	6.40	
Cyber Consultancy	Wireless Security	0.07	0	4.10	4.30	4.40	4.50	4.70	4.80	
Cyber Security Insurance	Business Interruption from Network Downtime	1.80	13	11.20	11.60	11.90	12.30	12.60	13.00	
Cyber Security Insurance	Cyber Extortion	1.69	12	11.00	11.40	11.70	12.10	12.50	12.80	
Cyber Security Insurance	Investigation of Privacy Breach	0.45	3	11.50	11.80	12.10	12.50	12.80	13.20	
Cyber Security Insurance	Loss of Third Party Data	2.40	16	10.30	10.60	10.90	11.20	11.60	11.90	
Cyber Security Insurance	Loss or Damage to Digital Assets	1.51	11	9.40	9.70	10.00	10.30	10.70	10.90	
Cyber Security Insurance	Multi-Media Liability	1.42	10	10.00	10.30	10.60	10.90	11.20	11.50	
Cyber Security Insurance	Reputational Damage	0.87	6	10.80	11.10	11.40	11.70	12.00	12.40	
Cyber Security Insurance	Security and Privacy Breaches	2.28	16	11.00	11.40	11.70	12.00	12.40	12.80	
Cyber Security Insurance	Theft of Money and Digital Assets	1.26	8	11.50	11.80	12.10	12.50	12.90	13.30	
Cyber Security Insurance	Third Party Breach Notification	0.88	6	10.90	11.20	11.60	12.00	12.30	12.60	
Encryption	Digital Signatures	1.43	10	12.00	12.40	12.60	12.80	12.90	13.10	
Encryption	Encryption/PKI/Digital Certificates	1.07	9	7.70	7.90	8.10	8.20	8.40	8.50	
Encryption	Storage Security, including Cloud	2.00	15	11.30	11.70	11.80	12.00	12.20	12.30	
Identity & Access	Access Management	2.00	9	6.20	6.30	6.50	6.70	6.90	7.10	
Identity & Access	Authentication	2.96	19	14.30	14.70	14.80	14.90	15.20	15.40	
Identity & Access	Identity Management	8.33	53	11.50	11.90	12.10	12.20	12.40	12.60	
Identity & Access	Intrusion & Anomaly Prevention	1.26	9	12.60	12.90	13.10	13.30	13.50	13.70	
Identity & Access	Messaging Security	4.10	13	12.50	13.00	13.20	13.40	13.60	13.80	
Infrastructure	Data Management	2.40	20	8.30	8.60	8.70	8.80	8.90	9.00	
Infrastructure	Firewalls	1.32	10	5.80	5.90	6.10	6.30	6.50	6.70	
Infrastructure	Infrastructure Monitoring	1.15	12	12.60	12.90	13.10	13.20	13.40	13.60	
Infrastructure	Infrastructure Resilience	1.02	6	11.60	11.90	12.00	12.20	12.30	12.40	
Infrastructure	Intrusion Detection	80.40	227	16.50	17.00	17.40	17.70	18.00	18.30	
Infrastructure	Outsourced/Managed Services	1.31	11	11.90	12.30	12.40	12.60	12.80	13.00	
Infrastructure	Storage Security, including Cloud	4.12	33	12.70	13.10	13.30	13.40	13.60	13.80	
Mobile	Mobile Security/Device management	2.30	15	7.10	7.30	7.60	7.80	8.10	8.30	
Mobile	PC/Mobile/End Point Security	3.59	19	9.30	9.70	9.90	10.30	10.50	10.90	
Mobile	VPN	1.41	12	10.90	11.20	11.40	11.50	11.70	11.80	
Mobile	Wireless Security	2.73	18	8.50	8.70	9.00	9.20	9.50	9.80	
Outsourced/Managed Services	Access Management	0.01	0	3.60	3.70	3.80	3.90	4.00	4.20	
Outsourced/Managed Services	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Anti Virus/Worm	0.01	0	6.10	6.30	6.40	6.60	6.80	7.10	
Outsourced/Managed Services	Application Code Security	0.06	0	7.20	7.40	7.60	7.80	8.00	8.30	
Outsourced/Managed Services	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Content Filtering & Monitoring	0.01	0	5.90	6.00	6.20	6.40	6.60	6.80	
Outsourced/Managed Services	Cyber Services	4.06	35	11.80	12.20	12.20	12.40	12.60	12.70	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.01	0	5.30	5.50	5.70	5.90	6.00	6.30	
Outsourced/Managed Services	Firewalls	0.06	0	7.50	7.70	8.00	8.30	8.50	8.70	
Outsourced/Managed Services	Identity Management	0.07	0	2.30	2.40	2.40	2.60	2.60	2.70	
Outsourced/Managed Services	Intrusion Detection	0.01	0	3.60	3.70	3.80	3.80	3.90	3.90	
Outsourced/Managed Services	Malware	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	Messaging Security	0.07	0	5.50	5.70	5.90	6.00	6.20	6.40	
Outsourced/Managed Services	Mobile Security/Device management	0.04	0	5.90	6.00	6.20	6.30	6.50	6.70	
Outsourced/Managed Services	Patch Management	0.00	0	0	0	0	0	0	0	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.01	0	4.60	4.80	4.90	5.00	5.20	5.40	
Outsourced/Managed Services	Vulnerability Assessment	0.04	0	7.30	7.50	7.70	7.90	8.20	8.40	
Outsourced/Managed Services	Wireless Security	0.01	0	2.70	2.80	2.90	2.90	3.00	3.20	
Situational Awareness	Darkweb	0.34	2	4.20	4.30	4.40	4.40	4.40	4.60	
Situational Awareness	External Cyber Threat Intelligence	26.73	91	16.60	17.10	17.40	17.70	18.00	18.30	
Situational Awareness	High Level Situational Awareness	22.72	67	12.60	12.90	13.30	13.70	14.10	14.60	
Situational Awareness	Internal Cyber Threat Intelligence	4.49	12	18.00	18.50	18.80	19.20	19.50	19.90	
Situational Awareness	Low Level Situational Awareness	25.21	119	16.20	16.60	17.10	17.60	18.10	18.60	
Situational Awareness	Media Monitoring	1.73	10	4.40	4.50	4.60	4.70	4.70	4.80	
Situational Awareness	Proactive Cyber Surveillance	10.33	45	14.30	14.80	14.90	15.10	15.30	15.50	
System Recovery & Data Cleansing	Data Recovery Services	17.52	59	17.90	18.40	18.60	18.90	19.10	19.40	
System Recovery & Data Cleansing	Manual Data Cleansing	8.59	25	15.70	16.20	16.40	16.60	16.80	17.10	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	34.83	131	16.70	17.30	17.50	17.70	18.00	18.20	
Training & Education	Access Management	0.02	0	5.40	5.60	5.80	6.00	6.20	6.30	
Training & Education	Anti Spam Solutions	0.00	0	0	0	0	0	0	0	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.01	0	4.90	5.00	5.20	5.30	5.40	5.50	
Training & Education	Business Continuity/Recovery	0.00	0	0	0	0	0	0	0	
Training & Education	Computer Forensics	0.00	0	0	0	0	0	0	0	
Training & Education	Content Filtering & Monitoring	0.00	0	0	0	0	0	0	0	
Training & Education	Encryption/PKI/Digital Certificates	0.00	0	0	0	0	0	0	0	
Training & Education	Firewalls	0.00	0	0	0	0	0	0	0	
Training & Education	Identity Management	0.05	0	6.60	6.80	7.00	7.30	7.50	7.70	
Training & Education	Intrusion Detection	0.00	0	0	0	0	0	0	0	
Training & Education	Malware	0.00	0	0	0	0	0	0	0	
Training & Education	Messaging Security	0.02	0	6.40	6.50	6.80	7.00	7.20	7.30	
Training & Education	Mobile Security/Device management	0.02	0	7.70	7.80	8.10	8.40	8.60	8.90	
Training & Education	Patch Management	0.00	0	0	0	0	0	0	0	
Training & Education	PC/Mobile/End Point Security	0.02	0	6.00	6.20	6.30	6.50	6.80	7.00	
Training & Education	Vulnerability Assessment	0.00	0	0	0	0	0	0	0	
Training & Education	Wireless Security	0.01	0	6.30	6.50	6.60	6.80	7.00	7.20	

1.1.69 Spain

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	
Anti Malware	Anti Spam Solutions	24.88	199	4.80	4.90	5.10	5.20	5.40	5.50	
Anti Malware	Anti Virus/Worm	107.23	794	8.00	8.30	8.60	8.80	9.00	9.30	
Anti Malware	Malware	24.76	157	5.30	5.50	5.70	5.80	6.00	6.10	
Anti Malware	Specialist Anti Malware	702.29	4628	19.30	19.70	20.40	20.90	21.50	22.20	
Application Security	Application Code Security	20.06	166	5.10	5.20	5.30	5.50	5.60	5.80	
Application Security	Content Filtering & Monitoring	20.55	163	7.00	7.20	7.40	7.60	7.80	8.10	
Application Security	Patch Management	16.67	115	4.80	4.90	5.10	5.30	5.40	5.60	
Application Security	Vulnerability Assessment	2413.64	14868	18.10	18.60	19.20	19.80	20.40	21.00	
Business Continuity	Business Continuity/Recovery	101.24	579	18.20	18.80	19.40	19.90	20.60	21.20	
Business Continuity	Computer Forensics	53.53	352	16.90	17.50	17.70	18.00	18.30	18.60	
Business Continuity	IT/Cyber Forensics	919.08	4404	13.60	14.10	14.50	14.90	15.40	15.80	
Cyber Consultancy	Access Management	2.26	15	7.10	7.30	7.40	7.70	7.90	8.10	
Cyber Consultancy	Anti Spam Solutions	1.92	9	6.60	6.80	7.10	7.20	7.50	7.70	
Cyber Consultancy	Anti Virus/Worm	2.59	17	5.70	5.80	6.00	6.20	6.40	6.60	
Cyber Consultancy	Application Code Security	1.70	9	4.90	5.00	5.20	5.30	5.50	5.70	
Cyber Consultancy	Business Continuity/Recovery	1.86	11	5.60	5.70	5.80	6.00	6.20	6.40	
Cyber Consultancy	Computer Forensics	2.11	14	5.10	5.20	5.40	5.50	5.70	5.90	
Cyber Consultancy	Content Filtering & Monitoring	1.75	8	7.70	7.90	8.10	8.40	8.70	8.90	
Cyber Consultancy	Corporate Services	107.29	741	18.60	19.10	19.40	19.60	19.80	20.10	
Cyber Consultancy	Encryption/PKI/Digital Certificates	2.39	12	4.50	4.70	4.80	5.00	5.10	5.30	
Cyber Consultancy	Firewalls	1.09	4	4.60	4.70	4.90	5.00	5.10	5.30	
Cyber Consultancy	Identity Management	3.81	24	6.00	6.10	6.30	6.50	6.70	6.90	
Cyber Consultancy	Intrusion Detection	1.77	9	5.10	5.30	5.40	5.60	5.80	6.00	
Cyber Consultancy	Malware	2.14	10	4.40	4.50	4.60	4.80	5.00	5.10	
Cyber Consultancy	Messaging Security	2.95	16	5.20	5.30	5.50	5.60	5.80	6.00	
Cyber Consultancy	Mobile Security/Device management	3.44	21	5.60	5.80	6.00	6.10	6.30	6.50	
Cyber Consultancy	Patch Management	1.90	11	5.70	5.90	6.10	6.30	6.40	6.60	
Cyber Consultancy	PC/Mobile/End Point Security	1.98	11	5.00	5.20	5.40	5.50	5.70	5.80	
Cyber Consultancy	Vulnerability Assessment	2.40	15	4.60	4.80	4.90	5.10	5.30	5.40	
Cyber Consultancy	Wireless Security	1.97	8	5.50	5.70	5.90	6.10	6.30	6.50	
Cyber Security Insurance	Business Interruption from Network Downtime	41.99	268	10.50	10.80	11.10	11.50	11.80	12.20	
Cyber Security Insurance	Cyber Extortion	41.50	284	10.90	11.20	11.50	11.90	12.30	12.60	
Cyber Security Insurance	Investigation of Privacy Breach	11.65	81	11.40	11.70	12.10	12.40	12.80	13.20	
Cyber Security Insurance	Loss of Third Party Data	54.94	371	10.70	11.10	11.40	11.70	12.10	12.40	
Cyber Security Insurance	Loss or Damage to Digital Assets	37.83	273	11.20	11.50	11.80	12.20	12.50	13.00	
Cyber Security Insurance	Multi-Media Liability	34.39	254	11.60	11.90	12.30	12.60	13.00	13.40	
Cyber Security Insurance	Reputational Damage	19.25	133	10.60	10.80	11.20	11.50	11.80	12.10	
Cyber Security Insurance	Security and Privacy Breaches	56.52	397	11.10	11.40	11.80	12.10	12.50	12.90	
Cyber Security Insurance	Theft of Money and Digital Assets	30.26	208	10.90	11.30	11.60	11.90	12.30	12.60	
Cyber Security Insurance	Third Party Breach Notification	20.74	128	10.80	11.10	11.40	11.70	12.00	12.50	
Encryption	Digital Signatures	41.46	288	21.30	22.10	22.30	22.60	23.00	23.10	
Encryption	Encryption/PKI/Digital Certificates	31.13	230	14.20	14.60	14.80	15.10	15.30	15.60	
Encryption	Storage Security, including Cloud	68.77	511	22.00	22.60	22.90	23.20	23.50	23.80	
Identity & Access	Access Management	61.45	452	7.70	8.00	8.20	8.50	8.70	9.00	
Identity & Access	Authentication	89.58	587	24.80	25.50	25.80	26.10	26.40	26.60	
Identity & Access	Identity Management	263.65	2115	21.00	21.60	21.90	22.20	22.50	22.80	
Identity & Access	Intrusion & Anomaly Prevention	43.64	316	24.40	25.30	25.70	25.90	26.20	26.60	
Identity & Access	Messaging Security	108.13	730	12.90	13.30	13.50	13.80	14.00	14.30	
Infrastructure	Data Management	73.13	526	15.80	16.30	16.50	16.70	16.90	17.10	
Infrastructure	Firewalls	38.11	256	5.40	5.60	5.80	5.90	6.10	6.30	
Infrastructure	Infrastructure Monitoring	32.33	331	23.50	24.10	24.50	24.90	25.20	25.50	
Infrastructure	Infrastructure Resilience	38.05	288	24.60	25.40	25.80	26.10	26.50	26.80	
Infrastructure	Intrusion Detection	1947.27	11737	16.20	16.70	17.00	17.30	17.70	18.00	
Infrastructure	Outsourced/Managed Services	44.51	342	22.40	23.00	23.40	23.70	23.80	24.20	
Infrastructure	Storage Security, including Cloud	127.74	865	24.20	24.90	25.20	25.50	25.90	26.10	
Mobile	Mobile Security/Device management	61.16	433	4.60	4.70	4.80	5.00	5.10	5.30	
Mobile	PC/Mobile/End Point Security	59.50	445	8.90	9.20	9.40	9.70	10.00	10.30	
Mobile	VPN	39.60	304	23.30	23.90	24.20	24.50	24.70	25.10	
Mobile	Wireless Security	53.24	416	5.00	5.20	5.30	5.40	5.60	5.80	
Outsourced/Managed Services	Access Management	0.67	1	5.80	6.00	6.20	6.30	6.50	6.70	
Outsourced/Managed Services	Anti Spam Solutions	0.47	2	5.90	6.10	6.30	6.50	6.70	6.90	
Outsourced/Managed Services	Anti Virus/Worm	0.78	3	5.60	5.80	6.00	6.10	6.30	6.50	
Outsourced/Managed Services	Application Code Security	1.69	7	5.40	5.50	5.80	5.90	6.10	6.30	
Outsourced/Managed Services	Business Continuity/Recovery	0.32	0	4.50	4.70	4.80	5.00	5.10	5.30	
Outsourced/Managed Services	Content Filtering & Monitoring	0.66	3	6.70	6.90	7.10	7.30	7.50	7.80	
Outsourced/Managed Services	Cyber Services	126.45	963	22.40	23.10	23.30	23.60	23.90	24.30	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	1.10	4	7.10	7.40	7.60	7.90	8.10	8.40	
Outsourced/Managed Services	Firewalls	1.18	6	4.70	4.80	4.90	5.10	5.20	5.40	
Outsourced/Managed Services	Identity Management	1.70	12	4.80	5.00	5.10	5.30	5.40	5.60	
Outsourced/Managed Services	Intrusion Detection	0.49	1	4.10	4.20	4.30	4.40	4.50	4.60	
Outsourced/Managed Services	Malware	0.25	0	5.30	5.50	5.60	5.80	5.90	6.10	
Outsourced/Managed Services	Messaging Security	1.29	6	4.40	4.50	4.60	4.80	4.90	5.10	
Outsourced/Managed Services	Mobile Security/Device management	1.22	6	6.60	6.80	7.00	7.30	7.50	7.70	
Outsourced/Managed Services	Patch Management	0.47	3	5.70	5.80	6.00	6.10	6.30	6.50	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.56	1	4.70	4.80	5.00	5.10	5.30	5.40	
Outsourced/Managed Services	Vulnerability Assessment	1.11	7	6.50	6.70	7.00	7.10	7.30	7.50	
Outsourced/Managed Services	Wireless Security	0.72	1	7.00	7.20	7.50	7.70	7.90	8.10	
Situational Awareness	Darkweb	8.36	67	7.70	8.00	8.10	8.20	8.30	8.40	
Situational Awareness	External Cyber Threat Intelligence	616.49	3547	16.00	16.50	16.70	17.00	17.30	17.60	
Situational Awareness	High Level Situational Awareness	510.22	2941	12.30	12.70	13.00	13.40	13.80	14.30	
Situational Awareness	Internal Cyber Threat Intelligence	119.05	641	17.90	18.40	18.60	19.00	19.30	19.60	
Situational Awareness	Low Level Situational Awareness	736.47	3920	17.20	17.70	18.20	18.70	19.30	19.90	
Situational Awareness	Media Monitoring	44.38	314	8.30	8.50	8.70	8.80	8.90	9.00	
Situational Awareness	Proactive Cyber Surveillance	243.47	1491	14.30	14.80	15.00	15.20	15.40	15.60	
System Recovery & Data Cleansing	Data Recovery Services	432.14	2537	17.50	18.00	18.20	18.40	18.70	18.90	
System Recovery & Data Cleansing	Manual Data Cleansing	173.40	1100	15.90	16.40	16.60	16.70	17.00	17.10	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	786.26	4793	17.20	17.70	17.90	18.10	18.40	18.60	
Training & Education	Access Management	0.95	4	7.50	7.70	7.90	8.20	8.40	8.60	
Training & Education	Anti Spam Solutions	0.23	0	5.30	5.50	5.60	5.80	6.00	6.20	
Training & Education	Anti Virus/Worm	0.07	0	6.40	6.60	6.80	7.00	7.30	7.50	
Training & Education	Application Code Security	0.59	1	4.10	4.30	4.40	4.50	4.60	4.80	
Training & Education	Business Continuity/Recovery	0.18	0	4.50	4.60	4.80	4.90	5.00	5.20	
Training & Education	Computer Forensics	0.11	0	4.40	4.50	4.70	4.80	4.90	5.10	
Training & Education	Content Filtering & Monitoring	0.36	0	9.00	9.30	9.50	9.80	10.10	10.40	
Training & Education	Encryption/PKI/Digital Certificates	0.43	0	5.20	5.30	5.50	5.60	5.80	6.10	
Training & Education	Firewalls	0.22	0	4.30	4.40	4.60	4.70	4.90	5.10	
Training & Education	Identity Management	1.48	10	4.00	4.10	4.20	4.40	4.50	4.60	
Training & Education	Intrusion Detection	0.32	0	4.50	4.70	4.80	5.00	5.10	5.30	
Training & Education	Malware	0.15	0	6.20	6.30	6.50	6.80	7.00	7.20	
Training & Education	Messaging Security	0.76	4	6.20	6.40	6.50	6.70	7.00	7.20	
Training & Education	Mobile Security/Device management	0.69	1	5.50	5.70	5.80	6.00	6.20	6.40	
Training & Education	Patch Management	0.20	0	4.80	4.90	5.10	5.20	5.30	5.50	
Training & Education	PC/Mobile/End Point Security	0.88	5	4.50	4.60	4.80	4.90	5.00	5.20	
Training & Education	Vulnerability Assessment	0.47	1	6.40	6.60	6.80	7.00	7.20	7.50	
Training & Education	Wireless Security	0.87	5	4.60	4.70	4.90	5.00	5.10	5.30	

1.1.70 Sweden

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	2022
Anti Malware	Anti Spam Solutions	7.23	60	4.80	4.90	5.10	5.20	5.40	5.50	
Anti Malware	Anti Virus/Worm	30.27	211	8.30	8.60	8.90	9.10	9.40	9.70	
Anti Malware	Malware	9.55	43	6.60	6.80	7.00	7.20	7.40	7.60	
Anti Malware	Specialist Anti Malware	161.43	845	19.60	20.20	20.70	21.20	21.80	22.60	
Application Security	Application Code Security	5.92	32	5.40	5.60	5.70	5.90	6.10	6.20	
Application Security	Content Filtering & Monitoring	6.03	34	6.50	6.70	6.90	7.10	7.30	7.50	
Application Security	Patch Management	5.45	21	6.10	6.30	6.50	6.70	6.90	7.10	
Application Security	Vulnerability Assessment	775.03	4472	17.90	18.50	19.00	19.60	20.20	20.80	
Business Continuity	Business Continuity/Recovery	25.20	110	18.50	19.10	19.60	20.10	20.70	21.30	
Business Continuity	Computer Forensics	12.47	73	19.90	20.50	20.80	21.10	21.40	21.70	
Business Continuity	IT/Cyber Forensics	203.53	1088	13.90	14.20	14.60	15.10	15.60	16.00	
Cyber Consultancy	Access Management	0.66	1	6.10	6.40	6.50	6.70	7.00	7.20	
Cyber Consultancy	Anti Spam Solutions	0.45	0	5.60	5.70	5.90	6.10	6.30	6.50	
Cyber Consultancy	Anti Virus/Worm	0.61	3	5.60	5.80	6.00	6.20	6.40	6.60	
Cyber Consultancy	Application Code Security	0.61	3	4.10	4.30	4.40	4.50	4.60	4.80	
Cyber Consultancy	Business Continuity/Recovery	0.54	1	4.10	4.20	4.30	4.50	4.60	4.80	
Cyber Consultancy	Computer Forensics	0.53	1	4.30	4.50	4.60	4.70	4.80	5.00	
Cyber Consultancy	Content Filtering & Monitoring	0.42	0	6.40	6.60	6.80	7.00	7.20	7.40	
Cyber Consultancy	Corporate Services	28.70	216	20.30	20.80	21.10	21.40	21.60	21.90	
Cyber Consultancy	Encryption/PKI/Digital Certificates	0.67	1	5.10	5.20	5.40	5.50	5.70	5.90	
Cyber Consultancy	Firewalls	0.26	0	4.10	4.20	4.30	4.40	4.60	4.70	
Cyber Consultancy	Identity Management	0.91	2	4.70	4.90	5.00	5.20	5.30	5.40	
Cyber Consultancy	Intrusion Detection	0.44	0	4.40	4.60	4.70	4.80	5.00	5.20	
Cyber Consultancy	Malware	0.72	1	7.80	8.00	8.30	8.50	8.70	9.00	
Cyber Consultancy	Messaging Security	0.95	2	5.80	5.90	6.10	6.30	6.50	6.70	
Cyber Consultancy	Mobile Security/Device management	0.71	1	5.10	5.30	5.50	5.60	5.70	5.90	
Cyber Consultancy	Patch Management	0.42	1	6.00	6.20	6.30	6.50	6.70	6.90	
Cyber Consultancy	PC/Mobile/End Point Security	0.45	0	6.90	7.20	7.30	7.60	7.80	8.10	
Cyber Consultancy	Vulnerability Assessment	0.65	1	7.10	7.30	7.60	7.80	8.10	8.30	
Cyber Consultancy	Wireless Security	0.54	3	7.40	7.60	7.80	8.10	8.30	8.60	
Cyber Security Insurance	Business Interruption from Network Downtime	12.05	80	11.20	11.60	11.90	12.20	12.60	13.00	
Cyber Security Insurance	Cyber Extortion	10.11	75	11.20	11.60	11.90	12.30	12.70	13.10	
Cyber Security Insurance	Investigation of Privacy Breach	3.02	19	10.40	10.60	11.00	11.30	11.70	12.10	
Cyber Security Insurance	Loss of Third Party Data	15.53	103	10.80	11.20	11.50	11.90	12.20	12.60	
Cyber Security Insurance	Loss or Damage to Digital Assets	10.12	68	10.50	10.80	11.10	11.40	11.80	12.10	
Cyber Security Insurance	Multi-Media Liability	9.79	65	10.40	10.70	11.10	11.40	11.80	12.10	
Cyber Security Insurance	Reputational Damage	4.82	35	10.00	10.30	10.70	10.90	11.30	11.70	
Cyber Security Insurance	Security and Privacy Breaches	14.42	99	11.60	11.90	12.30	12.70	13.10	13.50	
Cyber Security Insurance	Theft of Money and Digital Assets	7.77	57	11.00	11.40	11.70	12.00	12.40	12.80	
Cyber Security Insurance	Third Party Breach Notification	5.18	37	10.00	10.30	10.50	10.80	11.20	11.60	
Encryption	Digital Signatures	11.66	73	24.80	25.60	25.90	26.20	26.50	26.90	
Encryption	Encryption/PKI/Digital Certificates	9.58	53	14.20	14.70	14.90	15.10	15.40	15.60	
Encryption	Storage Security, including Cloud	18.64	140	23.70	24.30	24.60	24.90	25.30	25.50	
Identity & Access	Access Management	16.35	111	7.30	7.60	7.80	8.00	8.30	8.50	
Identity & Access	Authentication	26.55	180	27.00	27.70	28.10	28.50	28.90	29.20	
Identity & Access	Identity Management	76.70	519	21.70	22.40	22.70	23.10	23.30	23.70	
Identity & Access	Intrusion & Anomaly Prevention	11.03	89	25.50	26.10	26.40	26.70	26.90	27.20	
Identity & Access	Messaging Security	26.97	152	11.50	11.80	12.00	12.20	12.50	12.70	
Infrastructure	Data Management	20.99	139	17.60	18.10	18.30	18.60	18.80	19.00	
Infrastructure	Firewalls	12.75	66	5.50	5.70	5.90	6.10	6.20	6.40	
Infrastructure	Infrastructure Monitoring	10.26	72	25.00	25.60	26.00	26.20	26.70	27.20	
Infrastructure	Infrastructure Resilience	11.15	77	26.60	27.30	27.50	28.00	28.20	28.70	
Infrastructure	Intrusion Detection	516.57	2460	15.60	16.10	16.40	16.80	17.10	17.50	
Infrastructure	Outsourced/Managed Services	11.87	84	23.80	24.60	24.90	25.30	25.50	26.00	
Infrastructure	Storage Security, including Cloud	33.20	277	25.90	26.70	27.00	27.30	27.70	28.00	
Mobile	Mobile Security/Device management	17.72	125	4.80	5.00	5.10	5.30	5.40	5.60	
Mobile	PC/Mobile/End Point Security	14.13	83	8.20	8.40	8.70	8.90	9.20	9.50	
Mobile	VPN	11.53	79	24.70	25.30	25.60	26.00	26.30	26.60	
Mobile	Wireless Security	14.43	80	5.90	6.10	6.30	6.50	6.70	6.90	
Outsourced/Managed Services	Access Management	0.23	0	7.90	8.10	8.40	8.60	8.90	9.10	
Outsourced/Managed Services	Anti Spam Solutions	0.12	0	7.30	7.50	7.70	8.00	8.20	8.40	
Outsourced/Managed Services	Anti Virus/Worm	0.17	0	4.50	4.60	4.80	4.90	5.10	5.20	
Outsourced/Managed Services	Application Code Security	0.43	1	6.50	6.70	6.90	7.10	7.30	7.60	
Outsourced/Managed Services	Business Continuity/Recovery	0.09	0	6.50	6.70	6.90	7.00	7.30	7.50	
Outsourced/Managed Services	Content Filtering & Monitoring	0.14	0	4.90	5.10	5.20	5.40	5.60	5.70	
Outsourced/Managed Services	Cyber Services	34.48	282	23.80	24.60	25.00	25.30	25.60	25.90	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	0.16	0	4.30	4.50	4.60	4.70	4.90	5.00	
Outsourced/Managed Services	Firewalls	0.31	1	3.60	3.70	3.80	4.00	4.10	4.20	
Outsourced/Managed Services	Identity Management	0.48	3	4.70	4.80	4.90	5.10	5.30	5.50	
Outsourced/Managed Services	Intrusion Detection	0.17	0	4.20	4.30	4.40	4.50	4.60	4.70	
Outsourced/Managed Services	Malware	0.07	0	6.40	6.50	6.70	6.90	7.10	7.30	
Outsourced/Managed Services	Messaging Security	0.43	1	6.70	6.90	7.10	7.30	7.40	7.70	
Outsourced/Managed Services	Mobile Security/Device management	0.33	1	5.10	5.30	5.50	5.60	5.70	5.90	
Outsourced/Managed Services	Patch Management	0.09	0	4.40	4.50	4.70	4.70	4.90	5.10	
Outsourced/Managed Services	PC/Mobile/End Point Security	0.17	0	5.30	5.50	5.60	5.80	5.90	6.10	
Outsourced/Managed Services	Vulnerability Assessment	0.21	0	4.90	5.10	5.20	5.30	5.40	5.60	
Outsourced/Managed Services	Wireless Security	0.15	0	5.40	5.60	5.80	5.90	6.20	6.30	
Situational Awareness	Darkweb	2.24	17	8.10	8.40	8.50	8.70	8.80	8.90	
Situational Awareness	External Cyber Threat Intelligence	153.92	787	16.30	16.80	17.10	17.40	17.70	18.00	
Situational Awareness	High Level Situational Awareness	142.92	801	12.60	13.00	13.40	13.80	14.20	14.60	
Situational Awareness	Internal Cyber Threat Intelligence	24.30	107	18.00	18.60	18.90	19.20	19.50	19.80	
Situational Awareness	Low Level Situational Awareness	194.70	1012	16.50	17.00	17.40	17.90	18.40	18.90	
Situational Awareness	Media Monitoring	12.15	88	9.00	9.30	9.50	9.60	9.70	9.80	
Situational Awareness	Proactive Cyber Surveillance	71.48	394	14.00	14.40	14.60	14.70	14.90	15.10	
System Recovery & Data Cleansing	Data Recovery Services	122.66	645	18.10	18.60	18.90	19.10	19.30	19.60	
System Recovery & Data Cleansing	Manual Data Cleansing	51.41	314	16.00	16.40	16.60	16.80	17.00	17.20	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	220.49	1157	16.50	17.00	17.30	17.50	17.70	17.90	
Training & Education	Access Management	0.25	0	4.80	5.00	5.10	5.20	5.40	5.60	
Training & Education	Anti Spam Solutions	0.09	0	6.60	6.80	7.00	7.20	7.40	7.60	
Training & Education	Anti Virus/Worm	0.00	0	0	0	0	0	0	0	
Training & Education	Application Code Security	0.17	0	5.00	5.10	5.30	5.50	5.60	5.80	
Training & Education	Business Continuity/Recovery	0.04	0	5.00	5.20	5.30	5.50	5.70	5.80	
Training & Education	Computer Forensics	0.01	0	4.70	4.90	5.00	5.20	5.30	5.50	
Training & Education	Content Filtering & Monitoring	0.09	0	5.10	5.30	5.40	5.50	5.70	5.90	
Training & Education	Encryption/PKI/Digital Certificates	0.11	0	6.20	6.40	6.50	6.80	7.00	7.20	
Training & Education	Firewalls	0.07	0	5.10	5.30	5.40	5.60	5.70	5.90	
Training & Education	Identity Management	0.29	1	3.80	4.00	4.10	4.20	4.40	4.50	
Training & Education	Intrusion Detection	0.10	0	4.20	4.30	4.40	4.60	4.60	4.80	
Training & Education	Malware	0.05	0	6.20	6.40	6.60	6.70	6.90	7.10	
Training & Education	Messaging Security	0.16	0	4.70	4.80	5.00	5.10	5.30	5.50	
Training & Education	Mobile Security/Device management	0.16	0	6.50	6.70	6.90	7.00	7.30	7.50	
Training & Education	Patch Management	0.02	0	7.00	7.30	7.60	7.80	8.00	8.30	
Training & Education	PC/Mobile/End Point Security	0.31	1	5.60	5.80	5.90	6.10	6.30	6.50	
Training & Education	Vulnerability Assessment	0.12	0	6.10	6.20	6.40	6.70	6.80	7.00	
Training & Education	Wireless Security	0.20	0	5.00	5.10	5.30	5.40	5.60	5.80	

1.1.71 UK

Level 2	Level 3	Sales EURM	Employees	Forecast Growth %						
				2016	2017	2018	2019	2020	2021	2022
Anti Malware	Anti Spam Solutions	56.94	797	9.20	10.20	10.50	10.80	11.10	11.50	
Anti Malware	Anti Virus/Worm	171.98	1751	11.30	12.50	13.00	13.30	13.80	14.10	
Anti Malware	Malware	43.64	628	8.80	9.70	10.00	10.30	10.60	11.00	
Anti Malware	Specialist Anti Malware	1001.68	3700	21.20	23.50	24.20	25.10	25.80	26.50	
Application Security	Application Code Security	45.96	638	7.50	8.20	8.50	8.80	9.00	9.30	
Application Security	Content Filtering & Monitoring	38.80	545	9.00	9.90	10.20	10.50	10.80	11.10	
Application Security	Patch Management	32.18	451	8.60	9.40	9.80	10.10	10.30	10.60	
Application Security	Vulnerability Assessment	3731.67	14500	19.10	21.20	21.80	22.50	23.20	23.90	
Business Continuity	Business Continuity/Recovery	399.22	2087	20.70	22.90	23.60	24.30	25.00	25.70	
Business Continuity	Computer Forensics	203.67	1732	29.20	32.20	32.90	33.20	33.50	34.10	
Business Continuity	IT/Cyber Forensics	1645.52	4402	13.80	15.30	15.70	16.30	16.70	17.20	
Cyber Consultancy	Access Management	5.47	106	8.30	9.10	9.40	9.70	10.00	10.30	
Cyber Consultancy	Anti Spam Solutions	4.23	94	9.20	10.20	10.50	10.80	11.20	11.50	
Cyber Consultancy	Anti Virus/Worm	4.09	83	7.80	8.70	9.00	9.20	9.50	9.80	
Cyber Consultancy	Application Code Security	4.31	82	7.30	8.10	8.30	8.60	8.90	9.10	
Cyber Consultancy	Business Continuity/Recovery	3.72	76	8.20	9.10	9.40	9.60	9.90	10.20	
Cyber Consultancy	Computer Forensics	5.20	108	8.60	9.50	9.90	10.20	10.40	10.80	
Cyber Consultancy	Content Filtering & Monitoring	3.88	79	8.60	9.60	9.90	10.10	10.40	10.70	
Cyber Consultancy	Corporate Services	575.47	4248	26.90	29.80	30.20	30.60	31.00	31.40	
Cyber Consultancy	Encryption/PKI/Digital Certificates	5.69	102	8.50	9.40	9.70	10.00	10.30	10.60	
Cyber Consultancy	Firewalls	2.12	52	6.90	7.60	7.80	8.10	8.30	8.60	
Cyber Consultancy	Identity Management	7.37	122	8.00	8.90	9.10	9.40	9.70	10.00	
Cyber Consultancy	Intrusion Detection	3.45	70	7.30	8.10	8.30	8.60	8.80	9.10	
Cyber Consultancy	Malware	5.32	104	7.80	8.70	9.00	9.30	9.50	9.80	
Cyber Consultancy	Messaging Security	6.41	126	9.00	10.00	10.30	10.50	10.90	11.20	
Cyber Consultancy	Mobile Security/Device management	5.80	108	8.70	9.60	9.90	10.20	10.50	10.80	
Cyber Consultancy	Patch Management	3.43	74	8.80	9.80	10.00	10.30	10.60	11.00	
Cyber Consultancy	PC/Mobile/End Point Security	3.40	82	8.20	9.10	9.30	9.60	9.90	10.20	
Cyber Consultancy	Vulnerability Assessment	4.49	95	8.90	9.80	10.10	10.50	10.70	11.10	
Cyber Consultancy	Wireless Security	3.51	87	9.50	10.50	10.70	11.10	11.40	11.80	
Cyber Security Insurance	Business Interruption from Network Downtime	77.91	616	10.20	11.30	11.70	12.00	12.40	12.80	
Cyber Security Insurance	Cyber Extortion	71.16	599	10.20	11.30	11.70	12.00	12.40	12.70	
Cyber Security Insurance	Investigation of Privacy Breach	18.80	164	10.70	11.80	12.30	12.60	13.00	13.40	
Cyber Security Insurance	Loss of Third Party Data	101.82	862	10.30	11.30	11.70	12.00	12.40	12.80	
Cyber Security Insurance	Loss or Damage to Digital Assets	65.32	519	10.00	11.10	11.40	11.80	12.10	12.50	
Cyber Security Insurance	Multi-Media Liability	62.05	547	9.90	11.00	11.30	11.70	12.00	12.40	
Cyber Security Insurance	Reputational Damage	34.63	275	10.10	11.20	11.50	11.90	12.20	12.60	
Cyber Security Insurance	Security and Privacy Breaches	97.54	806	10.40	11.50	11.80	12.20	12.60	13.00	
Cyber Security Insurance	Theft of Money and Digital Assets	53.81	428	10.40	11.50	11.80	12.30	12.60	13.00	
Cyber Security Insurance	Third Party Breach Notification	34.83	270	9.70	10.80	11.10	11.50	11.80	12.10	
Encryption	Digital Signatures	215.46	1533	32.20	35.70	36.10	36.60	36.80	37.30	
Encryption	Encryption/PKI/Digital Certificates	120.55	1241	23.80	26.50	26.80	27.20	27.60	28.10	
Encryption	Storage Security, including Cloud	388.79	2723	31.30	34.60	35.00	35.40	35.90	36.40	
Identity & Access	Access Management	76.30	1000	9.10	10.10	10.40	10.70	11.10	11.30	
Identity & Access	Authentication	524.25	3649	35.30	39.10	39.60	40.20	40.70	41.20	
Identity & Access	Identity Management	1379.11	9361	32.10	35.60	35.90	36.50	36.90	37.30	
Identity & Access	Intrusion & Anomaly Prevention	235.02	1600	33.40	36.90	37.50	37.80	38.40	39.00	
Identity & Access	Messaging Security	281.66	2358	18.10	20.00	20.30	20.60	20.90	21.30	
Infrastructure	Data Management	382.32	2780	22.70	25.20	25.60	25.80	26.20	26.50	
Infrastructure	Firewalls	59.37	755	7.00	7.70	8.00	8.20	8.40	8.70	
Infrastructure	Infrastructure Monitoring	206.55	1518	33.90	37.60	38.20	38.50	38.70	39.40	
Infrastructure	Infrastructure Resilience	214.55	1289	35.30	39.10	39.70	40.00	40.30	41.20	
Infrastructure	Intrusion Detection	3098.18	10655	16.40	18.20	18.60	18.90	19.30	19.70	
Infrastructure	Outsourced/Managed Services	232.30	1447	32.40	35.80	36.40	36.80	37.40	37.80	
Infrastructure	Storage Security, including Cloud	723.38	4973	33.70	37.20	37.90	38.20	38.80	39.30	
Mobile	Mobile Security/Device management	94.65	1285	9.10	10.00	10.40	10.70	11.00	11.30	
Mobile	PC/Mobile/End Point Security	106.89	1082	12.40	13.70	14.10	14.50	15.00	15.40	
Mobile	VPN	224.22	1439	33.20	37.00	37.30	37.90	38.00	38.70	
Mobile	Wireless Security	90.64	1206	9.50	10.50	10.80	11.10	11.40	11.80	
Outsourced/Managed Services	Access Management	1.24	57	8.20	9.10	9.40	9.70	10.00	10.30	
Outsourced/Managed Services	Anti Spam Solutions	0.83	48	8.60	9.60	9.80	10.10	10.40	10.70	
Outsourced/Managed Services	Anti Virus/Worm	1.25	39	7.20	8.00	8.20	8.50	8.70	9.00	
Outsourced/Managed Services	Application Code Security	3.11	70	7.60	8.40	8.70	8.90	9.20	9.50	
Outsourced/Managed Services	Business Continuity/Recovery	0.64	40	8.20	9.10	9.30	9.60	9.80	10.20	
Outsourced/Managed Services	Content Filtering & Monitoring	1.07	42	8.10	9.00	9.30	9.50	9.80	10.10	
Outsourced/Managed Services	Cyber Services	690.66	4696	32.40	36.00	36.50	36.90	37.20	37.80	
Outsourced/Managed Services	Encryption/PKI/Digital Certificates	1.68	51	8.60	9.60	9.80	10.10	10.40	10.80	
Outsourced/Managed Services	Firewalls	2.30	56	7.20	7.90	8.10	8.40	8.70	8.90	
Outsourced/Managed Services	Identity Management	4.20	91	8.90	9.90	10.20	10.50	10.80	11.20	
Outsourced/Managed Services	Intrusion Detection	1.10	35	7.30	8.10	8.20	8.40	8.60	8.70	
Outsourced/Managed Services	Malware	0.42	36	8.40	9.30	9.60	9.80	10.10	10.40	
Outsourced/Managed Services	Messaging Security	2.93	74	8.30	9.10	9.40	9.70	10.00	10.40	
Outsourced/Managed Services	Mobile Security/Device management	2.66	65	8.80	9.80	10.10	10.40	10.70	11.00	
Outsourced/Managed Services	Patch Management	0.87	45	8.40	9.30	9.50	9.90	10.10	10.40	
Outsourced/Managed Services	PC/Mobile/End Point Security	1.04	50	8.00	8.90	9.10	9.40	9.70	10.00	
Outsourced/Managed Services	Vulnerability Assessment	1.79	68	8.80	9.70	10.00	10.30	10.60	10.90	
Outsourced/Managed Services	Wireless Security	1.37	60	9.20	10.20	10.60	10.80	11.20	11.50	
Situational Awareness	Darkweb	37.59	316	10.90	12.00	12.20	12.30	12.50	12.70	
Situational Awareness	External Cyber Threat Intelligence	2705.85	9213	17.40	19.40	19.60	20.00	20.30	20.70	
Situational Awareness	High Level Situational Awareness	2193.68	6840	12.10	13.40	13.80	14.20	14.60	15.10	
Situational Awareness	Internal Cyber Threat Intelligence	489.06	1963	19.10	21.20	21.50	21.80	22.20	22.60	
Situational Awareness	Low Level Situational Awareness	934.90	1739	17.20	19.00	19.50	20.20	20.70	21.40	
Situational Awareness	Media Monitoring	196.96	1375	11.60	12.80	12.90	13.10	13.30	13.50	
Situational Awareness	Proactive Cyber Surveillance	1133.67	4801	15.60	17.20	17.40	17.70	17.90	18.10	
System Recovery & Data Cleansing	Data Recovery Services	1915.76	7129	19.70	21.80	22.10	22.40	22.70	22.90	
System Recovery & Data Cleansing	Manual Data Cleansing	867.22	3703	17.80	19.70	20.00	20.20	20.40	20.70	
System Recovery & Data Cleansing	System Recovery & Data Cleansing	3437.19	12598	18.20	20.20	20.40	20.70	20.90	21.20	
Training & Education	Access Management	1.97	70	9.70	10.80	11.10	11.30	11.70	12.10	
Training & Education	Anti Spam Solutions	0.60	48	8.80	9.80	10.10	10.40	10.70	11.00	
Training & Education	Anti Virus/Worm	0.11	30	7.60	8.40	8.70	8.90	9.20	9.40	
Training & Education	Application Code Security	1.24	45	7.60	8.40	8.60	8.90	9.20	9.40	
Training & Education	Business Continuity/Recovery	0.37	44	8.90	9.90	10.10	10.40	10.70	11.10	
Training & Education	Computer Forensics	0.20	40	7.90	8.80	9.10	9.30	9.70	9.90	
Training & Education	Content Filtering & Monitoring	0.61	38	9.10	10.00	10.40	10.70	11.00	11.30	
Training & Education	Encryption/PKI/Digital Certificates	0.73	41	8.70	9.70	10.00	10.20	10.60	10.90	
Training & Education	Firewalls	0.43	31	6.70	7.40	7.70	7.90	8.10	8.30	
Training & Education	Identity Management	3.33	70	8.60	9.60	9.90	10.10	10.50	10.80	
Training & Education	Intrusion Detection	0.64	29	7.10	7.80	8.00	8.30	8.50	8.80	
Training & Education	Malware	0.32	37	8.60	9.50	9.90	10.20	10.40	10.80	
Training & Education	Messaging Security	1.44	61	8.80	9.80	10.10	10.40	10.70	10.90	
Training & Education	Mobile Security/Device management	1.49	52	7.80	8.70	8.90	9.20	9.40	9.70	
Training & Education	Patch Management	0.33	37	8.40	9.30	9.60	9.90	10.20	10.50	
Training & Education	PC/Mobile/End Point Security	1.82	64	8.30	9.20	9.50	9.80	10.00	10.30	
Training & Education	Vulnerability Assessment	0.80	47	8.30	9.20	9.50	9.80	10.10	10.40	
Training & Education	Wireless Security	1.57	59	9.30	10.20	10.60	10.90	11.20	11.50	

Appendix B : EU Sales by Sub-sector and Purchaser Industry

Austria													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communications EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR
Anti Malware	180.0	1.1	8.4	1.5	6.5	102.3	2.8	1.9	5.3	3.9	6.4	3.2	3.3
Application Security	518.8	5.5	17.1	4.8	17.2	21.1	290.2	6.7	18.2	9.2	18.3	9.8	7.9
Business Continuity	284.8	4.0	8.4	2.6	9.2	11.4	157.8	3.5	3.9	9.2	6.4	10.5	3.9
Cyber Consultancy	438.8	0.6	1.4	0.4	1.4	1.8	241.1	0.8	0.5	1.5	0.7	1.5	0.5
Cyber Security Insurance	920.0	0.9	3.6	0.8	2.9	3.8	502.1	1.8	1.4	2.8	1.7	3.5	1.7
Encryption	414.0	0.7	1.5	0.4	1.3	1.8	219.1	0.8	0.6	1.4	1.0	1.3	1.2
Identity & Access	179.2	1.2	6.8	1.7	5.6	7.4	98.4	3.4	2.1	5.6	2.7	6.4	3.2
Infrastructure	817.5	6.1	28.7	7.7	28.0	32.7	462.5	12.1	4.6	25.1	9.4	30.4	15.1
Mobile	581.0	0.5	2.1	0.5	1.8	2.4	31.4	1.3	0.8	1.9	0.8	1.1	0.8
Outsourced/Managed Services	418.0	0.2	1.7	0.4	1.3	1.7	22.5	0.9	0.6	1.4	0.8	0.7	0.7
Situational Awareness	607.7	7.8	22.4	5.6	18.5	24.5	332.4	11.7	7.6	20.4	9.9	21.1	11.8
System Recovery & Data Cleansing	385.6	3.6	14.2	3.6	11.8	16.0	212.1	6.2	4.1	12.1	7.1	12.7	6.5
Training & Education	2.3	0.0	0.1	0.0	0.1	0.1	1.3	0.0	0.0	0.1	0.1	0.0	0.0
Total	3,262.0	32.2	116.4	30.0	105.6	1,807.1	52.0	33.4	105.0	53.7	115.7	56.3	54.4
Belgium													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communications EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR
Anti Malware	232.1	3.2	8.6	2.0	4.6	15.9	124.8	2.8	3.7	7.8	2.6	8.0	1.0
Application Security	877.3	24.6	30.2	8.4	20.1	64.3	432.1	14.2	8.5	36.1	22.3	29.0	31.9
Business Continuity	484.8	10.4	17.9	4.3	11.1	36.9	248.3	5.8	10.3	15.1	8.3	16.7	18.8
Cyber Consultancy	500.0	1.3	1.8	0.5	1.1	3.7	25.4	0.7	0.7	2.1	0.6	1.9	1.3
Cyber Security Insurance	113.3	2.1	4.3	1.0	2.4	7.8	58.1	1.8	1.5	4.5	2.5	4.0	4.0
Encryption	493.1	0.8	2.1	0.4	1.1	3.9	24.8	1.0	0.8	2.1	0.4	2.0	1.8
Identity & Access	188.4	3.8	6.9	1.7	4.4	13.2	96.2	2.5	2.3	7.1	5.1	7.2	6.4
Infrastructure	1,163.8	21.0	36.9	10.2	28.2	82.6	601.0	14.0	28.7	44.9	23.8	41.0	32.8
Mobile	769.0	1.2	3.1	0.7	1.6	5.6	40.6	1.1	0.7	3.0	1.3	2.7	2.7
Outsourced/Managed Services	457.7	1.7	1.7	0.4	1.2	3.7	21.5	0.5	0.7	2.0	1.1	1.6	1.4
Situational Awareness	755.5	14.4	25.9	6.9	16.9	51.1	394.5	12.8	12.5	30.9	13.8	27.2	25.4
System Recovery & Data Cleansing	502.9	8.8	20.2	4.5	11.2	38.0	248.6	6.3	6.3	22.2	15.4	17.2	19.8
Training & Education	3.1	0.0	0.1	0.0	0.1	0.2	1.6	0.0	0.0	0.1	0.0	0.1	0.0
Total	4,542.9	83.3	159.7	41.0	104.0	336.9	2,317.5	63.5	77.7	177.9	97.2	156.6	49.8
Bulgaria													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communications EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR
Anti Malware	60.8	0.4	2.2	1.2	1.7	2.7	32.0	1.5	0.8	2.5	0.5	0.7	0.8
Application Security	137.6	1.2	6.3	4.8	3.8	7.3	68.0	1.7	2.9	4.5	2.8	5.2	6.7
Business Continuity	64.3	0.8	2.3	2.7	2.4	3.0	30.6	1.4	1.8	1.7	1.5	3.1	3.0
Cyber Consultancy	82.0	0.1	0.3	0.3	0.2	0.4	4.1	0.1	0.3	0.3	0.1	0.3	0.1
Cyber Security Insurance	229.0	0.3	0.9	0.8	0.7	1.1	11.6	0.3	0.4	0.7	0.5	0.9	0.3
Encryption	7.0	0.1	0.3	0.2	0.2	0.4	3.6	0.1	0.2	0.2	0.2	0.3	0.0
Identity & Access	31.4	0.4	1.2	1.3	0.9	1.4	15.5	0.5	0.9	1.0	0.7	1.2	0.4
Infrastructure	153.9	1.7	7.1	6.4	4.7	7.0	73.3	3.5	5.2	5.0	2.7	6.2	7.1
Mobile	109.0	0.1	0.4	0.4	0.4	0.6	5.4	0.2	0.3	0.3	0.2	0.4	0.5
Outsourced/Managed Services	6.7	0.1	0.3	0.3	0.2	0.3	3.3	0.1	0.1	0.2	0.1	0.3	0.1
Situational Awareness	153.7	1.6	6.4	5.7	5.1	7.6	74.9	3.0	3.8	4.9	3.0	8.1	1.6
System Recovery & Data Cleansing	95.3	1.1	3.9	3.2	3.0	4.7	47.9	1.5	2.9	2.8	1.1	3.7	1.5
Training & Education	0.3	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.0	0.0
Total	755.0	7.9	31.6	27.3	23.3	36.5	371.4	13.9	19.6	24.1	13.4	10.3	7.3
													17.6
													34.4
													23.3

© Anakyn bvba for LSEC – PWC - EC

Denmark																		
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level 2																		
Anti Malware	108.8	1.9	2.7	2.6	2.5	3.8	62.1	1.5	1.3	4.7	2.9	1.5	4.2	1.6	4.4	0.7	2.8	5.1
Application Security	372.0	2.9	9.3	5.8	8.3	12.6	206.8	7.0	4.7	13.8	2.0	15.7	7.3	16.6	3.5	11.3	17.3	8.3
Business Continuity	172.2	3.6	4.8	3.0	3.8	6.3	89.5	4.5	2.0	7.3	2.3	6.6	3.2	8.4	1.8	4.4	6.7	3.8
Cyber Consultancy	23.9	0.5	0.6	0.4	0.5	0.9	13.0	0.5	0.3	0.8	0.3	0.9	0.6	1.0	0.3	0.7	1.0	0.5
Cyber Security Insurance	62.1	1.2	1.6	1.2	1.4	2.3	33.3	1.1	1.0	2.4	0.8	2.5	1.4	3.0	0.6	1.7	2.6	1.4
Encryption	21.2	0.5	0.5	0.3	0.5	0.8	11.5	0.3	0.3	0.3	0.7	0.4	0.9	0.4	1.1	0.3	0.6	0.9
Identity & Access	80.0	1.1	2.2	1.3	1.7	2.9	44.3	1.5	0.8	2.6	1.1	3.3	1.9	3.3	1.9	2.3	3.3	1.7
Infrastructure	552.3	6.7	14.8	8.2	14.3	20.3	300.8	10.3	7.2	15.8	7.4	22.6	13.4	27.6	4.0	14.0	22.3	14.3
Mobile	35.1	0.5	1.0	0.6	0.8	1.2	19.1	0.6	0.7	1.2	0.6	1.4	0.9	1.4	0.3	1.0	1.5	0.8
Outsourced/Managed Services	20.5	0.2	0.5	0.4	0.5	0.7	11.2	0.3	0.2	0.8	0.3	0.8	0.3	0.9	0.2	0.6	0.9	0.5
Situational Awareness	390.2	4.7	11.0	6.3	8.6	14.3	210.6	8.0	7.3	14.1	5.5	16.6	9.0	16.4	2.8	11.2	16.4	8.6
System Recovery & Data Cleansing	236.7	4.2	6.4	4.2	5.2	8.2	130.1	3.6	4.2	8.9	2.8	10.0	4.8	10.5	2.4	6.6	9.6	5.2
Training & Education	1.7	0.0	0.0	0.0	0.0	0.0	0.9	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.1	0.0
Total	2,076.7	28.0	55.4	34.3	48.1	74.3	1,133.2	39.2	30.0	71.3	25.0	85.6	45.1	95.0	17.6	57.2	87.7	48.1
Estonia																		
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level 2																		
Anti Malware	20.0	0.1	0.9	0.5	0.4	1.8	10.1	0.5	0.3	0.3	0.7	0.3	0.7	0.2	1.1	0.4	0.6	0.4
Application Security	53.0	0.4	2.1	2.0	1.0	4.8	25.7	0.8	1.1	2.0	0.8	1.8	0.8	2.3	0.6	2.0	1.4	1.0
Business Continuity	20.7	0.2	0.8	1.0	0.4	1.5	9.7	0.2	0.8	0.9	0.4	0.7	0.5	0.8	0.4	0.6	0.5	0.4
Cyber Consultancy	2.6	0.0	0.1	0.1	0.0	0.2	1.3	0.0	0.1	0.1	0.0	0.1	0.0	0.1	0.0	0.1	0.1	0.0
Cyber Security Insurance	7.6	0.1	0.4	0.3	0.1	0.6	3.5	0.1	0.2	0.3	0.1	0.3	0.1	0.4	0.1	0.3	0.2	0.1
Encryption	2.8	0.0	0.1	0.1	0.0	0.2	1.3	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.0
Identity & Access	10.4	0.1	0.5	0.4	0.2	0.8	5.0	0.2	0.2	0.2	0.1	0.4	0.2	0.5	0.2	0.4	0.3	0.2
Infrastructure	55.9	0.4	1.9	2.1	1.0	4.7	28.1	0.9	0.7	2.2	1.5	2.0	1.2	2.4	0.5	1.5	1.6	1.0
Mobile	3.5	0.0	0.2	0.2	0.1	0.3	1.6	0.0	0.1	0.1	0.2	0.1	0.1	0.2	0.0	0.1	0.1	0.1
Outsourced/Managed Services	2.6	0.0	0.1	0.1	0.0	0.2	1.3	0.0	0.0	0.0	0.1	0.0	0.1	0.0	0.1	0.1	0.1	0.0
Situational Awareness	51.2	0.4	2.3	2.3	0.9	4.4	23.5	0.8	1.6	2.0	0.7	1.7	0.9	2.6	0.9	1.8	1.4	0.9
System Recovery & Data Cleansing	32.4	0.3	1.6	1.4	1.4	0.6	14.4	0.6	1.1	1.5	0.6	1.1	0.6	1.6	0.6	1.1	0.9	0.6
Training & Education	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total	262.7	2.0	11.0	10.5	4.7	22.1	125.6	4.1	6.3	10.7	4.7	9.1	4.7	12.2	3.9	8.7	7.2	4.7
Finland																		
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level 2																		
Anti Malware	75.9	0.8	3.6	1.6	1.4	4.7	40.3	0.4	2.5	1.4	0.6	2.8	1.2	4.9	0.2	3.2	2.2	1.4
Application Security	384.0	4.7	17.0	7.7	6.8	26.3	201.1	9.4	8.9	7.0	4.7	14.0	7.8	18.5	2.5	15.7	10.8	6.8
Business Continuity	210.1	1.2	7.0	2.9	3.5	12.5	123.7	3.5	3.7	3.5	2.0	6.9	3.7	7.1	1.2	8.4	5.9	3.5
Cyber Consultancy	24.5	0.3	1.0	0.4	0.4	1.7	12.5	0.5	0.8	0.4	0.4	0.8	0.4	1.4	0.2	1.1	0.6	0.4
Cyber Security Insurance	55.2	0.5	2.2	1.1	1.0	3.7	29.4	1.0	1.4	1.0	0.7	2.0	1.0	2.8	0.3	2.3	1.6	1.0
Encryption	23.6	0.2	0.9	0.5	0.4	1.5	12.9	0.3	0.5	0.4	0.2	0.9	0.4	1.3	0.2	0.9	0.7	0.4
Identity & Access	90.3	1.3	3.8	2.0	1.6	5.8	47.4	2.3	1.8	1.6	1.3	3.1	1.4	4.9	0.6	3.3	2.4	1.6
Infrastructure	356.8	2.8	15.4	7.4	6.3	25.8	185.1	9.7	7.1	6.3	6.4	13.3	6.0	16.8	3.4	13.3	9.8	6.3
Mobile	38.3	0.4	1.7	0.7	0.7	2.7	20.7	0.8	0.7	0.7	0.5	1.4	0.6	1.9	0.3	1.4	1.0	0.7
Outsourced/Managed Services	24.1	0.3	1.0	0.4	0.4	1.5	12.8	0.4	0.7	0.4	0.2	0.9	0.5	1.1	0.2	0.9	0.6	0.4
Situational Awareness	360.2	3.1	15.6	6.8	6.6	22.9	190.0	9.3	10.6	6.7	3.7	12.2	6.9	17.8	2.6	14.7	9.9	6.6
System Recovery & Data Cleansing	219.9	2.8	9.4	4.0	4.0	15.4	116.9	3.5	7.4	3.9	1.9	8.3	4.1	10.5	1.4	8.3	5.9	4.0
Training & Education	1.4	0.0	0.0	0.0	0.0	0.1	0.8	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0
Total	1,864.3	18.4	78.6	35.5	33.1	124.6	993.6	42.1	46.1	33.3	22.6	66.6	34.0	89.1	13.1	73.6	51.4	33.1

France																			
Level 2	Chemicals & Pharma		Commercial Facilities	Communi- cations	Manufacturing	Defence Industries	Public	Construction	Financial Services	Food & Agriculture	Other Utilities	Government Facilities	Healthcare Technology	Education	Transport & Logistics	Water Utilities	Emergency Services		
	Total EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR		
	838.8	6.3	38.7	26.9	29.9	62.4	385.8	4.6	10.1	45.2	18.0	35.1	12.1	39.8	23.0	24.4	34.6	29.9	
	3713.6	36.5	153.0	172.2	123.1	36.5	216.2	52.3	88.6	123.2	36.4	142.4	99.8	157.1	63.5	99.8	130.6	123.1	
	2587.4	27.3	100.6	86.2	86.4	150.9	1383.7	26.1	45.0	104.3	15.3	90.0	51.3	103.6	36.2	66.4	83.4	86.4	
	287.3	2.3	10.9	11.8	9.2	18.7	140.1	5.0	7.5	11.7	2.8	10.7	6.8	11.7	5.5	7.7	10.3	9.2	
	624.1	5.4	27.7	24.1	19.2	38.9	301.1	7.7	17.1	25.3	6.8	25.9	13.9	25.7	13.4	17.2	23.5	19.2	
	274.9	3.2	11.6	11.9	7.6	16.7	135.5	3.4	7.0	9.3	3.2	11.2	7.5	10.0	4.5	7.6	9.5	7.6	
	1004.2	12.4	42.9	40.9	31.0	63.6	501.7	15.6	12.5	41.0	6.9	40.7	22.0	42.6	16.8	25.7	35.2	31.0	
	5462.3	69.9	246.1	152.2	198.9	351.1	2652.4	69.5	64.6	209.5	63.3	235.7	150.9	243.3	103.0	146.5	188.0	198.9	
	431.9	3.9	20.1	16.9	13.3	27.7	209.3	6.9	11.2	17.8	4.9	17.9	9.4	17.6	5.8	12.0	15.6	13.3	
	265.4	3.0	11.2	10.5	7.1	16.9	131.1	4.3	8.4	8.7	3.6	9.8	5.2	8.4	5.5	7.0	10.4	7.1	
	5286.2	57.3	206.8	249.6	157.6	356.3	2572.9	82.8	86.3	188.7	78.9	210.9	110.2	204.0	104.1	138.6	184.4	157.6	
2515.1	20.7	95.3	102.5	81.2	61.3	165.0	32.7	61.3	96.2	25.1	105.1	63.3	101.7	56.5	68.7	92.1	81.2		
16.8	0.2	0.7	0.7	0.5	1.1	8.3	0.2	0.3	0.7	0.2	0.2	0.7	0.4	0.7	0.3	0.5	0.6	0.5	
23308.0	248.4	965.6	906.4	765.0	1485.5	11451.3	311.1	419.9	881.1	265.4	936.1	552.8	966.2	438.1	622.1	818.2	765.0	765.0	
Germany																			
Level 2	Chemicals & Pharma		Commercial Facilities	Communi- cations	Manufacturing	Defence Industries	Public	Construction	Financial Services	Food & Agriculture	Other Utilities	Government Facilities	Healthcare Technology	Education	Transport & Logistics	Water Utilities	Emergency Services		
	Total EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR		
	1683.7	9.4	78.0	20.7	34.2	150.4	913.5	15.4	17.8	62.7	29.0	54.6	45.2	52.1	15.0	39.2	49.2	34.2	
	7600.8	73.0	285.9	147.8	174.1	497.4	4175.5	59.0	164.6	237.7	137.7	256.4	115.4	290.3	77.9	207.7	235.8	174.1	
	2240.3	6.9	81.4	33.5	42.9	185.2	1203.9	26.7	40.3	90.0	60.2	88.8	38.6	75.7	31.3	53.5	64.3	42.9	
	439.3	4.2	19.3	7.1	8.8	29.2	236.5	5.4	8.0	17.9	8.9	14.8	7.5	15.8	5.3	10.8	14.9	8.8	
	860.0	6.6	37.6	16.2	19.5	68.8	453.1	9.2	14.4	32.1	15.8	31.4	15.9	31.1	7.9	22.7	28.4	19.5	
	460.1	4.2	18.7	8.3	10.6	33.7	242.9	5.5	11.6	16.6	8.6	15.0	8.5	17.0	7.0	10.8	15.0	10.6	
	1668.2	17.3	70.5	31.9	38.1	119.8	898.6	15.7	14.9	60.6	40.5	57.5	28.8	57.2	19.0	47.8	53.3	38.1	
	8494.4	98.4	381.8	140.7	175.4	667.5	4488.7	93.8	121.0	314.8	142.8	260.3	153.0	355.7	101.5	222.3	257.4	175.4	
	576.6	4.5	22.7	11.9	14.2	4.5	32.5	317.2	5.3	13.5	12.9	20.3	9.8	22.0	3.8	14.8	17.6	14.2	
	454.5	4.1	21.0	6.7	11.3	32.8	245.1	6.5	4.8	15.1	9.4	18.1	7.7	16.1	4.0	12.8	13.9	11.3	
	6436.2	71.1	269.5	111.6	153.0	414.3	3477.4	101.7	124.1	224.1	83.2	258.4	115.5	218.4	70.3	161.0	204.2	153.0	
3332.5	24.3	138.6	60.0	78.6	248.4	1727.7	42.7	56.4	132.3	85.6	119.1	61.9	124.9	51.7	88.8	106.3	78.6		
22.6	0.2	0.9	0.4	0.5	1.7	12.3	0.2	0.4	0.7	0.4	0.4	0.8	0.4	0.9	0.6	0.7	0.5		
34269.2	324.2	1425.9	596.8	761.2	2481.7	18392.4	387.1	591.8	1222.4	635.0	1195.5	608.2	1277.2	395.0	892.8	1061.0	761.2	761.2	
Greece																			
Level 2	Chemicals & Pharma		Commercial Facilities	Communi- cations	Manufacturing	Defence Industries	Public	Construction	Financial Services	Food & Agriculture	Other Utilities	Government Facilities	Healthcare Technology	Education	Transport & Logistics	Water Utilities	Emergency Services		
	Total EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR	EUR		
	57.6	2.1	2.5	1.3	1.9	3.2	30.5	0.8	0.8	1.7	0.3	2.0	1.3	1.3	0.3	2.0	2.4	1.9	
	135.9	2.5	5.5	5.4	4.6	9.8	68.7	1.3	2.1	3.5	1.3	5.1	3.3	2.9	0.9	5.3	6.1	4.6	
	107.5	2.5	5.0	3.2	4.1	6.9	52.5	0.7	2.5	3.1	1.1	3.7	2.7	2.5	0.5	4.5	5.4	4.1	
	31.3	0.6	1.2	1.0	1.0	1.9	15.9	0.4	0.8	0.9	0.2	1.2	0.6	0.7	0.2	1.3	1.5	1.0	
	83.5	1.9	3.2	3.1	2.5	5.7	42.2	0.9	1.8	2.3	0.7	3.1	2.0	1.8	0.6	3.4	3.6	2.5	
	28.4	0.6	1.4	1.0	1.0	1.8	13.8	0.2	0.9	0.8	0.3	1.1	0.7	0.7	0.2	1.0	1.2	1.0	
	97.2	1.5	4.0	3.3	3.1	6.3	47.7	1.1	4.1	2.7	0.9	3.4	2.0	2.2	0.6	4.1	4.5	3.1	
	192.1	3.2	7.7	7.1	6.3	13.0	96.2	1.9	4.4	5.1	1.6	7.0	5.1	4.6	1.1	7.8	8.8	6.3	
	37.7	0.6	1.5	1.4	1.3	2.7	19.0	0.3	0.8	1.1	0.4	1.4	0.7	0.9	0.3	1.4	1.9	1.3	
	28.0	0.5	1.3	1.0	0.8	1.9	13.9	0.3	0.8	1.0	0.7	0.3	0.9	0.5	0.6	0.2	1.3	1.4	0.8
	413.9	7.3	16.5	15.6	13.4	27.7	208.5	3.9	9.2	11.5	3.9	14.6	9.4	8.8	3.4	16.3	19.5	13.4	
331.5	5.2	13.1	11.9	9.7	22.2	168.4	1.8	3.3	10.3	2.8	11.9	7.3	7.4	3.2	12.6	14.5	9.7		
2.1	0.0	0.1	0.1	0.1	0.1	1.1	0.0	0.1	0.0	0.0	0.1	0.0	0.0	0.1	0.1	0.1	0.1		
1546.7	28.5	63.0	55.4	49.8	103.2	778.4	15.1	38.6	42.1	13.8	55.5	35.6	34.4	11.5	61.1	70.9	49.8		

Hungary													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR
Anti Malware	28.3	0.2	0.8	0.3	0.6	1.5	15.3	0.4	1.3	1.0	0.2	1.2	0.5
Application Security	80.6	0.7	2.7	0.7	1.8	4.9	43.2	1.7	1.6	3.1	1.4	3.7	1.1
Business Continuity	68.8	0.6	2.2	0.6	1.6	4.3	36.4	1.0	2.7	2.1	0.9	2.6	0.9
Cyber Consultancy	20.3	0.2	0.7	0.2	0.5	1.3	10.5	0.3	0.8	0.8	0.5	0.9	0.2
Cyber Security Insurance	54.4	0.5	1.7	0.5	1.2	3.6	29.2	0.8	1.3	2.1	0.7	2.5	0.7
Encryption	17.4	0.1	0.5	0.2	0.4	1.2	9.3	0.3	0.5	0.6	0.3	0.8	0.2
Identity & Access	57.1	0.6	1.8	0.5	1.3	3.8	30.2	1.2	1.3	2.0	0.4	2.6	0.9
Infrastructure	124.7	1.2	3.7	1.1	2.8	8.3	66.6	1.9	3.0	4.4	2.0	6.2	1.7
Mobile	21.6	0.3	0.7	0.2	0.5	1.4	11.5	0.2	0.7	0.8	0.3	1.0	0.3
Outsourced/Managed Services	17.6	0.1	0.4	0.1	0.4	1.1	9.8	0.2	0.2	0.2	0.4	0.9	0.2
Situational Awareness	278.1	2.3	9.4	2.5	6.3	17.0	147.7	5.2	8.3	10.8	4.7	11.9	3.9
System Recovery & Data Cleansing	252.8	1.8	8.0	2.3	5.7	16.3	137.3	4.4	4.7	9.6	4.4	11.0	3.7
Training & Education	1.0	0.0	0.0	0.0	0.0	0.0	0.6	0.0	0.0	0.0	0.0	0.0	0.0
Total	1,022.7	8.6	32.6	9.2	23.1	64.7	547.6	17.6	26.4	37.9	16.2	45.3	14.2

Ireland													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR
Anti Malware	86.9	1.1	1.9	2.1	2.7	4.1	48.9	0.9	1.8	2.4	1.2	2.5	1.2
Application Security	391.0	7.1	8.8	8.9	13.8	18.3	225.6	6.8	4.7	10.6	6.3	10.4	5.7
Business Continuity	146.0	4.0	3.0	2.1	6.5	6.6	83.0	2.3	2.1	3.5	0.7	3.9	2.0
Cyber Consultancy	22.4	0.3	0.5	0.5	0.7	1.0	12.8	0.4	0.4	0.6	0.3	0.6	0.3
Cyber Security Insurance	47.1	0.9	1.0	1.1	1.7	2.1	26.6	0.7	0.6	1.3	0.7	1.3	0.7
Encryption	22.5	0.3	0.5	0.5	0.7	1.0	12.6	0.3	0.6	0.6	0.3	0.6	0.3
Identity & Access	75.4	0.7	1.7	1.4	2.7	3.4	43.3	1.1	1.4	2.0	1.1	2.0	1.0
Infrastructure	345.1	11.5	7.7	7.3	14.3	16.4	192.5	4.6	3.8	9.8	5.0	9.6	4.4
Mobile	27.0	0.4	0.7	0.6	1.0	1.2	14.8	0.5	0.5	0.8	0.5	0.7	0.4
Outsourced/Managed Services	20.3	0.4	0.5	0.6	0.8	0.8	11.4	0.3	0.2	0.5	0.3	0.5	0.3
Situational Awareness	309.3	5.5	7.1	6.0	11.6	13.8	175.1	4.4	5.9	13.7	5.0	8.5	3.9
System Recovery & Data Cleansing	202.6	4.0	4.5	4.9	7.7	9.4	111.3	3.1	4.1	5.2	2.8	5.6	2.7
Training & Education	0.9	0.0	0.0	0.0	0.0	0.0	0.6	0.0	0.0	0.0	0.0	0.0	0.0
Total	1,696.5	36.2	37.9	36.0	64.2	76.1	988.5	25.4	26.1	45.2	24.2	46.2	22.9

Italy													
Level 2	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR
Anti Malware	1,809.0	2.8	39.6	56.8	80.2	125.6	835.0	39.4	90.4	55.7	15.8	48.1	27.8
Application Security	3,201.2	54.4	70.3	82.8	133.9	216.4	1,537.7	58.3	86.6	111.4	40.0	87.8	74.3
Business Continuity	1,682.7	39.9	40.2	51.6	49.6	120.0	791.6	43.2	26.7	50.3	16.7	46.6	30.2
Cyber Consultancy	227.6	3.3	4.7	5.8	7.2	15.1	111.6	5.0	8.7	7.5	1.9	6.2	4.9
Cyber Security Insurance	577.3	8.4	13.0	15.2	22.0	39.9	282.5	12.0	15.5	19.0	6.6	15.5	14.0
Encryption	216.5	2.0	4.8	5.5	8.5	15.7	103.6	4.3	5.3	7.3	2.7	6.1	5.5
Identity & Access	846.7	18.9	17.6	21.5	26.2	62.7	410.2	14.6	20.9	28.7	10.9	22.2	17.8
Infrastructure	4,887.0	57.7	104.1	118.8	145.2	299.2	2,437.9	164.0	118.5	137.9	57.7	132.3	117.6
Mobile	360.7	6.2	8.3	11.2	13.3	24.8	178.7	7.0	7.7	10.8	3.7	9.8	7.9
Outsourced/Managed Services	208.9	3.8	4.0	6.2	9.7	15.5	96.1	6.4	4.9	6.8	2.9	5.6	5.7
Situational Awareness	3,647.8	55.2	77.7	101.9	121.0	238.4	1,823.5	49.7	78.9	118.0	52.1	102.4	79.2
System Recovery & Data Cleansing	2,234.3	37.6	48.6	56.0	71.1	148.5	1,115.2	41.2	53.0	71.5	22.7	60.0	56.3
Training & Education	14.8	0.2	0.3	0.4	0.6	1.1	7.2	0.4	0.3	0.5	0.1	0.4	0.3
Total	19,914.5	290.4	433.2	533.7	688.5	1,322.9	9,726.8	445.4	517.4	625.4	233.8	543.0	441.5

Latvia																	
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level2																	
Anti Malware	48.9	0.9	1.1	1.2	1.5	3.2	26.4	1.1	2.0	1.6	0.6	1.5	0.8	1.6	0.1	1.5	1.3
Application Security	83.3	0.9	2.0	2.3	2.5	5.0	45.7	0.7	2.4	2.5	0.8	2.6	1.6	2.7	0.9	3.7	2.5
Business Continuity	39.9	0.7	1.0	1.0	1.2	2.6	20.7	0.9	1.1	1.2	0.3	1.2	0.8	1.4	0.4	1.7	1.0
Cyber Consiliency	3.5	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.0	0.1	0.1	0.1	0.0	0.1	0.1
Cyber Security Insurance	10.3	0.1	0.2	0.2	0.4	0.7	5.5	0.1	0.3	0.3	0.1	0.3	0.2	0.4	0.1	0.4	0.3
Encryption	3.3	0.0	0.1	0.1	0.1	0.2	1.8	0.0	0.1	0.1	0.0	0.1	0.1	0.1	0.0	0.1	0.1
Identity & Access Infrastructure	13.1	0.2	0.3	0.3	0.5	1.0	7.0	0.2	0.4	0.4	0.2	0.4	0.3	0.5	0.1	0.4	0.5
Mobile	71.0	0.6	1.5	1.4	2.6	4.1	38.6	1.5	2.4	2.2	0.6	2.1	1.5	2.6	0.4	2.4	1.9
Outsourced/Managed Services	5.9	0.1	0.1	0.1	0.1	0.4	3.1	0.1	0.2	0.2	0.1	0.2	0.1	0.2	0.0	0.2	0.2
Situational Awareness	2.8	0.0	0.1	0.1	0.1	0.1	1.6	0.0	0.0	0.1	0.0	0.1	0.0	0.1	0.0	0.1	0.1
System Recovery & Data Cleansing	60.3	0.7	1.4	1.4	2.2	3.9	32.5	0.7	1.9	1.9	0.7	1.9	1.1	2.1	0.5	2.1	2.2
Training & Education	42.0	0.5	1.0	1.1	1.6	2.8	22.5	0.6	1.0	1.4	0.5	1.3	0.8	1.5	0.2	1.5	1.1
Total	384.4	4.7	8.9	9.3	13.0	24.2	207.4	6.0	11.9	12.0	3.9	11.8	7.4	13.3	2.7	14.2	13.0
Lithuania																	
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level2																	
Anti Malware	9.0	0.1	0.2	0.1	0.2	0.6	5.0	0.1	0.1	0.2	0.1	0.4	0.2	0.3	0.2	0.3	0.2
Application Security	28.8	0.4	0.8	0.5	0.5	2.1	15.8	0.3	0.3	0.3	0.6	1.4	0.7	0.9	0.3	1.2	0.9
Business Continuity	19.0	0.3	0.5	0.4	0.4	1.8	9.7	0.2	0.3	0.4	0.3	1.0	0.4	0.6	0.3	0.8	0.4
Cyber Consiliency	6.6	0.1	0.2	0.1	0.1	0.5	3.6	0.1	0.1	0.1	0.1	0.3	0.1	0.2	0.1	0.3	0.2
Cyber Security Insurance	17.1	0.3	0.5	0.3	0.3	1.3	9.2	0.2	0.2	0.4	0.2	0.7	0.4	0.5	0.3	0.7	0.5
Encryption	6.8	0.1	0.2	0.1	0.1	0.4	3.7	0.1	0.1	0.1	0.1	0.3	0.1	0.2	0.2	0.3	0.2
Identity & Access Infrastructure	22.3	0.4	0.6	0.4	0.4	1.7	12.0	0.3	0.2	0.5	0.3	1.0	0.6	0.6	0.4	0.9	0.7
Mobile	42.0	1.1	1.1	0.8	0.7	3.4	22.3	0.4	0.7	0.9	0.5	2.0	0.9	1.3	0.5	1.8	1.3
Outsourced/Managed Services	8.0	0.2	0.2	0.1	0.1	0.6	4.3	0.1	0.1	0.2	0.1	0.3	0.2	0.2	0.1	0.3	0.1
Situational Awareness	6.6	0.2	0.2	0.1	0.1	0.5	3.3	0.1	0.1	0.1	0.1	0.3	0.1	0.2	0.2	0.2	0.1
System Recovery & Data Cleansing	83.5	1.4	2.3	1.5	1.5	6.1	45.0	0.8	1.1	1.9	1.1	3.8	1.9	2.6	1.5	3.8	2.7
Training & Education	66.4	1.6	1.8	1.3	1.2	5.3	34.5	1.0	0.8	1.5	0.9	3.1	1.3	1.9	1.4	2.9	2.1
Total	316.4	6.2	8.6	5.7	5.6	24.3	168.6	3.7	4.1	6.9	4.3	14.6	6.9	9.5	5.5	13.5	10.0
Luxembourg																	
	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level2																	
Anti Malware	32.6	0.4	1.1	0.6	1.3	1.6	17.0	0.7	0.2	0.6	0.6	0.7	0.9	1.4	0.1	1.1	1.7
Application Security	70.8	0.7	2.2	3.0	2.1	3.1	38.0	1.3	1.1	1.3	0.6	1.9	1.5	3.0	0.6	3.2	2.7
Business Continuity	27.5	0.4	0.9	1.0	0.8	1.1	13.9	0.3	0.2	0.5	0.3	0.8	0.8	1.8	0.3	1.2	1.4
Cyber Consiliency	4.7	0.1	0.1	0.1	0.1	0.2	2.5	0.0	0.0	0.1	0.0	0.1	0.1	0.2	0.0	0.1	0.2
Cyber Security Insurance	10.2	0.1	0.3	0.4	0.3	0.5	5.3	0.1	0.2	0.2	0.1	0.3	0.2	0.5	0.1	0.4	0.5
Encryption	4.9	0.1	0.1	0.2	0.1	0.2	2.7	0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.0	0.2	0.2
Identity & Access Infrastructure	17.0	0.2	0.5	0.8	0.5	0.7	8.8	0.2	0.3	0.3	0.2	0.5	0.4	0.8	0.3	0.7	0.8
Mobile	60.5	0.8	2.1	2.2	1.5	2.8	31.6	1.0	1.0	1.0	0.5	1.7	1.3	2.7	0.6	2.7	2.8
Outsourced/Managed Services	6.2	0.1	0.2	0.3	0.2	0.3	3.3	0.1	0.1	0.1	0.1	0.2	0.1	0.3	0.0	0.3	0.2
Situational Awareness	4.8	0.0	0.1	0.3	0.1	0.2	2.6	0.1	0.1	0.1	0.0	0.1	0.1	0.2	0.0	0.2	0.1
System Recovery & Data Cleansing	68.0	1.1	1.9	2.9	1.8	3.2	34.6	0.9	1.3	1.2	0.5	1.8	1.6	3.5	1.0	2.8	3.1
Training & Education	42.3	0.8	1.4	2.0	1.1	1.9	21.2	0.6	0.8	0.8	0.5	1.2	1.0	2.3	0.6	1.6	1.8
Total	349.6	4.8	10.9	13.8	9.9	15.8	181.6	5.4	5.4	6.3	3.6	9.6	8.1	16.9	3.6	14.5	15.7

Malta																																
	Chemicals & Pharma EUR		Commercial Facilities EUR		Communications EUR		Manufacturing Industries EUR		Defence Industries EUR		Public EUR		Construction EUR		Financial Services EUR		Food & Agriculture EUR		Other Utilities EUR		Government Facilities EUR		Healthcare Technology EUR		Education EUR		Transport & Logistics EUR		Water Utilities EUR		Emergency Services EUR	
	Total EUR	Level 2																														
	12.0	0.2	0.3	0.3	0.4	1.0	6.7	0.0	0.1	0.5	0.2	0.3	0.2	0.5	0.2	0.3	0.2	0.5	0.2	0.3	0.3	0.3	0.2	0.5	0.2	0.3	0.3	0.3	0.4	0.4		
	16.3	0.2	0.4	0.6	0.7	1.3	8.4	0.1	0.3	0.7	0.3	8.4	0.1	0.3	0.7	0.3	0.4	0.2	0.6	0.2	0.5	0.4	0.2	0.6	0.2	0.5	0.4	0.7	0.7	0.7		
	6.0	0.0	0.2	0.2	0.2	0.3	3.2	0.0	0.1	0.2	0.1	3.2	0.0	0.1	0.2	0.2	0.2	0.1	0.2	0.1	0.2	0.2	0.1	0.2	0.1	0.2	0.2	0.2	0.2	0.2		
	0.9	0.0	0.0	0.0	0.0	0.1	0.6	0.0	0.0	0.0	0.0	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		
	2.6	0.0	0.1	0.1	0.1	0.2	1.3	0.0	0.1	0.1	0.1	0.1	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1		
	1.1	0.0	0.0	0.0	0.0	0.0	0.1	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		
	4.3	0.1	0.1	0.2	0.2	0.3	2.2	0.0	0.0	0.2	0.2	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.2	0.2		
	21.7	0.2	0.6	0.8	0.8	1.8	10.7	0.1	0.1	1.1	0.5	0.6	0.5	0.6	0.9	0.7	0.7	0.6	0.8	0.7	0.7	0.6	0.8	0.7	0.7	0.6	0.8	0.7	0.7	0.8		
1.5	0.0	0.0	0.1	0.1	0.1	0.8	0.0	0.0	0.1	0.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1			
1.1	0.0	0.0	0.1	0.0	0.0	0.1	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0			
19.3	0.3	0.5	0.6	0.8	0.8	1.6	9.9	0.2	0.2	0.8	0.5	0.6	0.3	0.7	0.3	0.6	0.5	0.8	0.7	0.3	0.6	0.5	0.8	0.7	0.3	0.6	0.5	0.8	0.7	0.8		
10.8	0.1	0.3	0.4	0.4	0.9	5.5	0.1	0.1	0.4	0.1	0.4	0.2	0.3	0.2	0.4	0.2	0.4	0.2	0.4	0.2	0.4	0.3	0.4	0.2	0.4	0.2	0.4	0.3	0.4	0.4		
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		
97.6	1.1	2.5	3.4	3.7	7.9	50.5	0.5	0.9	4.1	2.1	2.6	1.6	3.7	1.9	2.9	2.5	3.7	2.5	2.9	2.5	3.7	1.6	3.7	1.9	2.9	2.5	3.7	2.5	3.7	3.7		
Netherlands																																
	Chemicals & Pharma EUR		Commercial Facilities EUR		Communications EUR		Manufacturing Industries EUR		Defence Industries EUR		Public EUR		Construction EUR		Financial Services EUR		Food & Agriculture EUR		Other Utilities EUR		Government Facilities EUR		Healthcare Technology EUR		Education EUR		Transport & Logistics EUR		Water Utilities EUR		Emergency Services EUR	
	Total EUR	Level 2																														
	691.3	14.3	14.7	25.0	12.1	46.4	334.4	31.0	3.7	27.5	6.8	32.7	7.3	35.3	21.6	20.7	63.9	13.9	50.9	38.3	70.0	20.7	20.7	63.9	13.9	50.9	38.3	70.0	20.7	20.7	63.9	
	1512.6	17.0	34.1	39.1	82.1	88.7	834.4	29.0	14.2	59.2	21.7	70.0	20.7	63.9	13.9	50.9	38.3	70.0	20.7	63.9	13.9	70.0	20.7	63.9	13.9	50.9	38.3	70.0	20.7	20.7	63.9	
	491.4	5.2	11.5	15.0	2.4	26.9	257.3	11.6	6.4	24.3	6.4	24.3	6.4	24.3	6.5	22.0	5.4	17.3	13.5	8.2	24.3	6.5	24.3	6.5	22.0	5.4	17.3	13.5	8.2	24.3	8.2	
	76.5	0.8	1.7	2.1	1.4	4.5	40.8	1.7	0.9	2.9	0.9	2.9	0.9	3.7	1.1	1.1	3.6	1.0	2.7	2.1	3.7	1.1	3.7	1.1	3.6	1.0	2.7	2.1	2.1	1.4	1.4	
	170.6	2.2	3.8	4.4	7.2	11.6	89.0	3.4	1.8	7.2	1.8	7.2	1.8	8.0	2.3	9.2	2.0	6.6	4.6	3.2	8.0	2.3	8.0	2.3	9.2	2.0	6.6	4.6	3.2	8.0	3.2	
	71.7	1.3	1.6	2.1	1.3	4.6	38.2	1.0	0.9	2.6	0.9	2.6	0.9	3.2	0.9	3.6	1.4	2.2	1.9	1.3	3.2	0.9	3.2	0.9	3.6	1.4	2.2	1.9	1.3	1.3		
	290.4	3.5	6.3	8.3	5.3	18.9	155.1	5.2	2.5	12.1	2.6	12.1	2.6	13.6	4.2	13.9	4.6	9.5	7.9	5.3	13.6	4.2	13.6	4.2	13.9	4.6	9.5	7.9	5.3	7.9	5.3	
	1266.7	17.7	27.0	28.5	21.8	85.6	706.8	27.5	8.2	47.4	8.4	51.7	14.7	57.2	17.7	37.9	33.6	21.8	51.7	14.7	51.7	14.7	51.7	14.7	37.9	33.6	21.8	51.7	14.7	37.9	33.6	
113.6	1.1	2.7	3.2	2.1	7.6	60.0	2.5	1.2	5.4	1.1	4.8	1.5	5.3	1.5	4.3	2.9	2.1	4.8	1.5	4.8	1.5	4.8	1.5	5.3	1.5	4.3	2.9	2.1	2.1	2.1		
75.8	0.8	1.6	1.7	1.3	4.8	41.5	0.9	1.0	3.2	0.7	3.3	1.2	3.3	1.2	3.1	1.5	2.6	2.1	1.3	3.3	1.2	3.3	1.2	3.1	1.5	2.6	2.1	1.3	1.3	1.3		
1009.6	15.3	23.1	27.7	18.0	65.0	537.1	14.8	10.3	40.9	9.7	49.1	10.3	40.9	9.7	47.9	15.7	35.3	27.8	18.0	49.1	10.3	47.9	15.7	35.3	27.8	18.0	47.9	15.7	35.3	27.8		
711.6	8.2	15.9	19.8	12.6	44.8	380.8	13.6	6.2	27.9	7.7	34.2	10.5	37.0	7.2	37.0	7.2	25.0	18.9	12.6	34.2	10.5	37.0	7.2	37.0	7.2	25.0	18.9	12.6	18.9	12.6		
4.8	0.1	0.1	0.1	0.1	0.1	0.3	2.6	0.1	0.1	0.2	0.0	0.2	0.1	0.2	0.1	0.2	0.1	0.1	0.1	0.2	0.0	0.2	0.1	0.2	0.1	0.2	0.1	0.1	0.1	0.1		
6486.6	87.5	144.1	177.0	114.8	409.7	3478.0	142.3	57.4	260.8	68.7	298.8	83.8	302.2	93.6	218.1	170.8	114.8	298.8	83.8	68.7	298.8	83.8	302.2	93.6	218.1	170.8	114.8	218.1	170.8	114.8		
Poland																																
	Chemicals & Pharma EUR		Commercial Facilities EUR		Communications EUR		Manufacturing Industries EUR		Defence Industries EUR		Public EUR		Construction EUR		Financial Services EUR		Food & Agriculture EUR		Other Utilities EUR		Government Facilities EUR		Healthcare Technology EUR		Education EUR		Transport & Logistics EUR		Water Utilities EUR		Emergency Services EUR	
	Total EUR	Level 2																														
	98.0	2.1	4.0	3.2	1.6	7.9	49.4	1.0	1.4	4.4	0.5	4.4	1.6	3.9	1.0	2.3	3.8	4.4	0.5	4.4	1.6	4.4	1.6	3.9	1.0	2.3	3.8	4.4	1.6	1.6		
	306.6	4.7	10.7	8.1	5.6	25.5	148.0	4.3	10.3	11.7	4.6	12.4	4.0	11.8	5.8	7.0	13.6	11.7	4.6	12.4	4.0	12.4	4.0	11.8	5.8	7.0	13.6	11.8	5.8	5.6		
	195.0	5.4	7.1	6.1	3.5	19.0	92.0	1.6	3.5	7.7	3.3	8.0	2.8	7.2	3.4	4.3	9.1	7.7	3.3	8.0	2.8	8.0	2.8	7.2	3.4	4.3	9.1	3.1	3.5	3.5		
	58.5	1.1	1.9	1.7	1.1	5.4	26.7	0.8	2.4	2.5	1.0	2.2	0.9	2.4	0.9	1.3	3.0	2.5	1.0	2.2	0.9	2.2	0.9	2.4	0.9	1.3	3.0	1.1	1.1	1.1		
	168.2	3.0	6.1	6.0	3.0	15.1	77.9	2.6	4.7	6.7	3.6	6.7	2.1	7.5	3.0	3.8	6.9	6.7	3.6	6.7	2.1	6.7	2.1	7.5	3.0	3.8	6.9	3.0	3.0	3.0		
	52.5	0.8	1.8	1.5	0.9	5.4	24.8	0.9	1.0	2.0	0.5	2.3	0.7	2.1	1.4	1.2	2.3	2.0	0.5	2.3	0.7	2.3	0.7	2.1	1.4	1.2	2.3	0.9	0.9	0.9		
	181.7	3.1	6.2	6.3	3.3	15.2	86.1	2.2	6.4	7.6	3.4	7.2	2.3	7.1	2.6	4.1	8.5	7.6	3.4	7.2	2.3	7.2	2.3	7.1	2.6	4.1	8.5	3.3	3.3	3.3		
	346.0	6.4	12.5	10.4	6.1	29.6	161.4	7.1	11.6	14.8	5.5	14.6	4.4	14.9	4.2	7.8	16.6	14.8	5.5	14.6	4.4	14.6	4.4	14.9	4.2	7.8	16.6	6.1	6.1	6.1		
55.3	0.7	1.9	1.7	1.0	5.5	24.7	0.9	2.0	2.5	0.9	2.2	0.8	2.6	0.9	1.3	2.6	1.0	2.2	0.8	2.2	0.8	2.2	0.8	2.6	0.9	1.3	2.6	1.0	1.0			
836.2	13.4	29.5	26.9	15.3	77.4	398.8	13.2	21.4	33.0	10.9	35.0	11.1	34.5	14.2	19.3	35.2	33.0	10.9	35.0	11.1	35.0	11.1	34.5	14.2	19.3	35.2	15.3	15.3	15.3			
687.1	15.3	25.0	20.2	12.4	61.3	316.0	12.1	24.9	30.4	10.0	28.1	9.5	28.7	9.9	15.4	30.3	24.9	30.4	10.0	28.1	9.5	28.1	9.5	28.7	9.9	15.4	30.3	12.4	12.4			
3.9	0.1	0.1	0.1	0.1	0.4	1.8	0.1	0.1	0.1	0.1	0.1	0.2	0.0	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.2	0.0	0.1	0.1	0.1	0.2	0.1	0.1	0.1			
3040.3	56.8	108.7	93.6	54.9	272.2	1430.0	48.0	92.5	125.5	45.7	125.6	40.8	125.0	48.1	69.1	134.4	54.9	125.6	45.7	125.6	40.8	69.1	40.8	125.0	48.1	69.1	134.4	54.9	54.9	54.9		

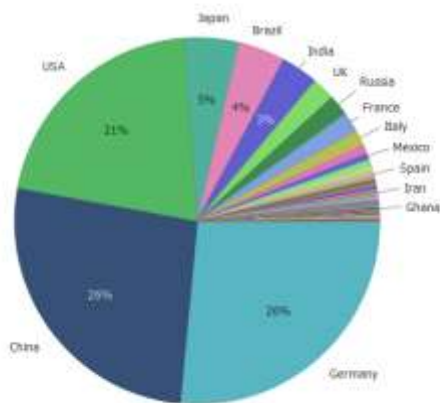
Portugal														
Level 2	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Information Technology EUR
Anti Malware	41.4	0.3	0.7	1.0	1.5	1.9	22.4	0.7	0.6	0.8	1.3	1.1	1.4	0.5
Application Security	109.4	1.1	2.0	3.2	3.5	4.5	60.8	2.6	1.0	5.1	3.1	1.6	3.8	1.5
Business Continuity	80.3	0.8	1.4	2.2	3.0	3.4	45.0	1.9	0.7	2.7	2.7	1.4	2.9	1.2
Cyber Consultancy	24.2	0.3	0.4	0.7	0.9	0.9	13.5	0.3	0.2	0.8	0.5	0.8	0.3	0.3
Cyber Security Insurance	66.5	0.7	1.2	1.8	2.9	2.9	36.6	1.3	0.6	2.1	1.3	2.5	0.9	3.2
Encryption	19.7	0.2	0.4	0.5	0.8	0.8	11.2	0.4	0.2	0.6	0.3	0.7	0.3	1.0
Identity & Access	72.0	0.7	1.3	1.7	3.3	3.2	40.4	1.4	0.7	1.9	0.8	2.9	1.0	3.6
Infrastructure	139.2	1.8	2.7	3.5	5.3	6.2	76.5	4.3	1.0	4.6	1.8	5.2	1.9	6.6
Mobile	27.8	0.4	0.5	0.8	1.2	1.4	15.3	0.6	0.3	0.8	0.2	1.0	0.3	1.3
Outsourced/Managed Services	19.5	0.3	0.3	0.5	0.7	0.7	11.3	0.2	0.2	0.5	0.2	0.8	0.2	0.8
Situational Awareness	316.9	3.7	5.8	8.9	12.6	13.7	175.4	6.9	3.1	10.4	5.0	11.4	4.6	15.7
System Recovery & Data Cleansing	261.7	2.6	4.7	7.0	11.0	11.4	145.5	6.3	3.0	7.9	4.4	9.3	3.3	12.3
Training & Education	1.8	0.0	0.0	0.0	0.0	0.1	1.1	0.0	0.0	0.0	0.0	0.1	0.0	0.1
Total	1,180.4	12.9	21.4	31.8	47.8	52.0	655.0	26.8	11.6	37.1	18.9	42.8	16.0	57.7
Romania														
Level 2	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Information Technology EUR
Anti Malware	40.8	0.6	0.8	0.7	1.4	1.7	22.6	0.4	0.7	0.7	1.3	0.3	2.2	0.9
Application Security	105.1	1.3	1.9	3.0	3.0	4.0	53.7	0.7	2.6	3.1	1.6	5.0	2.6	5.6
Business Continuity	73.6	0.4	1.3	1.3	3.0	3.0	38.4	0.7	2.7	3.1	2.1	3.5	1.6	3.1
Cyber Consultancy	21.9	0.2	0.4	0.3	0.9	0.9	11.3	0.1	0.7	0.7	0.3	1.0	0.5	1.2
Cyber Security Insurance	65.1	0.6	1.2	1.2	2.4	2.7	34.2	0.5	1.5	1.7	0.9	3.0	1.5	3.3
Encryption	19.3	0.1	0.4	0.3	0.8	0.8	9.7	0.2	1.1	0.5	0.3	0.9	0.4	0.9
Identity & Access	65.1	1.2	1.1	1.1	2.7	2.7	33.3	0.5	2.4	2.7	1.0	3.0	1.5	3.5
Infrastructure	139.9	1.3	2.5	2.5	6.0	5.7	74.5	1.1	4.3	3.6	1.9	6.6	3.3	5.6
Mobile	20.4	0.1	0.4	0.5	0.8	0.8	10.5	0.2	0.6	0.6	0.2	1.0	0.5	1.1
Outsourced/Managed Services	19.7	0.2	0.3	0.4	0.7	0.7	10.1	0.1	0.9	0.5	0.2	0.9	0.5	1.2
Situational Awareness	303.9	2.6	5.5	5.0	12.9	12.7	160.1	2.5	8.7	9.0	3.7	13.6	6.5	15.6
System Recovery & Data Cleansing	263.9	2.3	4.7	5.5	11.9	10.9	139.6	2.7	7.5	10.9	6.8	2.6	11.8	6.3
Training & Education	1.4	0.0	0.0	0.0	0.0	0.0	0.7	0.0	0.0	0.0	0.0	0.1	0.0	0.1
Total	1,140.1	10.4	20.6	20.7	47.5	46.8	597.7	9.7	33.7	31.6	13.9	52.6	26.1	55.5
Slovakia														
Level 2	Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communi- cations EUR	Manufacturing Industries EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare Technology EUR	Information Technology EUR
Anti Malware	136.5	1.6	3.6	5.2	2.8	2.8	67.6	1.1	2.7	2.5	4.8	1.1	5.1	3.0
Application Security	232.8	1.2	6.3	11.2	9.1	4.1	153.3	6.2	3.4	9.1	2.9	8.0	3.6	4.2
Business Continuity	102.2	0.7	2.4	3.6	1.9	1.9	56.5	1.3	1.2	4.5	1.4	4.0	1.9	2.0
Cyber Consultancy	11.2	0.1	0.3	0.4	0.2	0.2	5.8	0.2	0.2	0.5	0.1	0.4	0.2	0.4
Cyber Security Insurance	29.3	0.5	0.8	1.0	1.2	0.5	22.2	0.7	0.5	1.2	0.3	1.1	0.5	0.5
Encryption	9.7	0.2	0.2	0.3	0.2	0.2	5.1	0.2	0.1	0.4	0.1	0.3	0.2	0.2
Identity & Access	35.9	0.5	1.0	1.1	0.7	0.7	3.0	0.8	0.6	1.6	0.6	1.3	0.7	0.7
Infrastructure	188.7	3.2	5.3	7.1	3.5	3.5	99.1	3.2	1.8	7.6	2.0	7.1	2.7	3.4
Mobile	13.9	0.1	0.4	0.5	1.3	0.2	1.1	7.4	0.2	0.2	0.2	0.5	0.2	0.2
Outsourced/Managed Services	9.2	0.1	0.3	0.3	0.1	0.1	0.6	0.4	0.1	0.4	0.2	0.3	0.2	0.1
Situational Awareness	212.0	3.0	6.0	7.9	3.8	3.8	151.1	4.3	3.9	8.0	2.1	7.2	3.9	3.9
System Recovery & Data Cleansing	127.3	1.9	3.3	4.7	2.3	2.3	66.6	2.0	2.3	5.1	2.0	4.7	2.3	2.3
Training & Education	0.5	0.0	0.0	0.0	0.0	0.0	0.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total	1,109.2	13.1	29.9	43.3	20.3	81.4	575.7	22.0	16.8	43.8	13.5	40.0	19.4	20.3

UK		Total EUR	Chemicals & Pharma EUR	Commercial Facilities EUR	Communications EUR	Manufacturing EUR	Defence Industries EUR	Public EUR	Construction EUR	Financial Services EUR	Food & Agriculture EUR	Other Utilities EUR	Government Facilities EUR	Healthcare EUR	Information Technology EUR	Education EUR	Transport & Logistics EUR	Water Utilities EUR	Emergency Services EUR
Level 2		1,274.6	14.0	36.8	29.3	31.3	80.2	699.3	19.7	24.4	30.5	15.9	49.3	20.0	41.7	13.8	36.3	50.2	31.3
Anti Malware		3,849.6	60.0	118.9	93.4	103.2	273.3	2,038.3	60.6	95.6	96.8	52.0	140.7	63.1	121.1	41.6	109.9	156.3	103.2
Application Security		2,249.0	38.0	69.5	95.8	58.0	152.6	1,204.9	35.8	46.0	56.5	29.0	86.7	37.8	69.2	22.1	63.3	88.1	58.0
Business Continuity		657.5	9.1	20.6	17.6	16.4	44.3	354.4	9.3	15.1	16.3	7.8	24.5	10.8	20.9	5.7	19.2	25.9	16.4
Cyber Consultancy		618.0	9.2	18.5	14.8	16.2	41.9	332.2	9.3	13.4	15.1	8.2	23.6	10.0	20.1	6.2	17.1	25.5	16.2
Cyber Security Insurance		725.0	12.5	20.7	18.8	19.0	47.6	388.7	12.3	15.9	17.7	9.2	28.0	11.6	23.0	7.6	19.8	30.0	19.0
Encryption		2,496.9	34.3	74.6	64.1	64.7	169.9	1,329.2	40.5	59.8	61.1	30.4	96.5	40.3	81.5	27.1	68.2	105.6	64.7
Identity & Access		4,917.8	74.6	149.7	129.8	125.6	342.2	2,602.3	79.7	116.7	121.7	63.2	188.6	83.7	158.5	49.4	139.2	200.5	125.6
Infrastructure		516.5	7.1	16.7	13.0	13.2	35.6	274.4	8.7	9.5	12.6	6.3	19.3	8.8	17.2	6.5	15.0	21.0	13.2
Mobile		719.3	9.9	22.6	18.6	17.9	51.4	376.1	12.2	18.7	17.5	10.6	28.3	11.8	24.8	6.0	19.9	31.7	17.9
Outsourced/Managed Services		7,693.6	113.2	239.7	197.3	191.5	524.0	4,119.0	125.6	167.8	185.9	101.0	285.1	129.3	254.1	76.0	212.6	315.0	191.5
Situational Awareness		6,221.7	102.1	187.8	155.1	158.8	436.2	3,327.8	94.7	132.5	154.8	82.0	235.2	99.9	202.0	57.7	167.5	252.3	158.8
System Recovery & Data Cleansing		18.0	0.2	0.6	0.4	0.5	1.2	9.7	0.3	0.3	0.4	0.2	0.7	0.3	0.6	0.2	0.5	0.7	0.5
Training & Education																			
Total		31,957.5	484.2	976.7	812.0	816.3	2,200.4	17,056.3	508.7	715.7	786.9	415.8	1,206.5	527.4	1,034.7	319.9	888.5	1,302.8	816.3

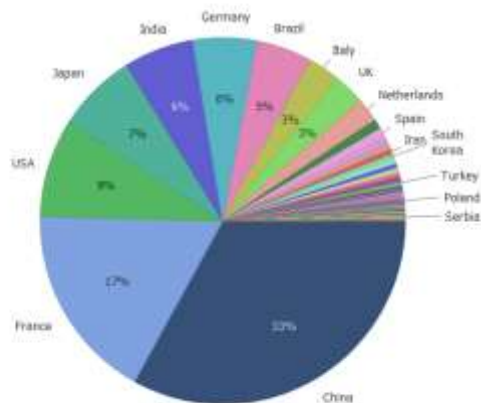
Appendix C : Imports by Country of Origin per EU Member State

Imports of each Member State for the year 2016 showing country of origin of the imports.

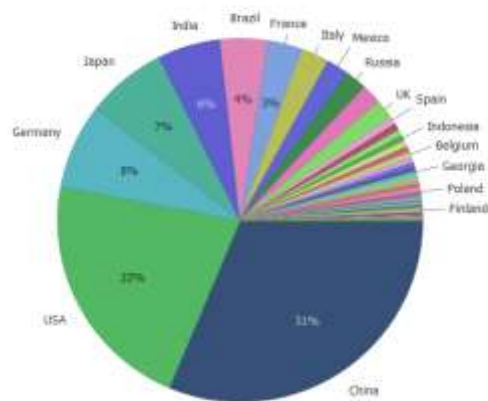
Austria



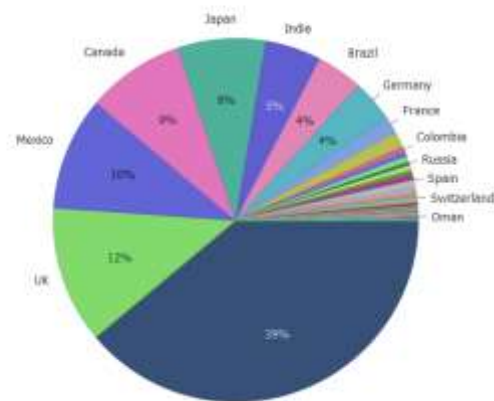
Belgium



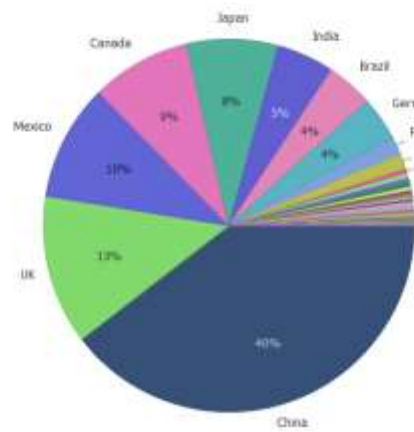
Bulgaria



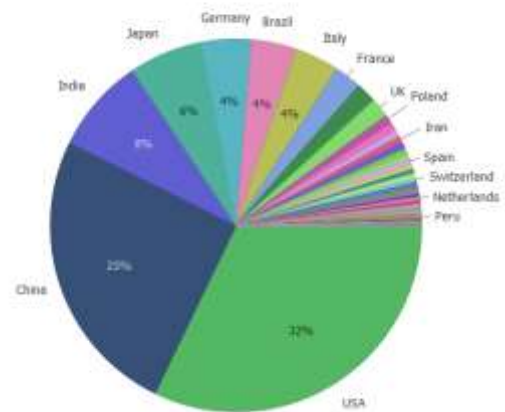
Croatia



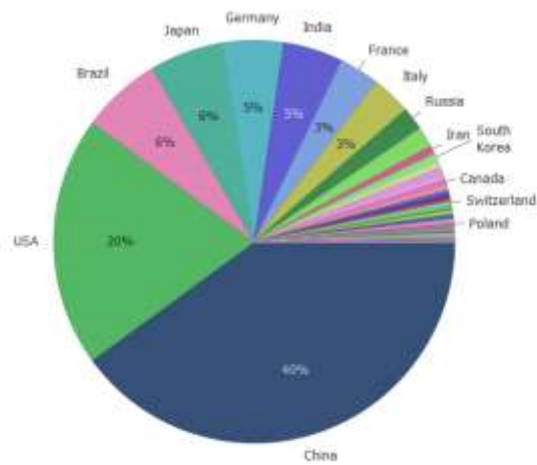
Cyprus



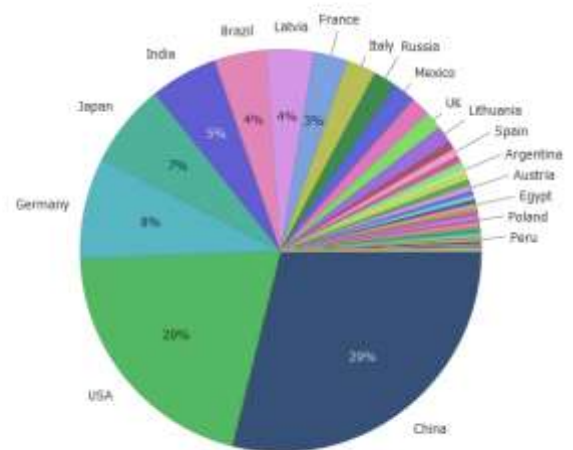
Czech Republic



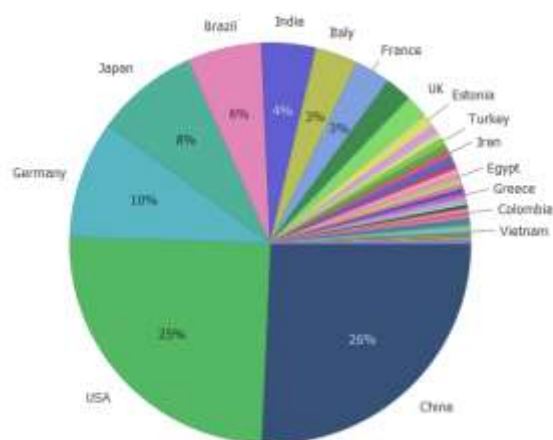
Denmark



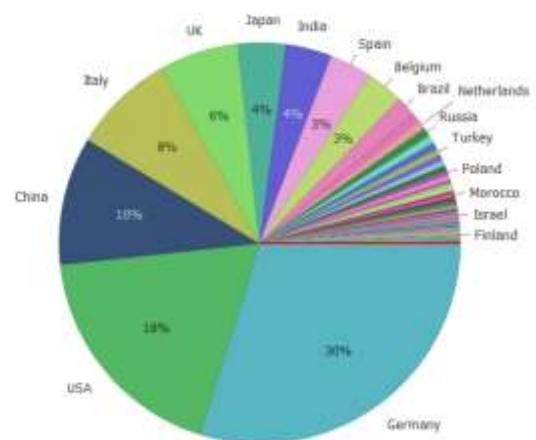
Estonia



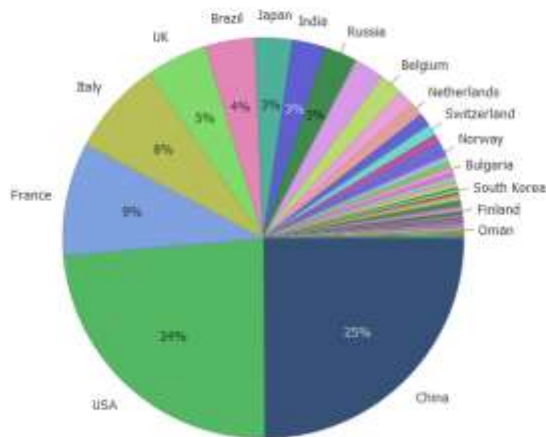
Finland



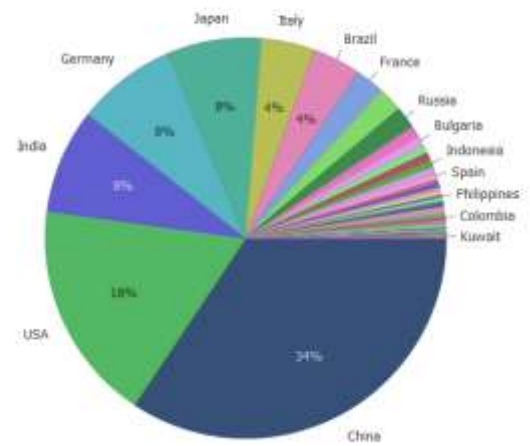
France



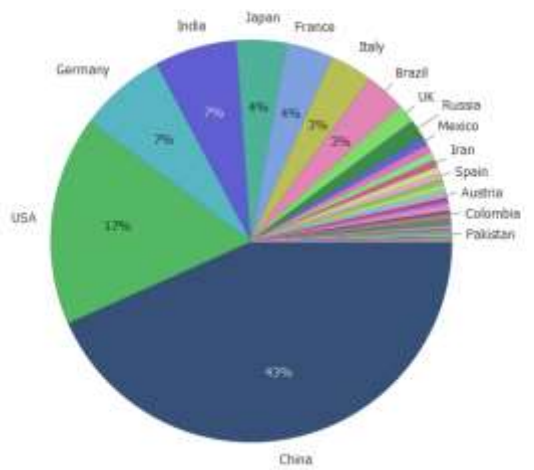
Germany



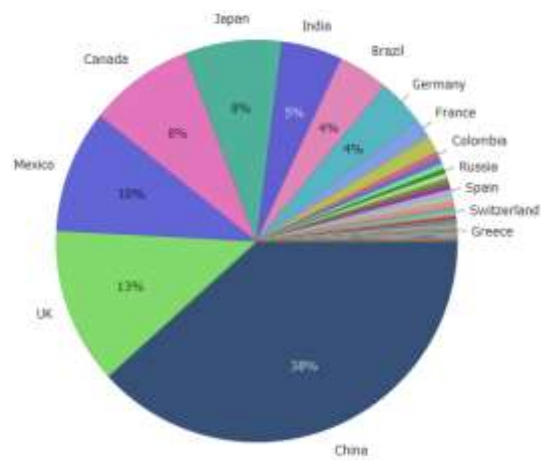
Greece



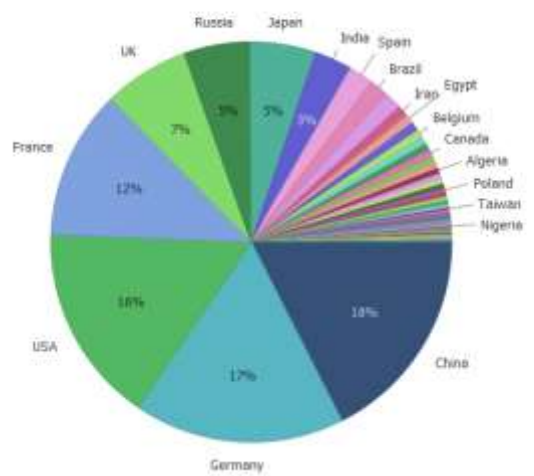
Hungary



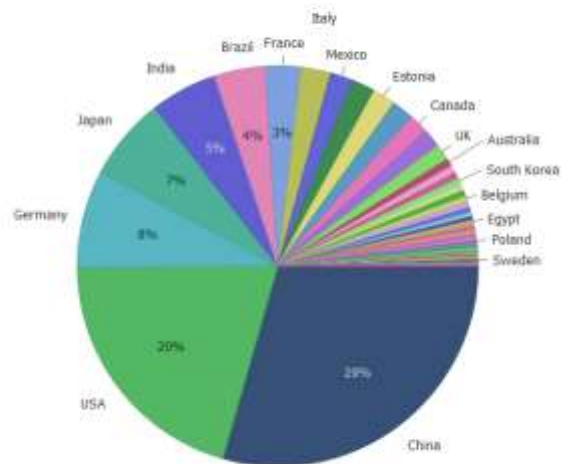
Ireland



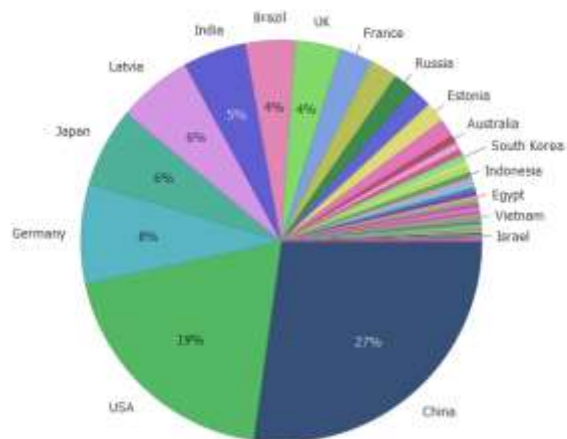
Italy



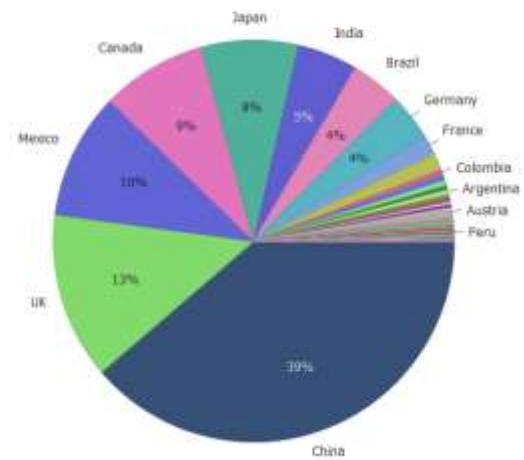
Latvia



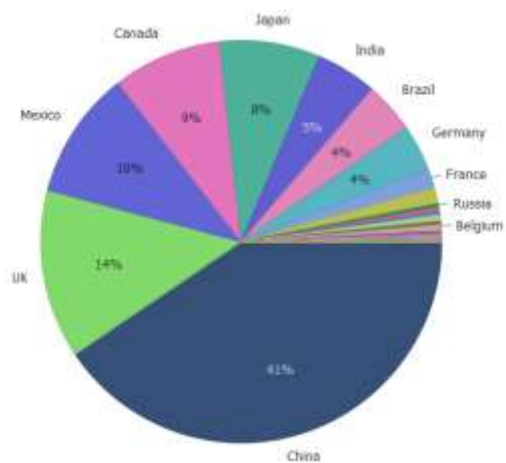
Lithuania



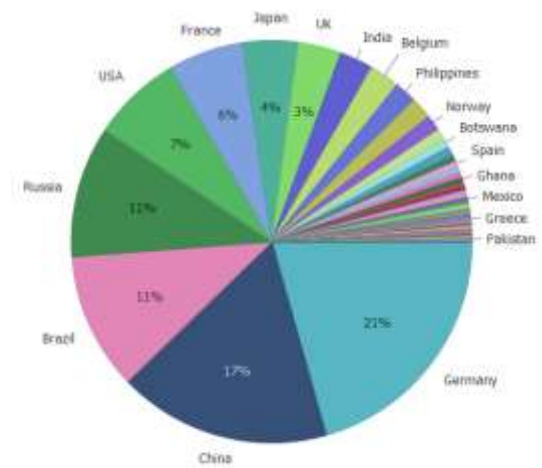
Luxembourg



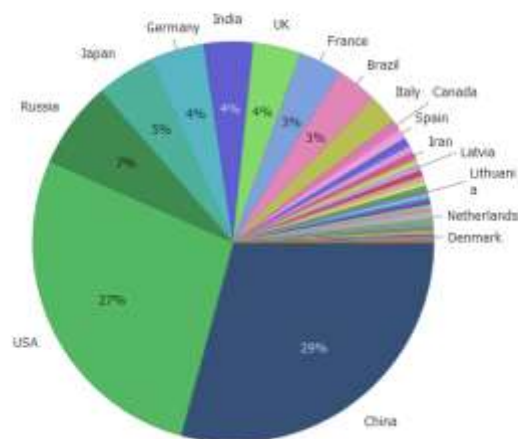
Malta



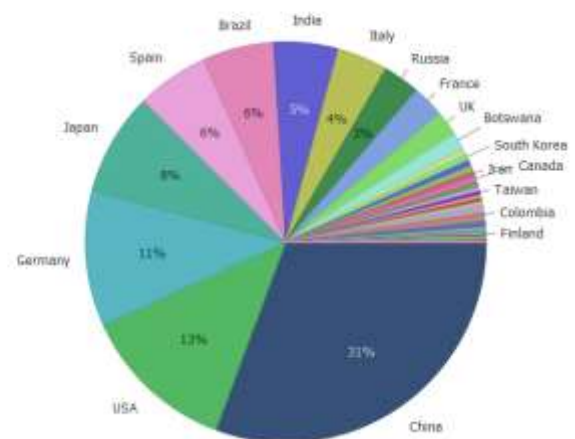
Netherlands



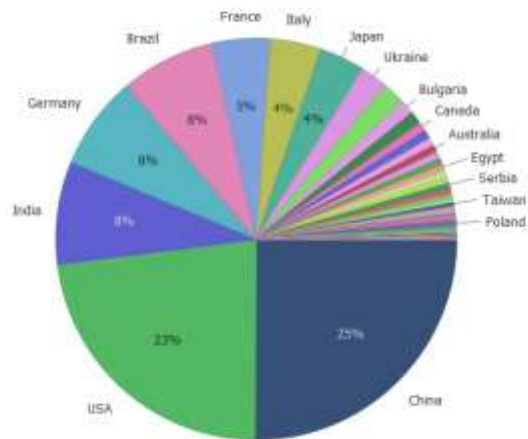
Poland



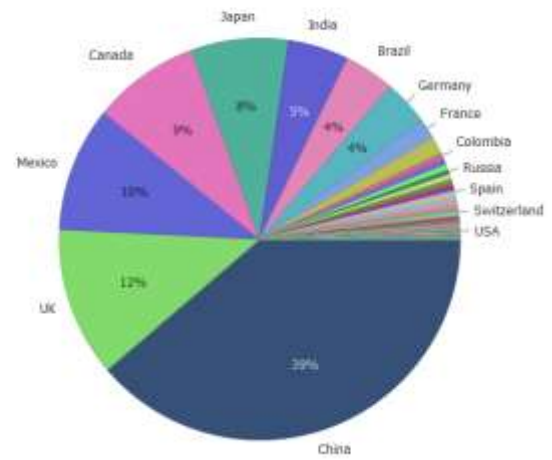
Portugal



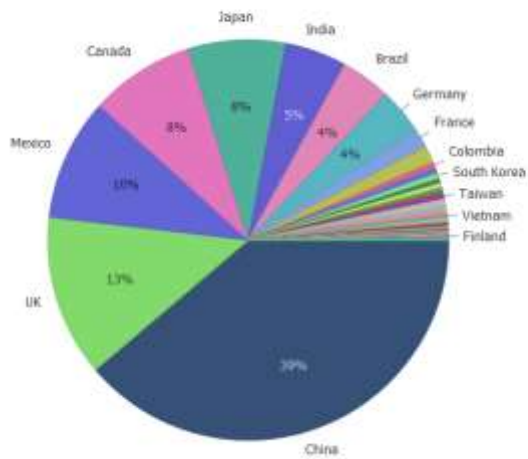
Romania



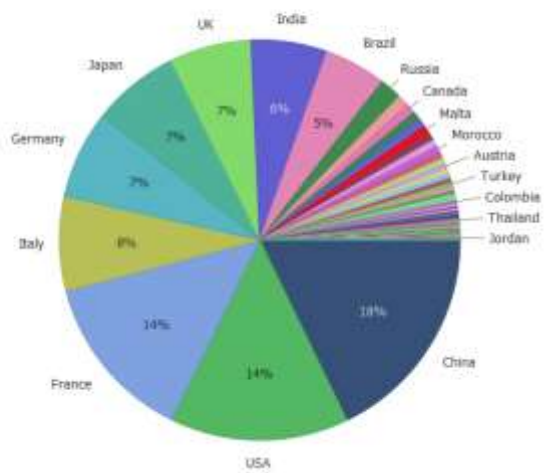
Slovakia



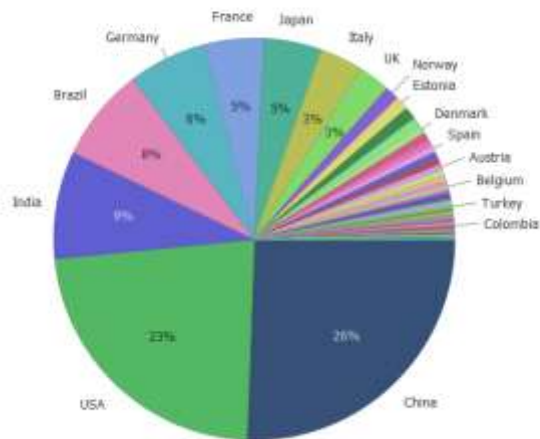
Slovenia



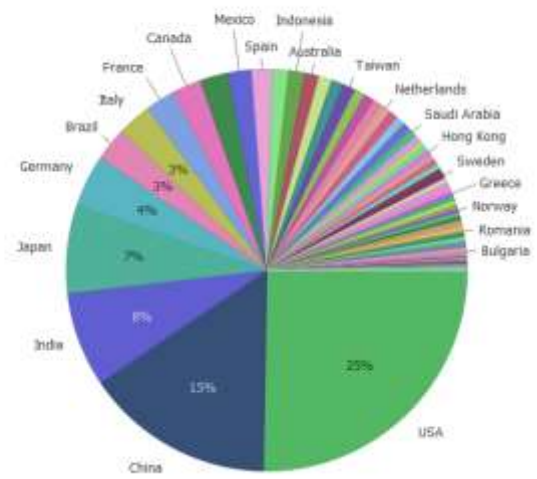
Spain



Sweden

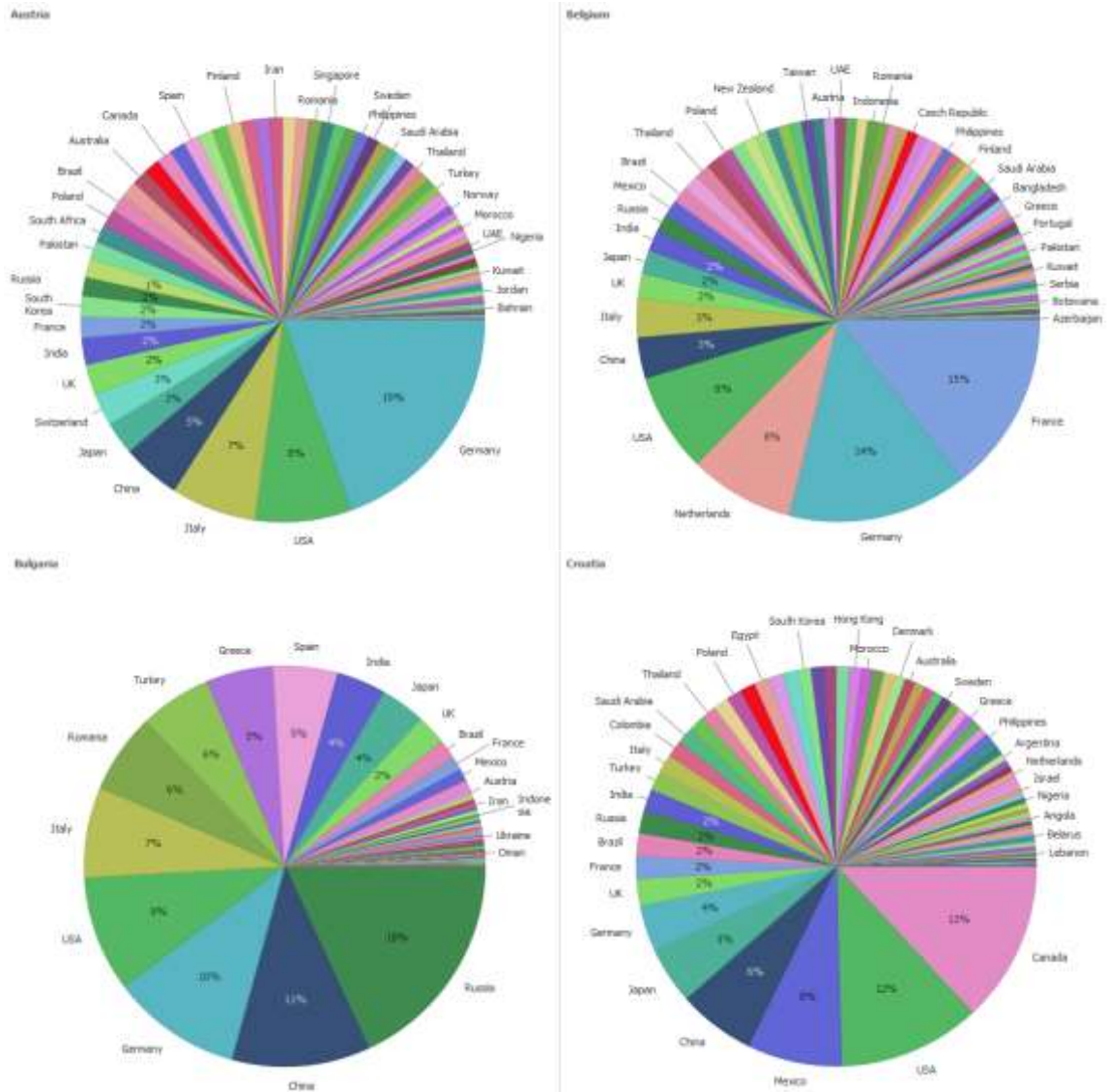


UK

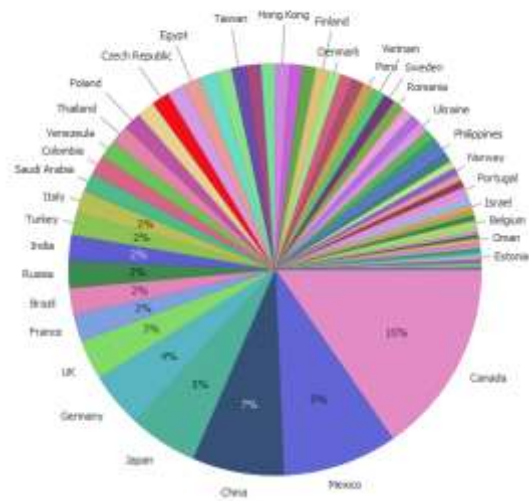


Appendix D : Exports by Country of Origin per EU Member State

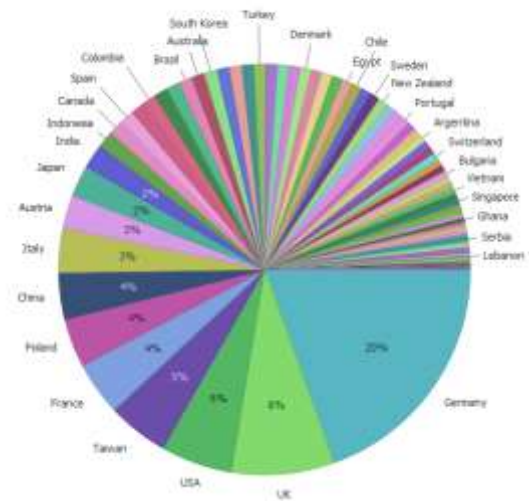
Exports from each Member State for the year 2016 showing destination of the exports.



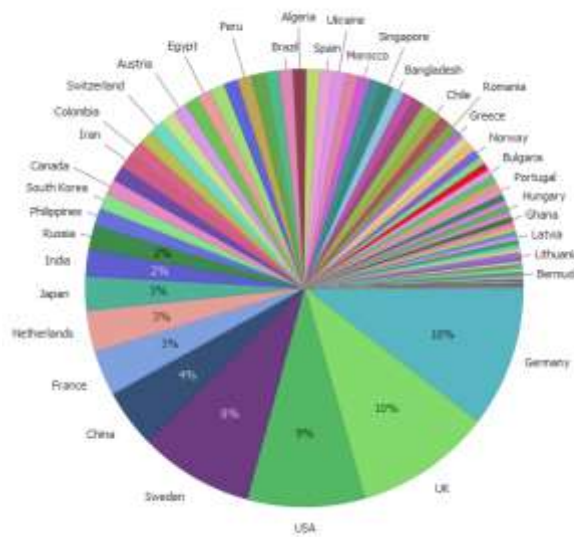
Cyprus



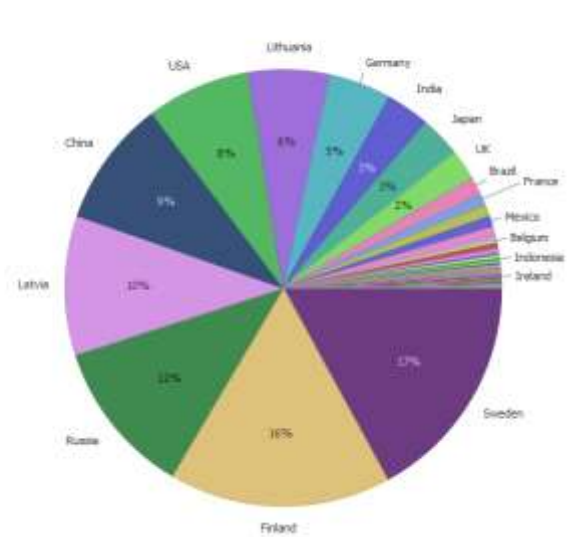
Czech Republic



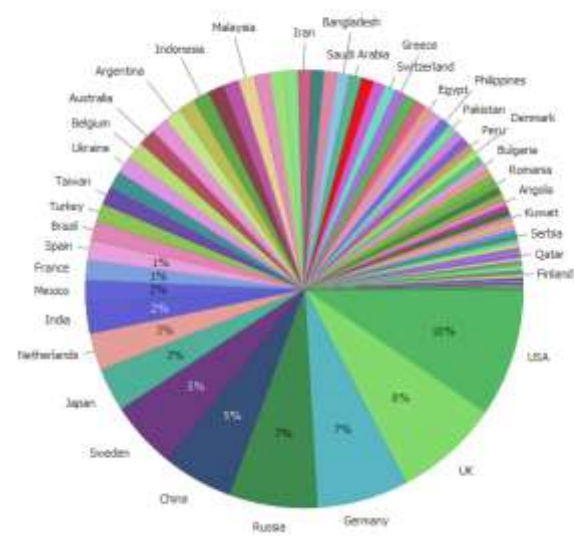
Denmark



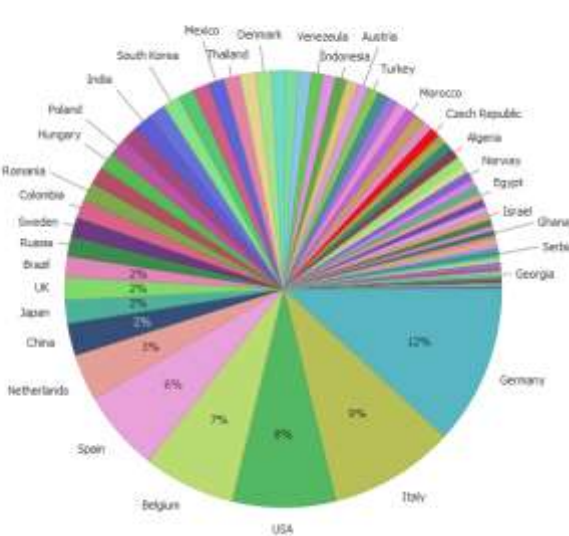
Estonia



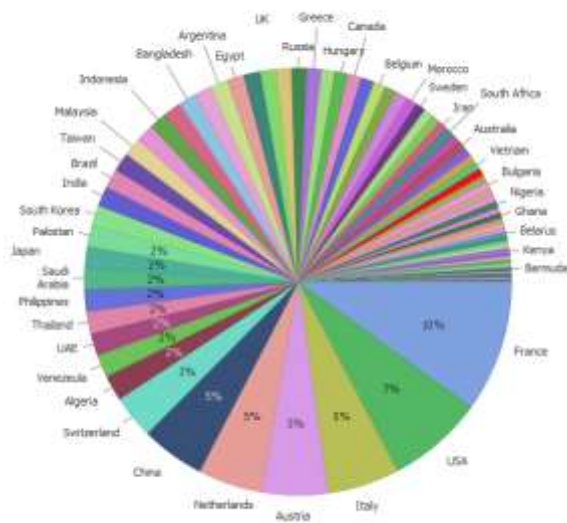
Finland



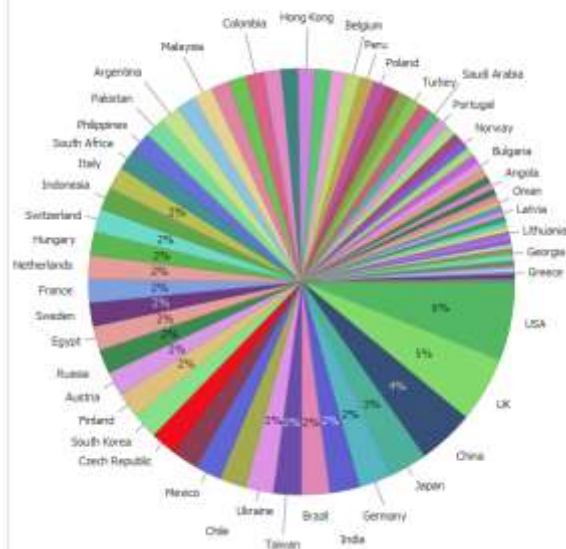
France



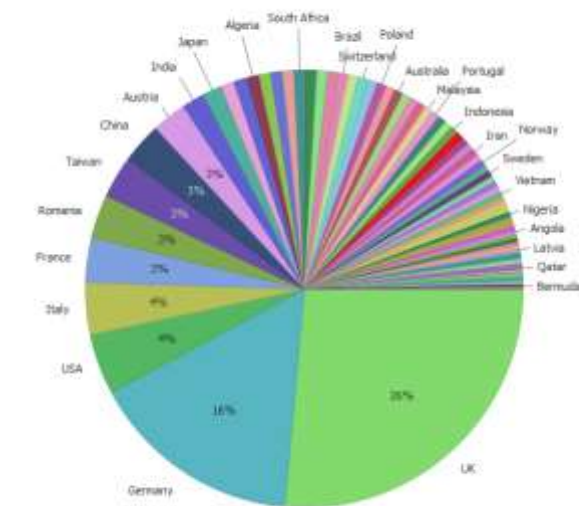
Germany



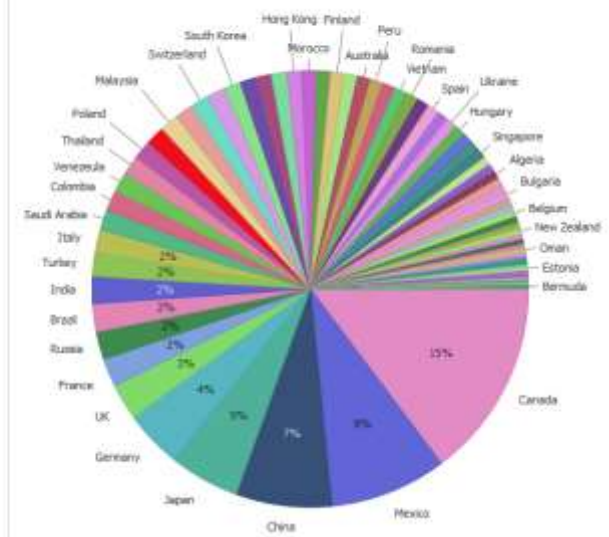
Greece



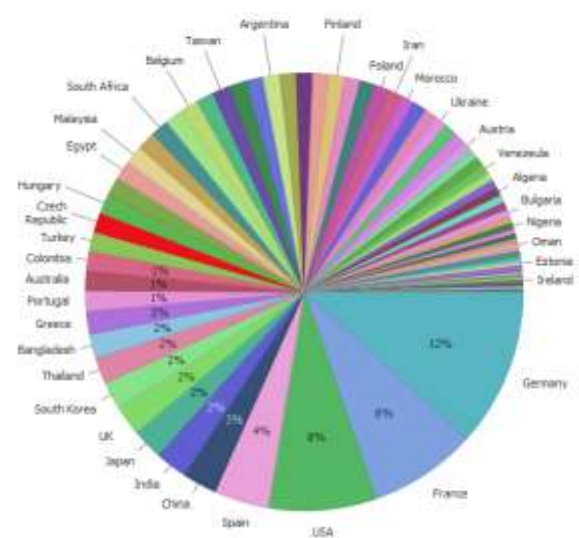
Hungary



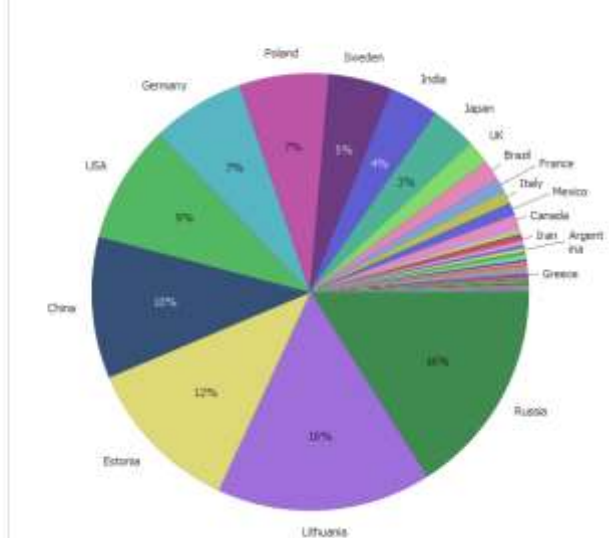
Ireland



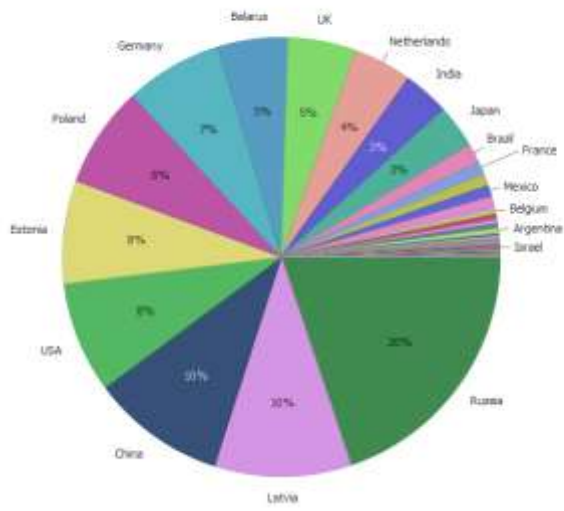
Italy



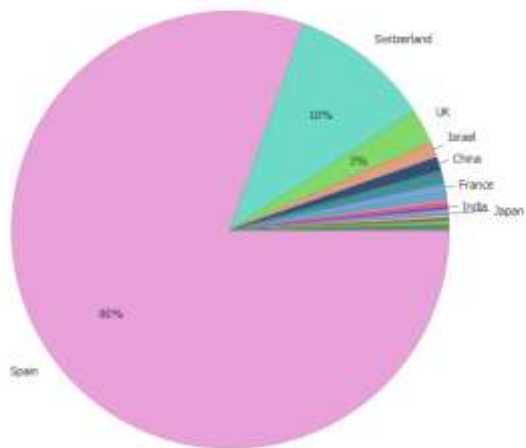
Lithuania



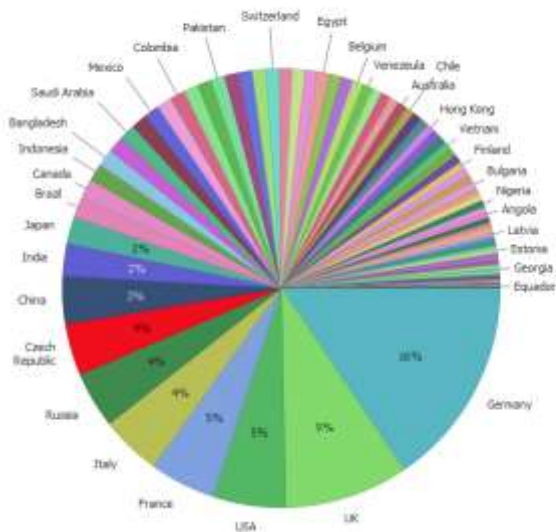
Lithuania



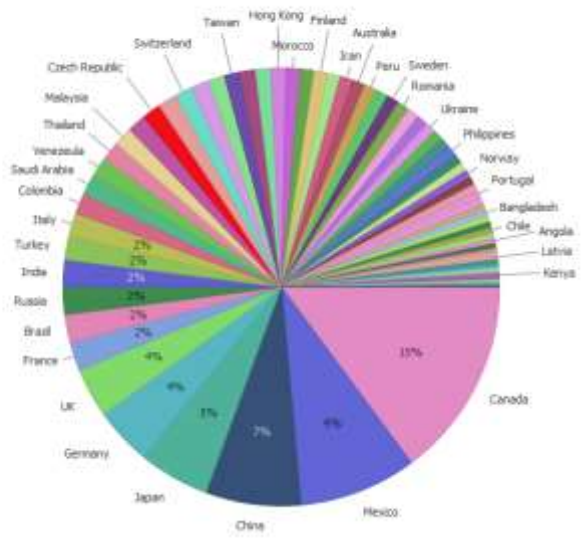
Haiti



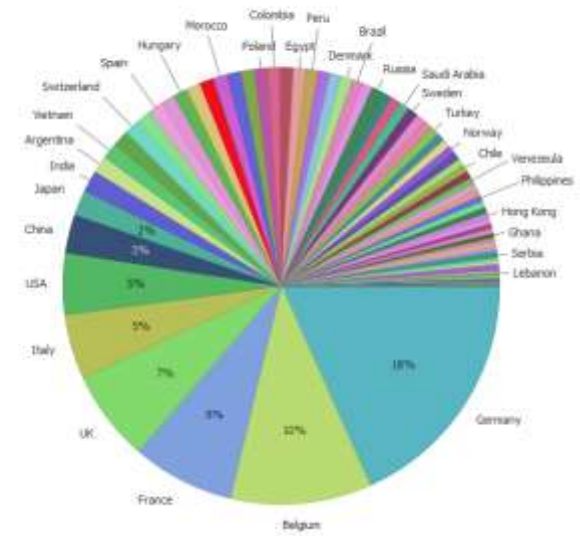
Poland



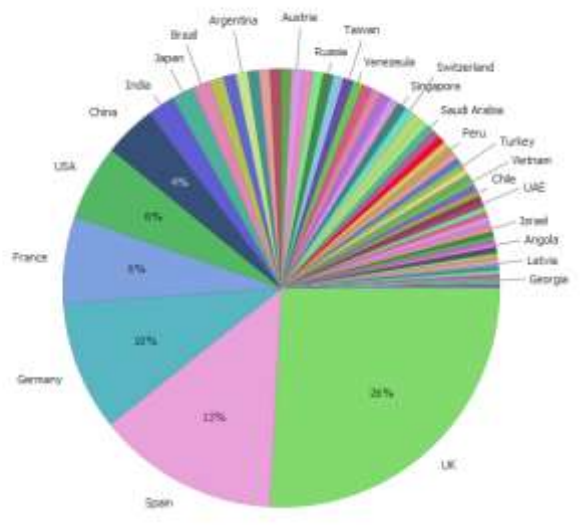
Luxembourg



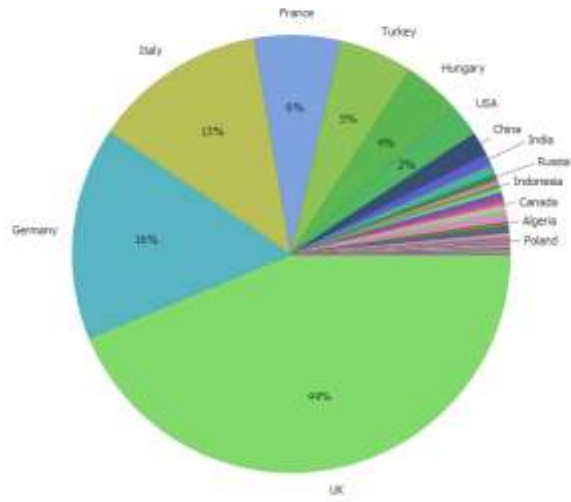
Netherlands



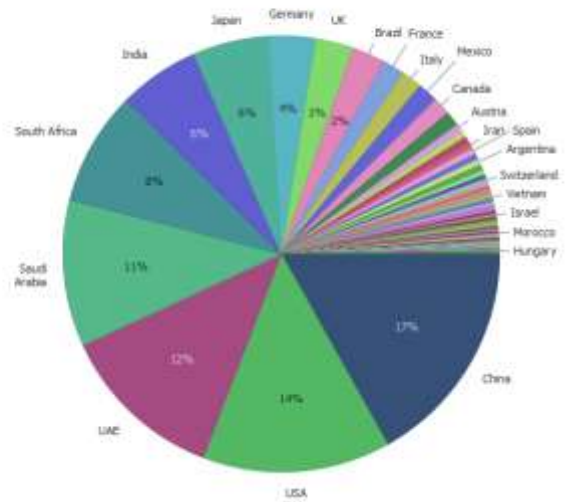
Portugal



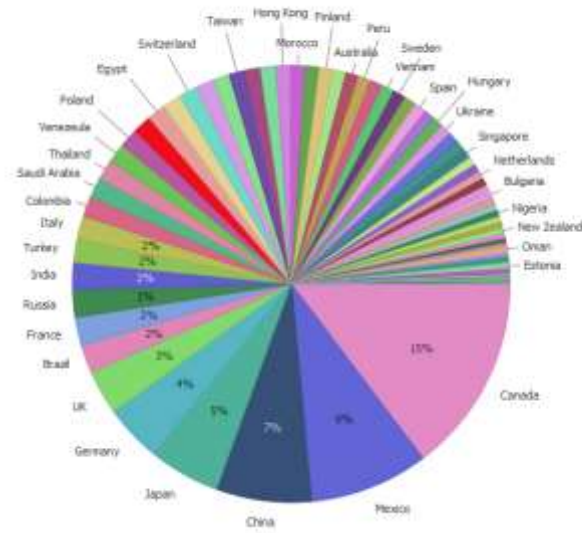
Romania



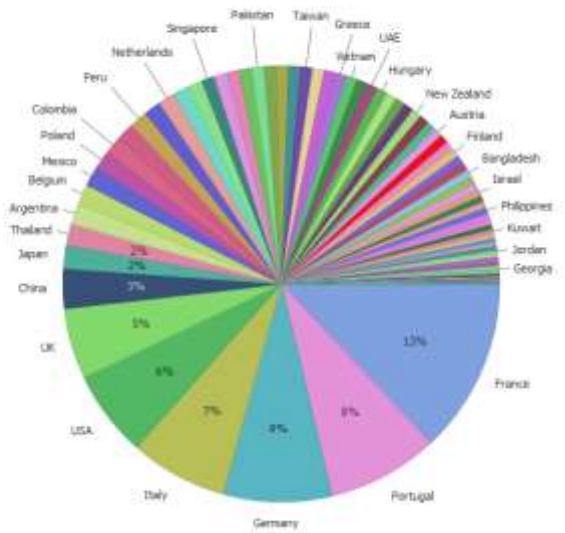
Slovakia



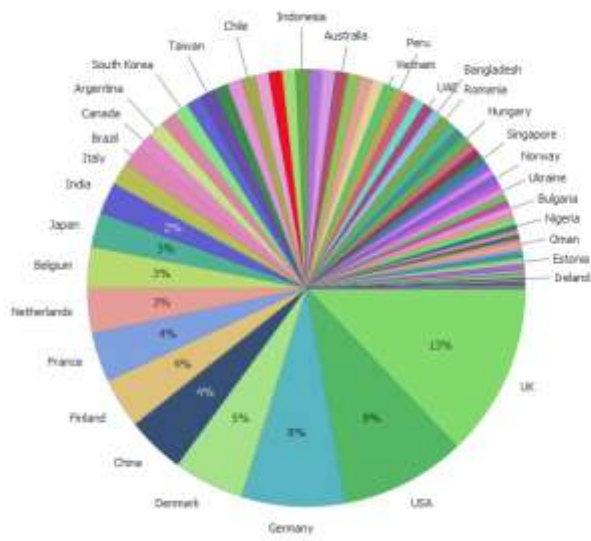
Slovenia



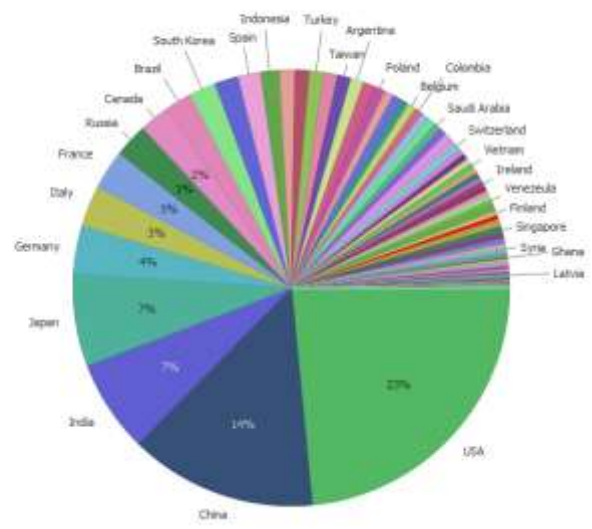
Spain



Sweden



UK



Appendix E : Competitive Dashboards

This part of the document provides dashboards which include metrics for:

- Sales
- Imports (by leading countries and by EU/ non- EU)
- Exports (by leading destination countries and by EU/ non- EU)
- Domestic Market (Sales + Imports – Exports)
- Employment
- Forecast Growth

All values are in million EUR.

Individual data dashboards

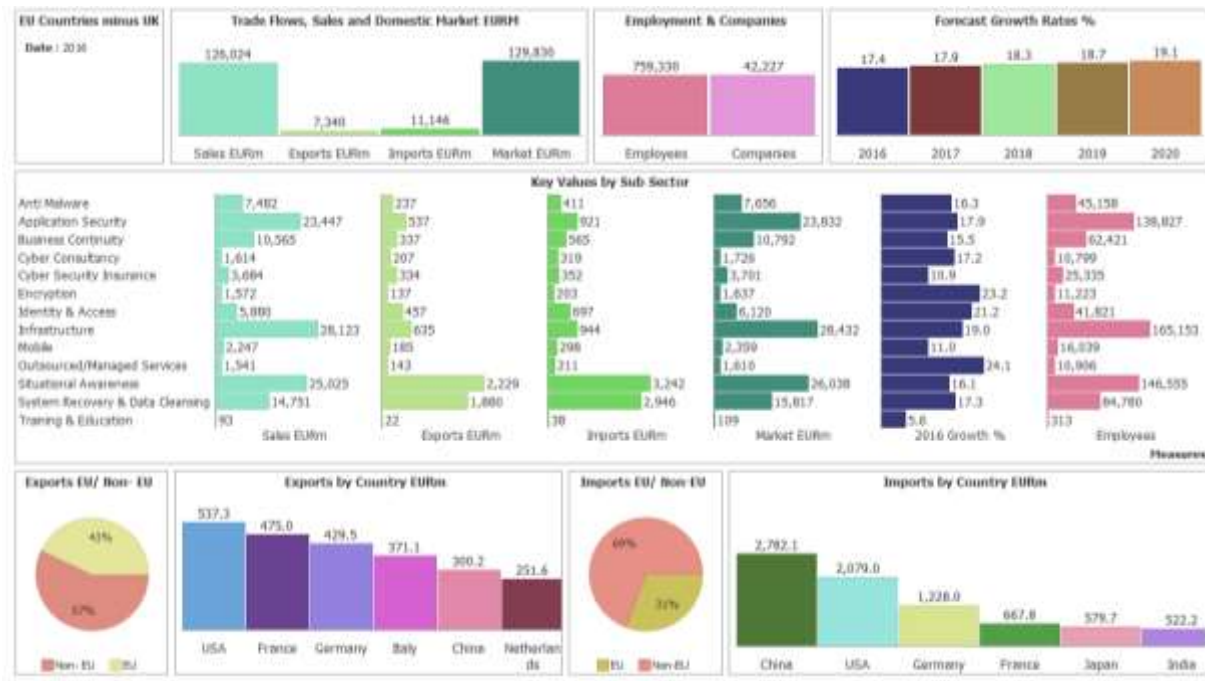
Data are provided in the following Sections for:

- The EU 28 Member States
- The EU 27 (minus UK)
- Major EU competitors
 - USA
 - China
 - Japan
 - India.
- Individual Member States

1.1.72 EU 28



1.1.73 EU 27



1.1.74 USA



1.1.75 China



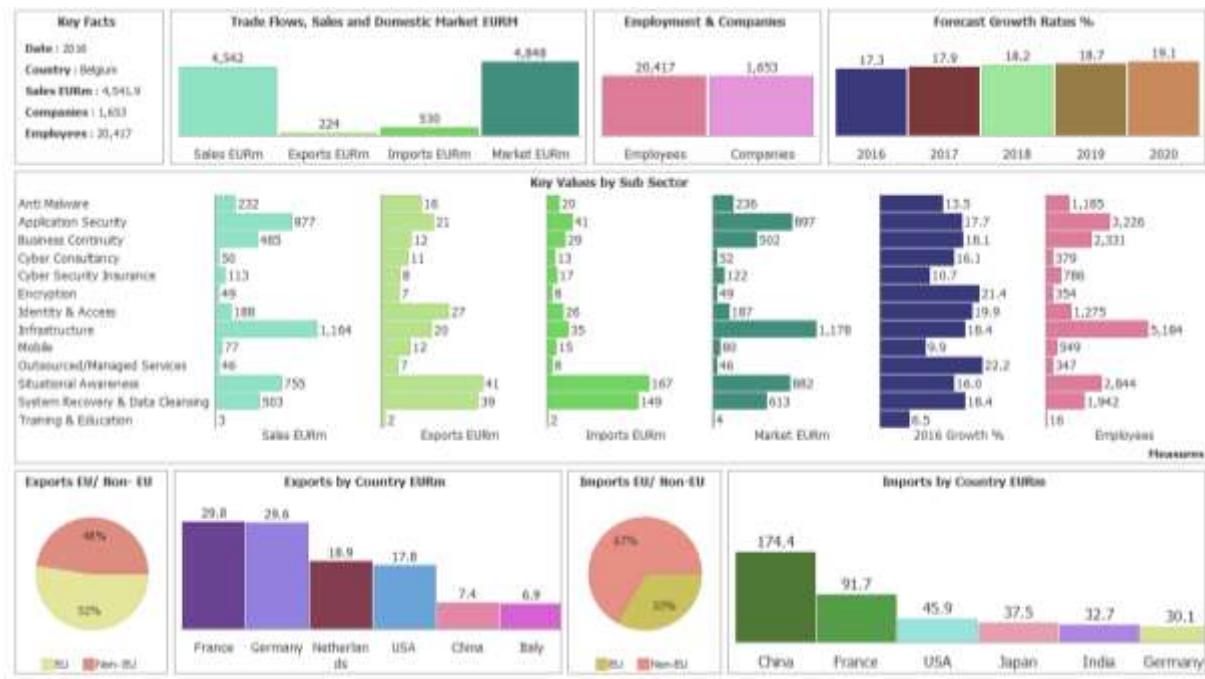
1.1.76 Japan



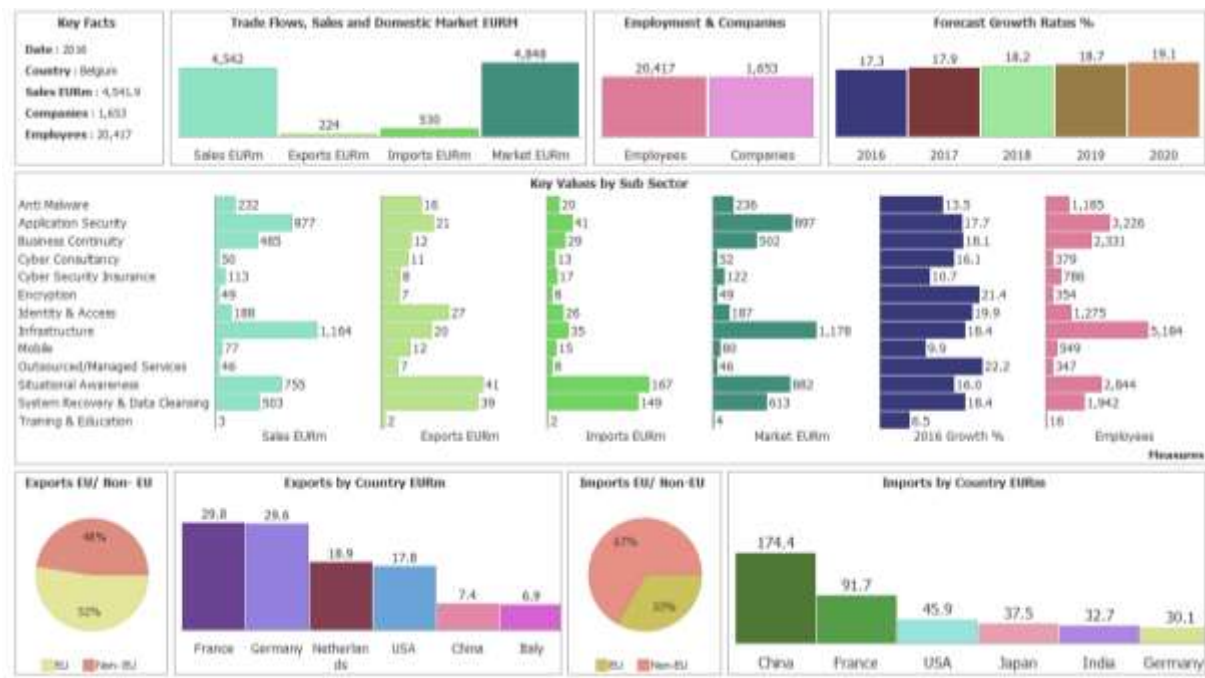
1.1.77 India



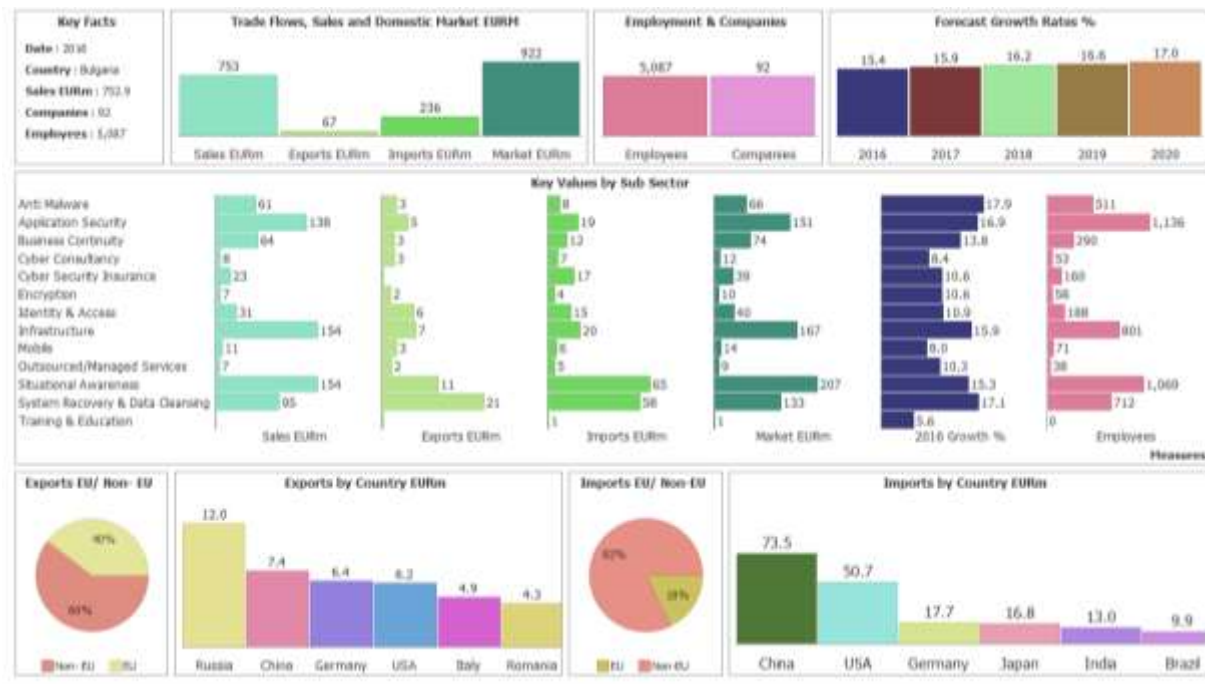
1.1.78 Belgium



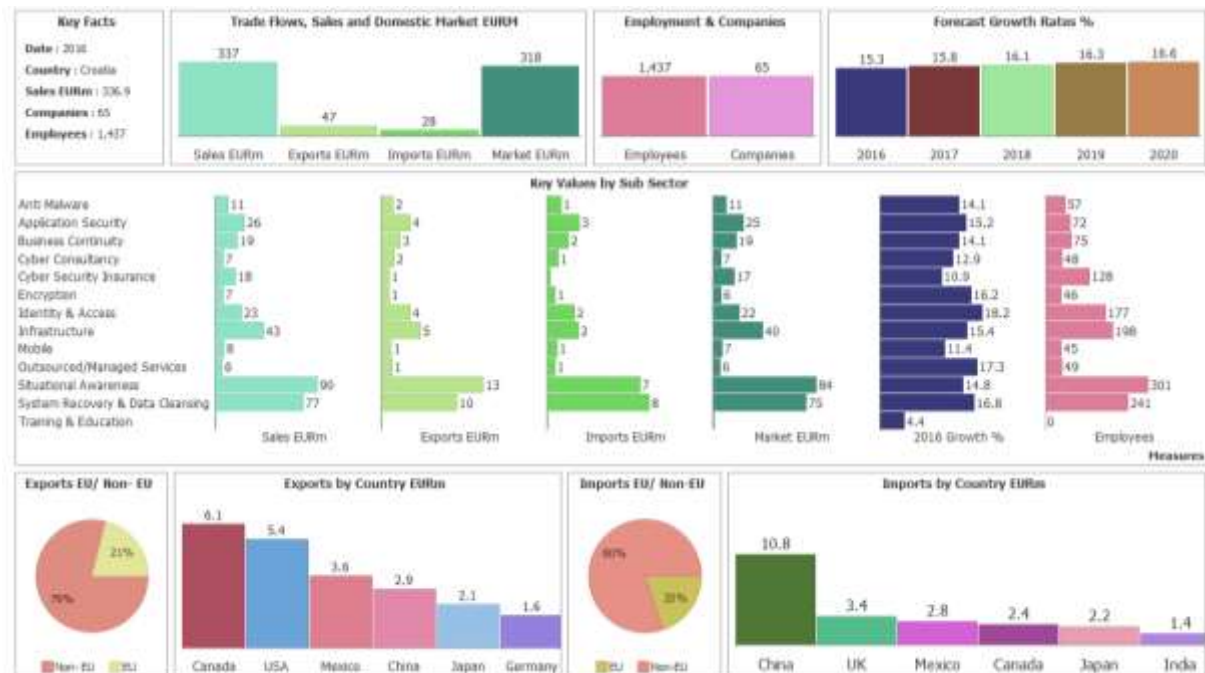
1.1.79 Austria



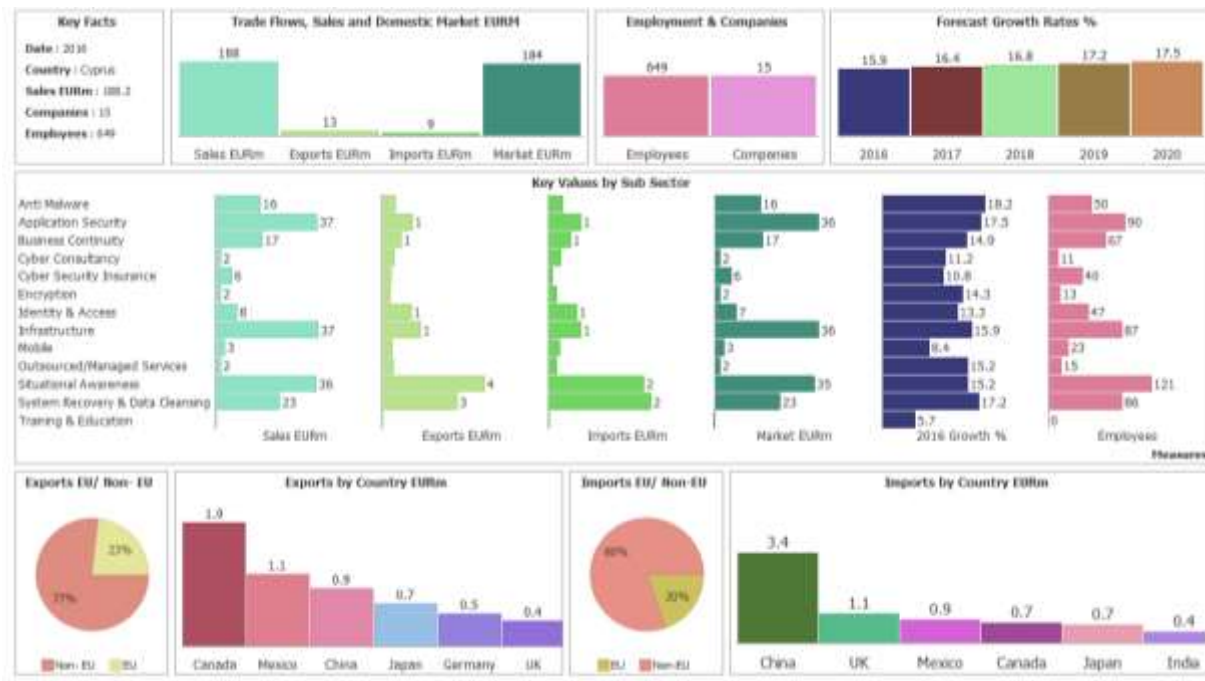
1.1.80 Bulgaria



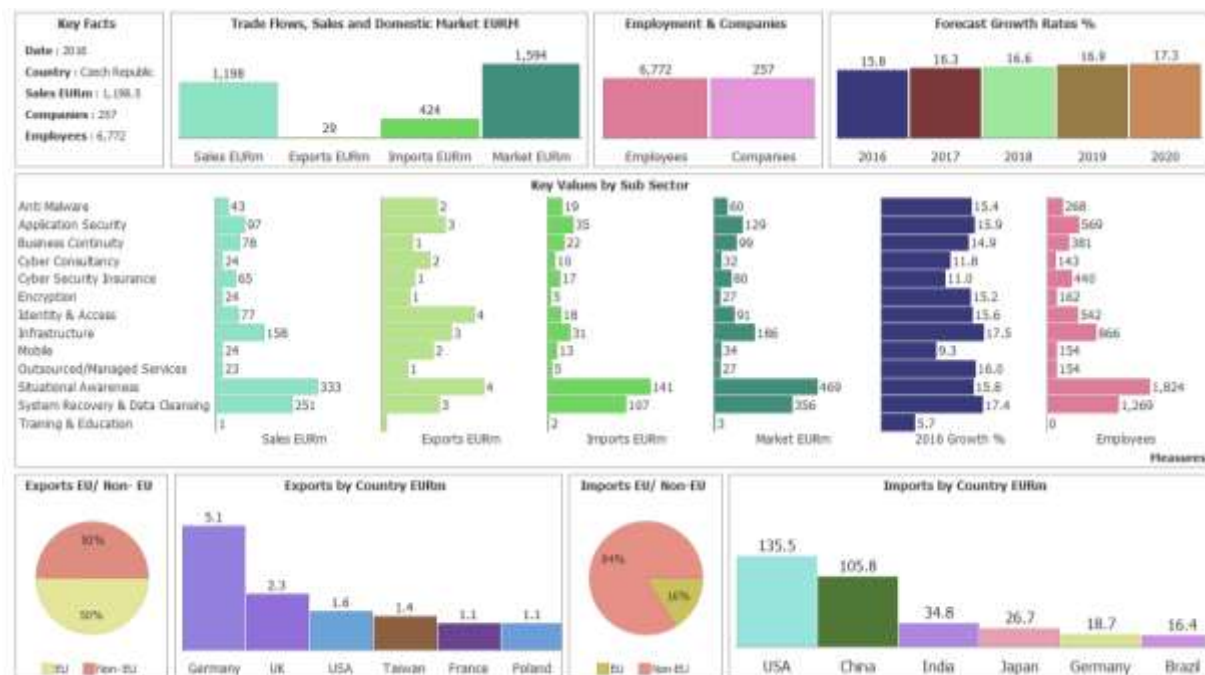
1.1.81 Croatia



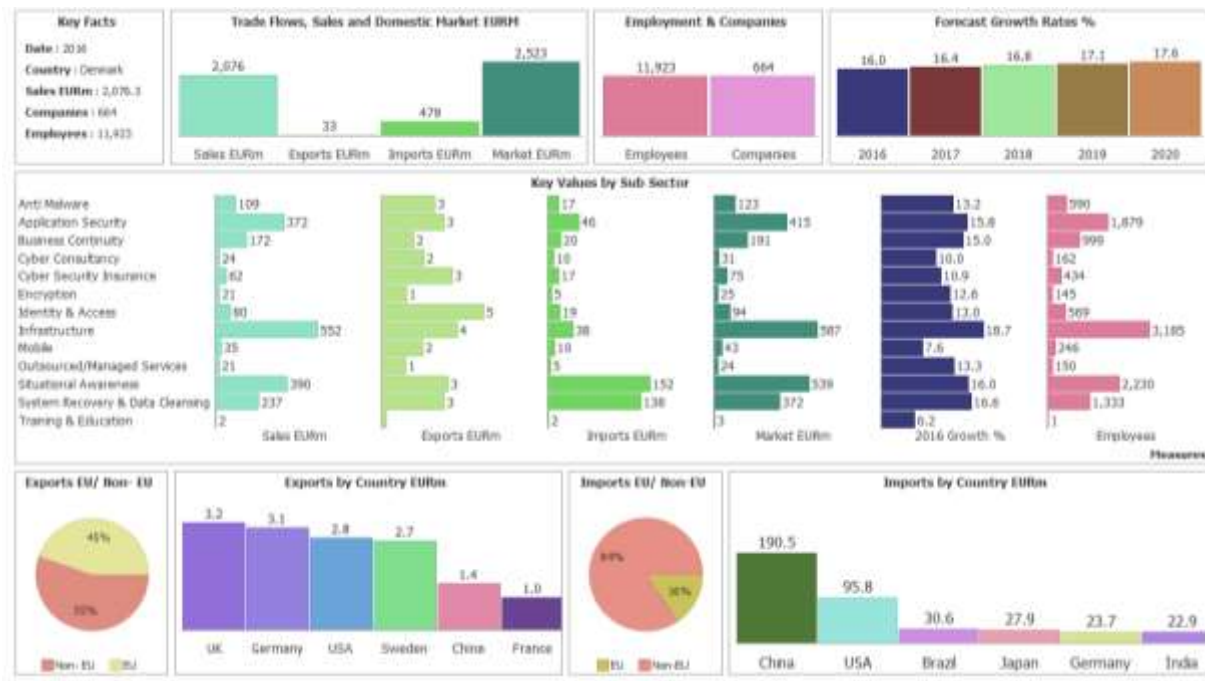
1.1.82 Cyprus



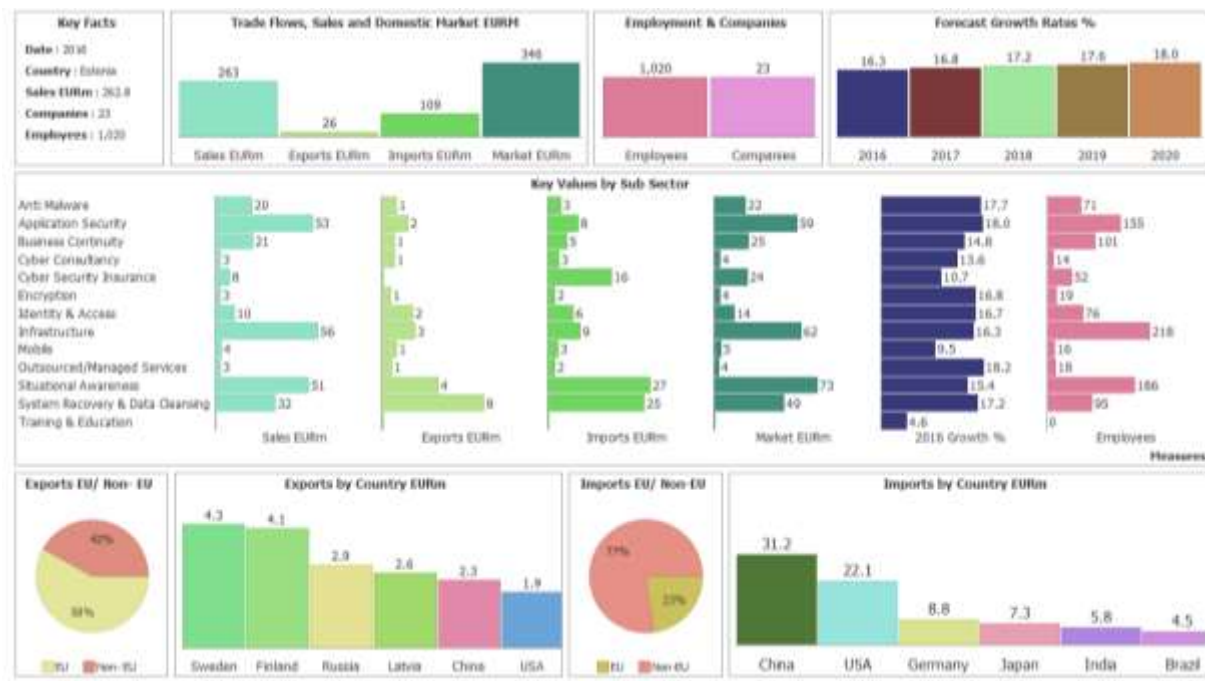
1.1.83 Czech Republic



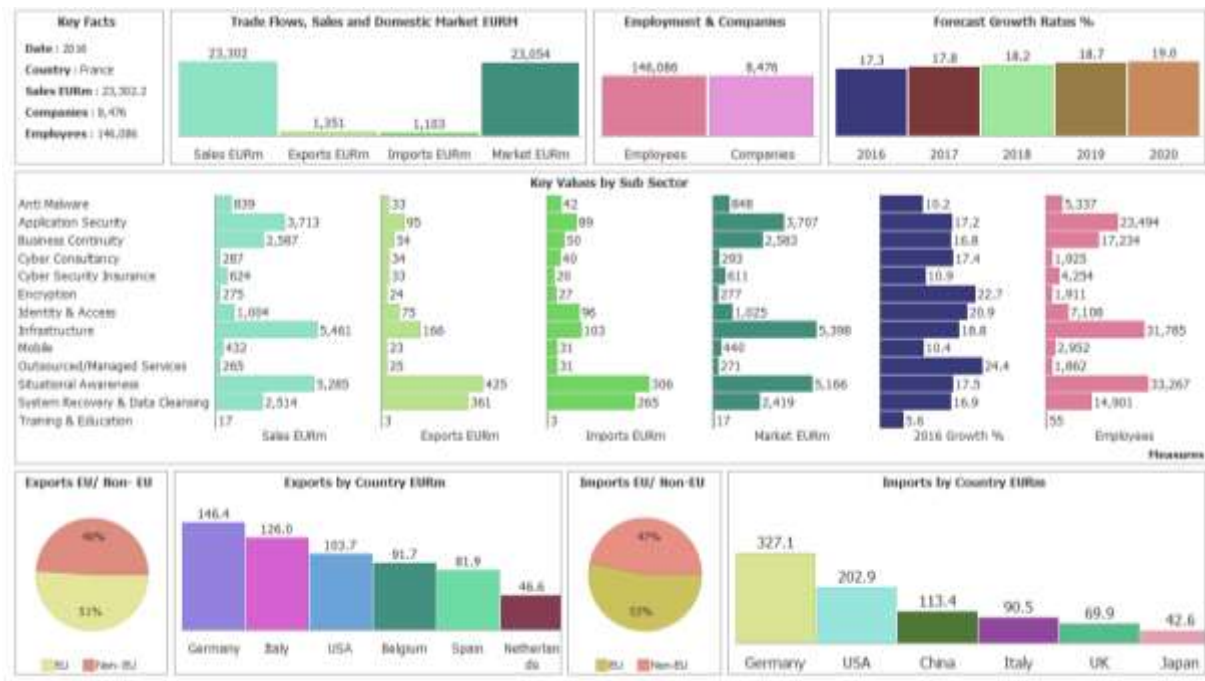
1.1.84 Denmark



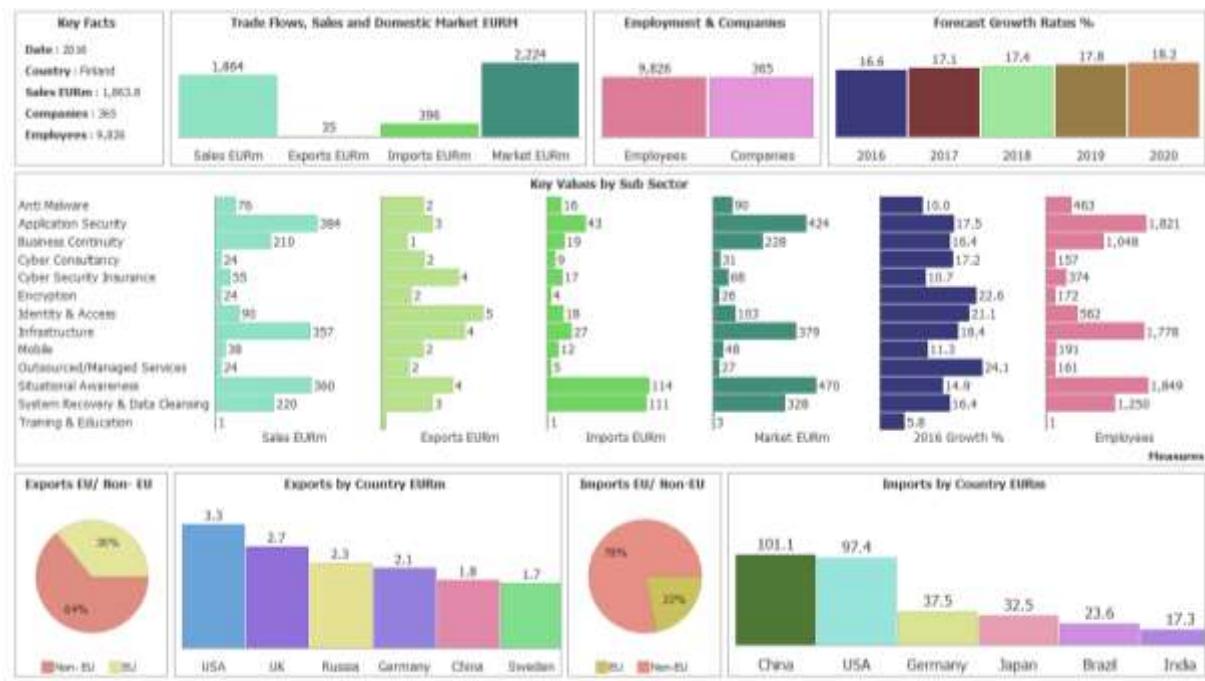
1.1.85 Estonia



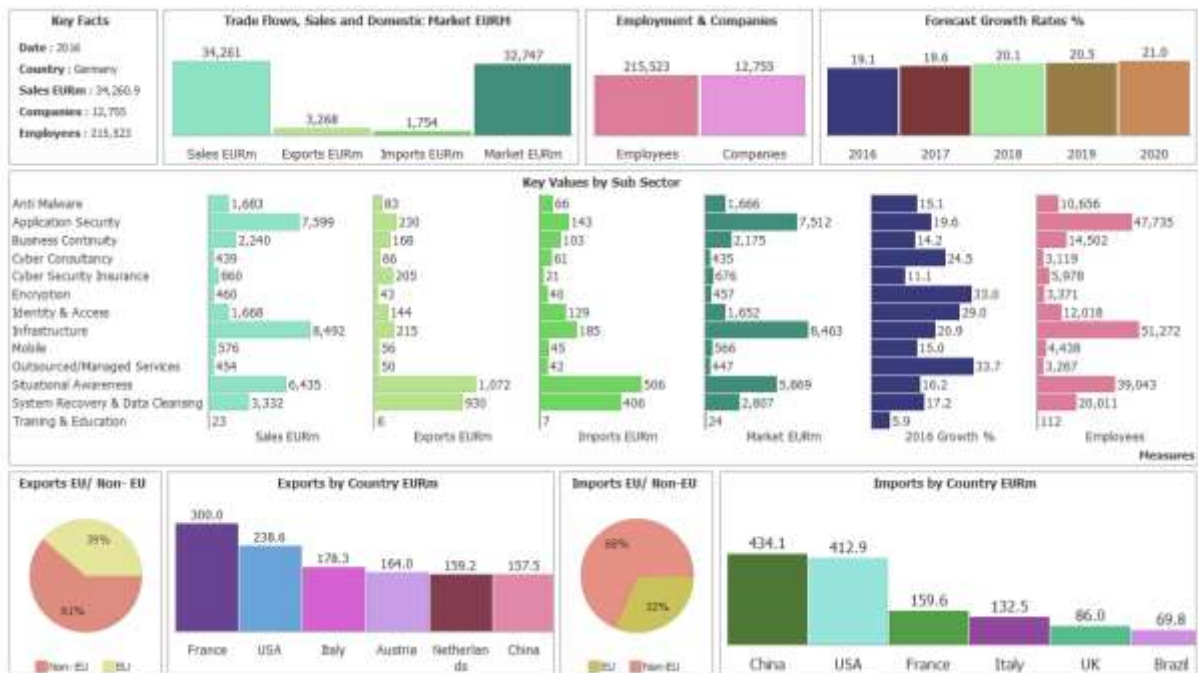
1.1.86 France



1.1.87 Finland



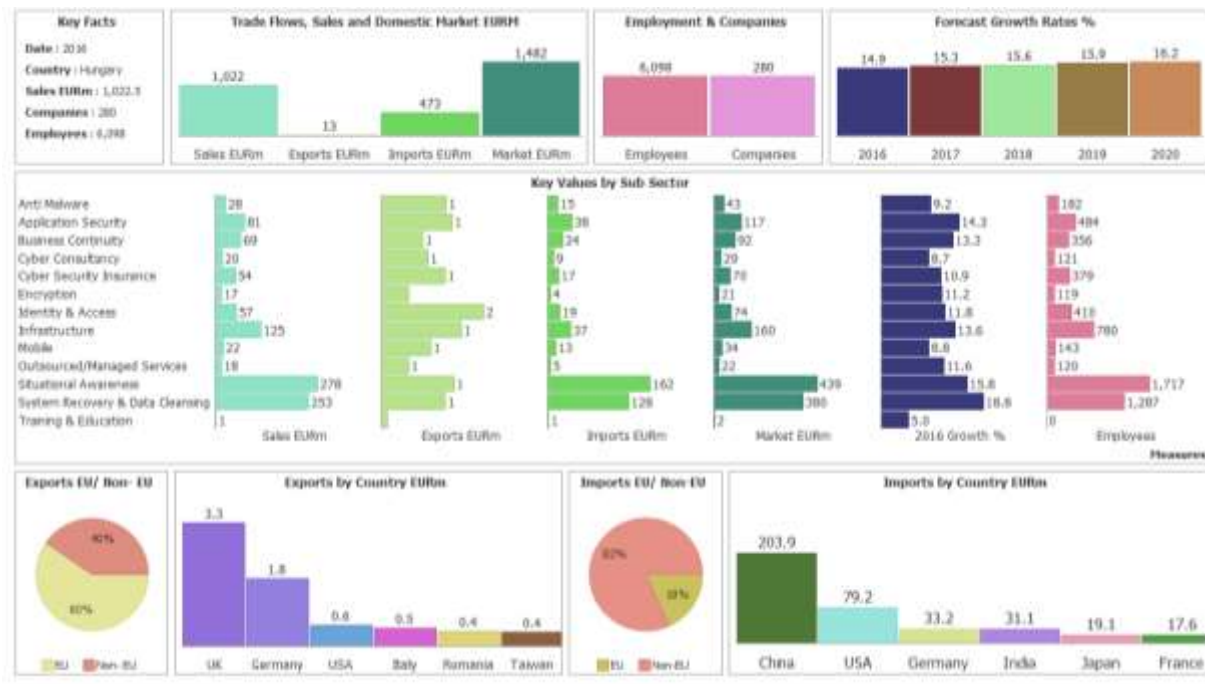
1.1.88 Germany



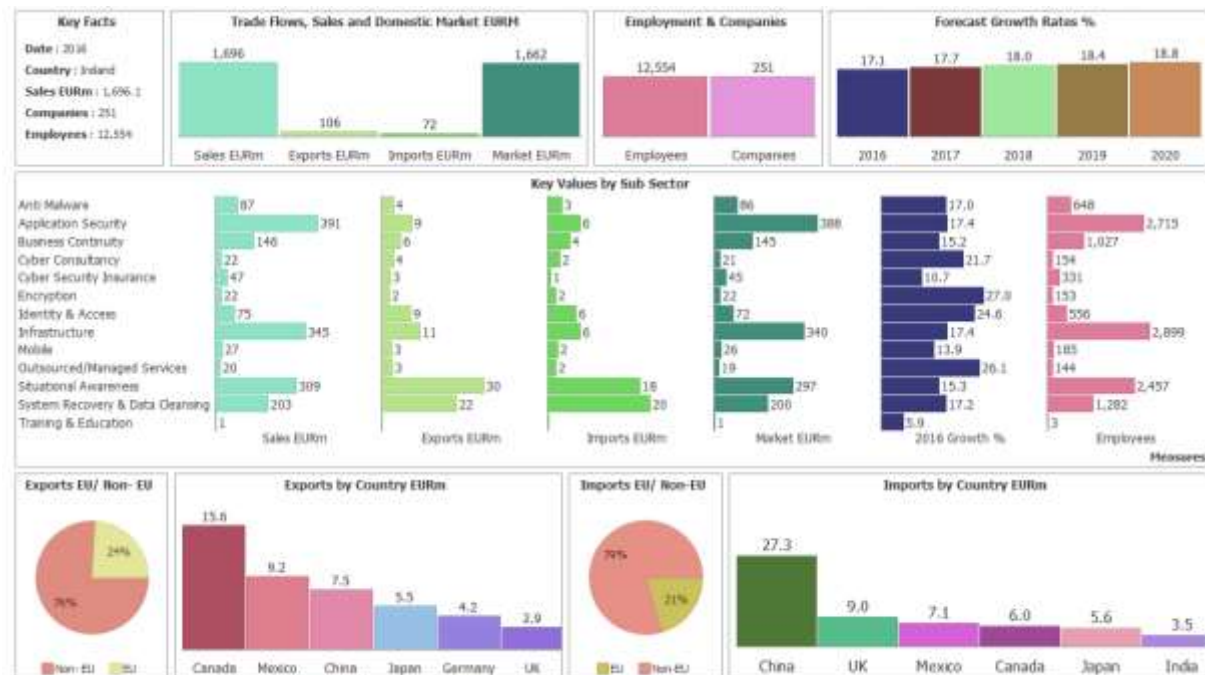
1.1.89 Greece



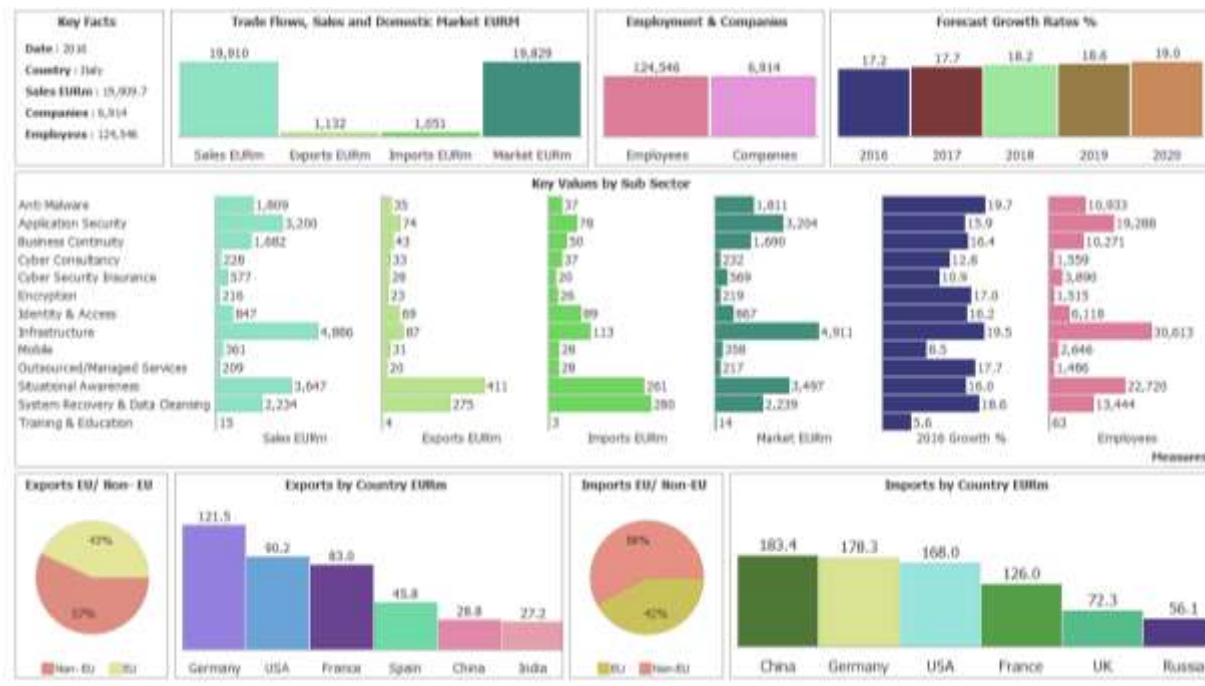
1.1.90 Hungary



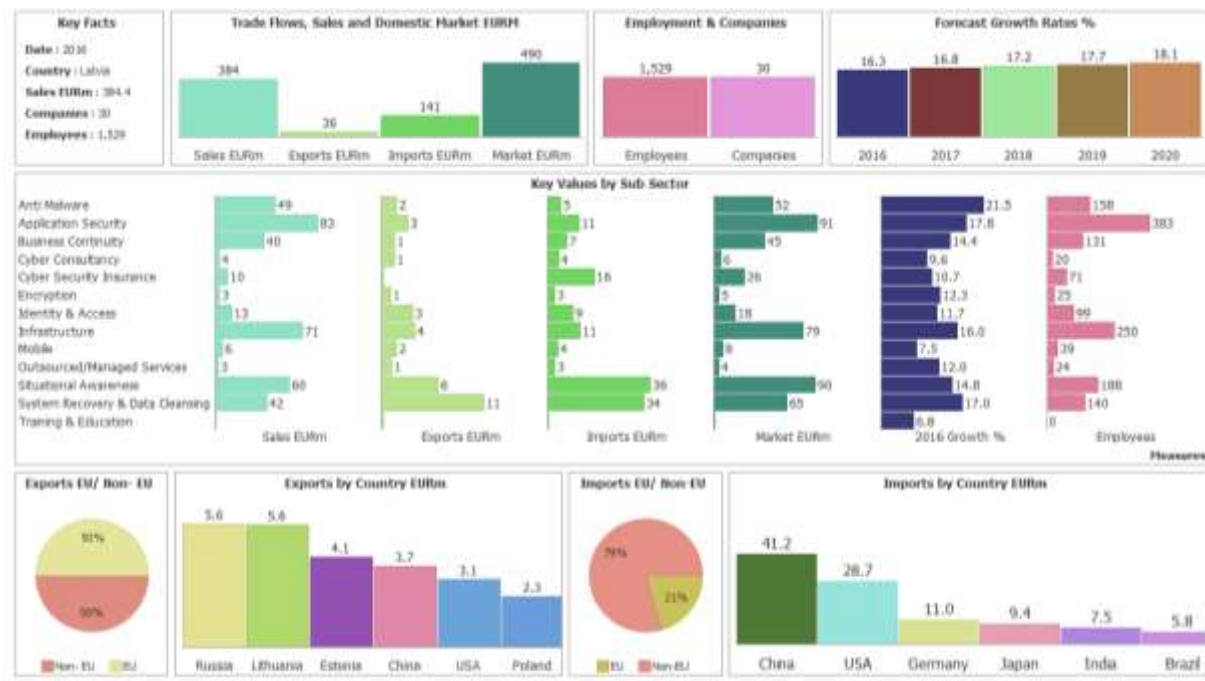
1.1.91 Ireland



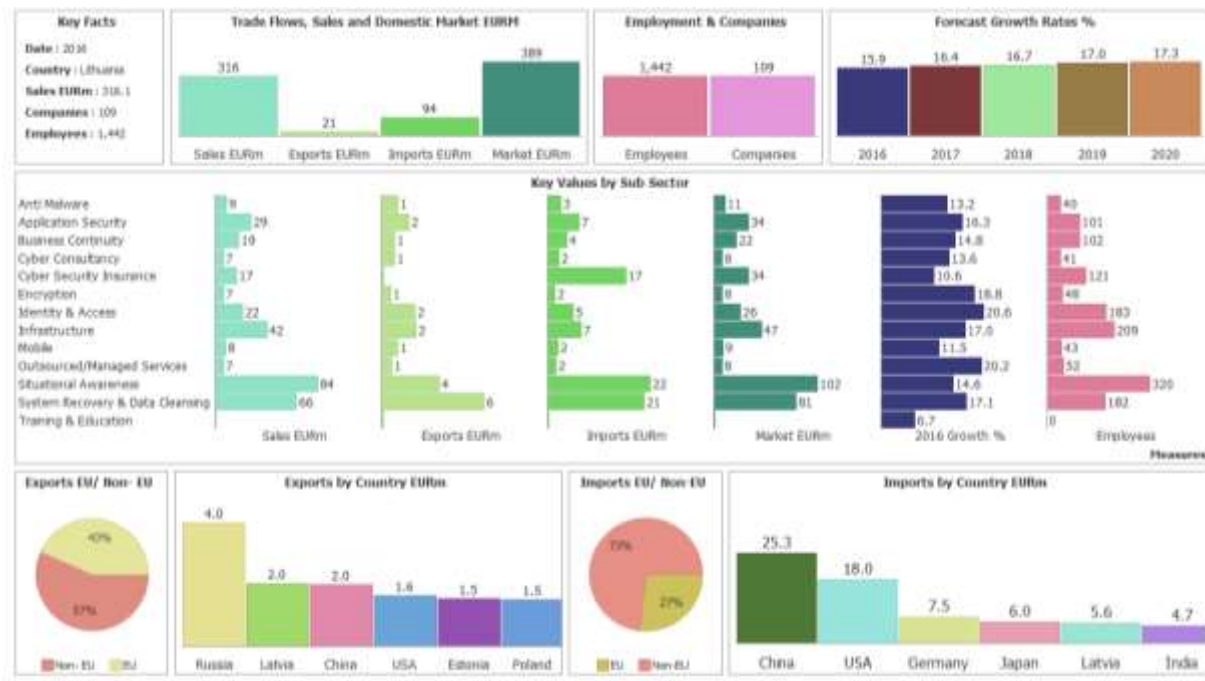
1.1.92 Italy



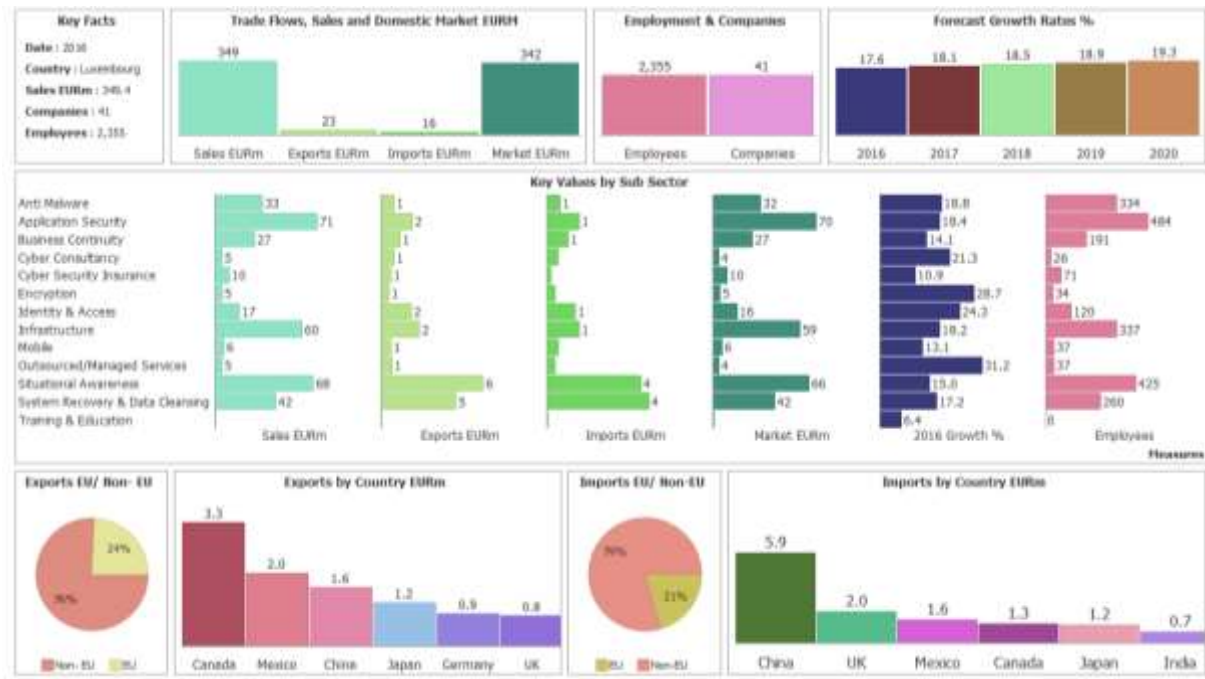
1.1.93 Latvia



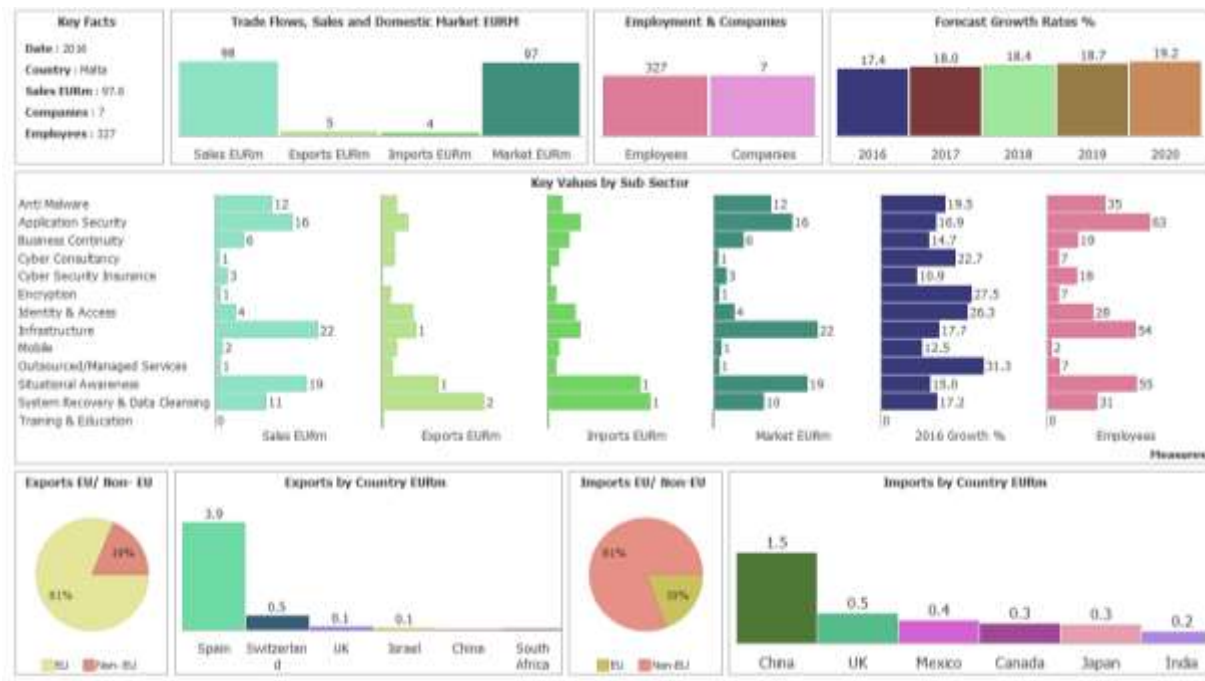
1.1.94 Lithuania



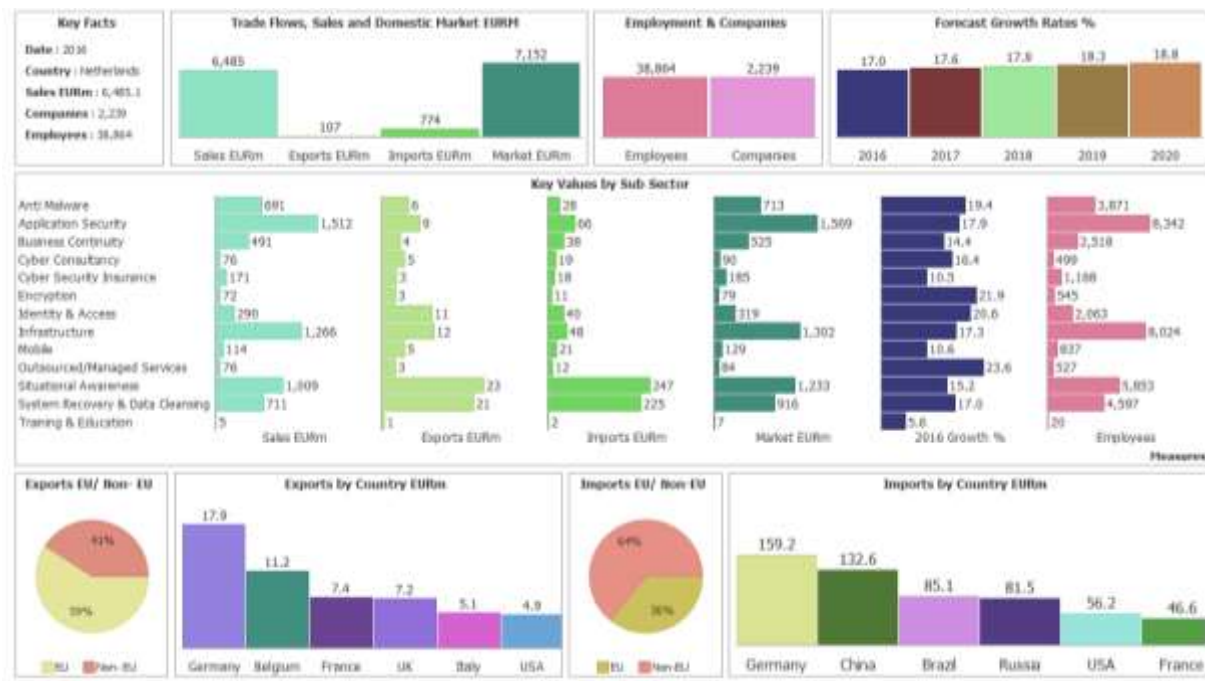
1.1.95 Luxembourg



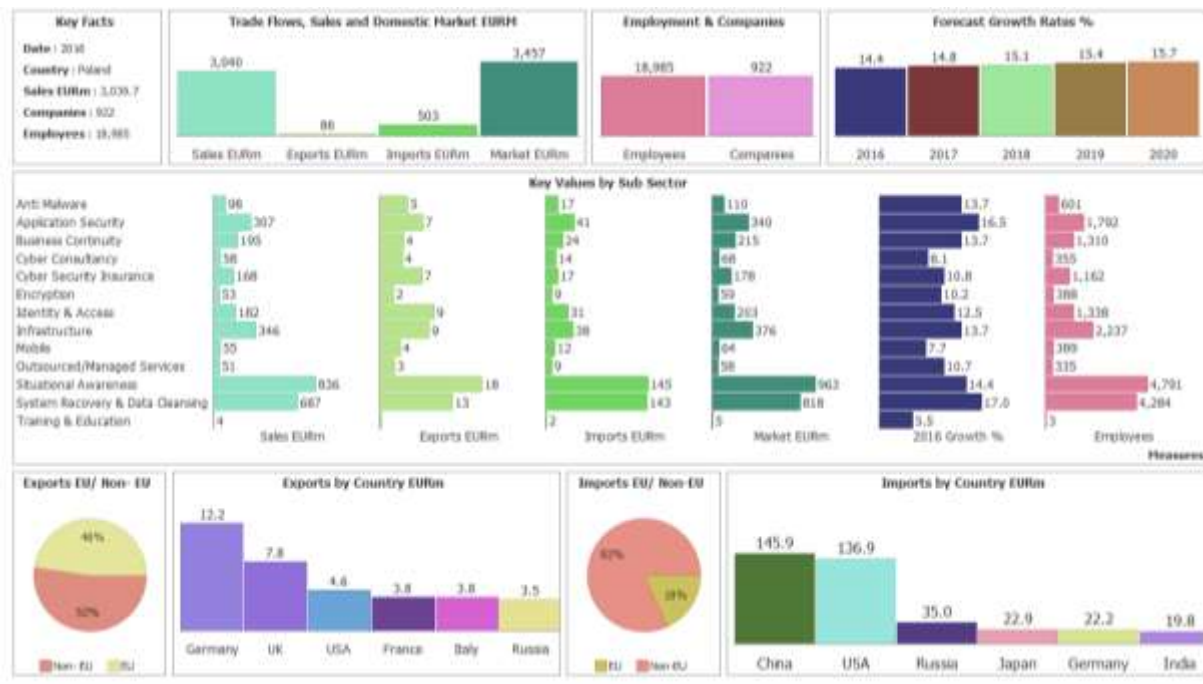
1.1.96 Malta



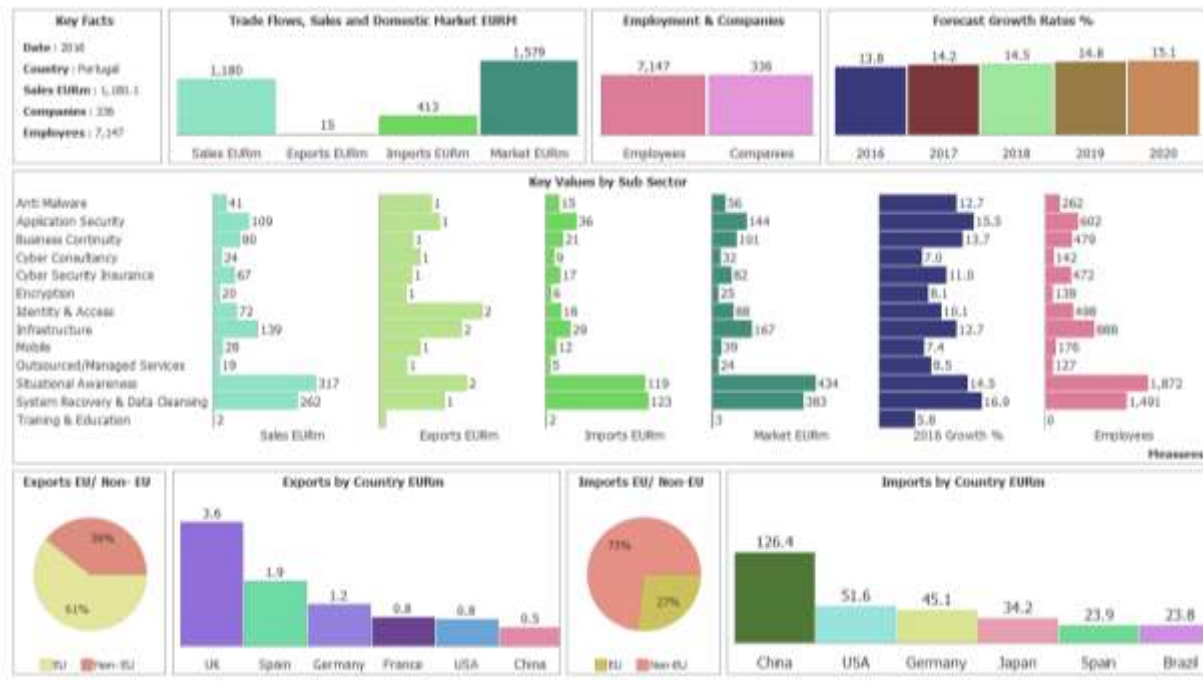
1.1.97 Netherlands



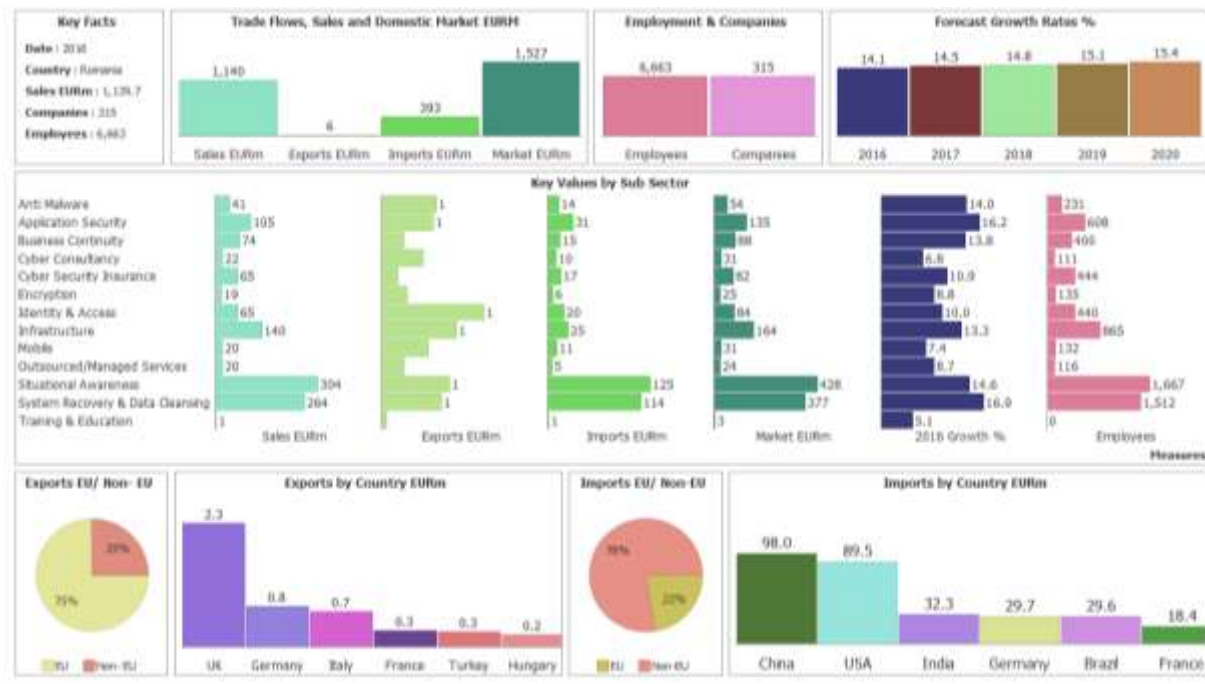
1.1.98 Poland



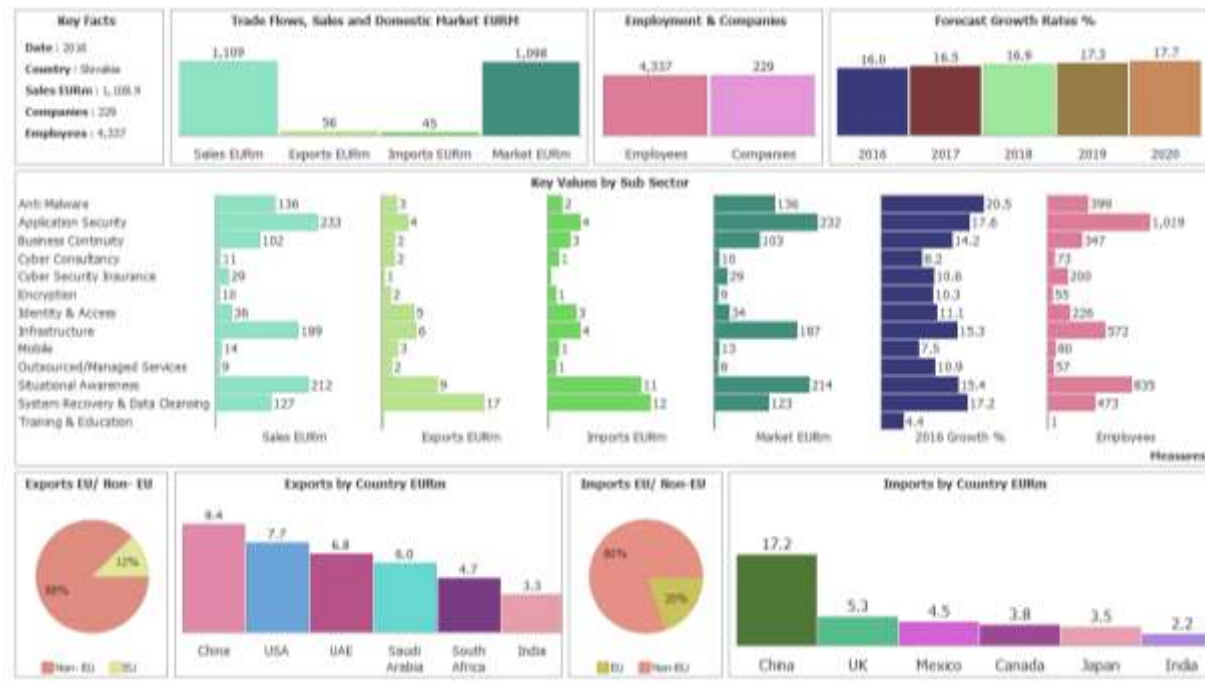
1.1.99 Portugal



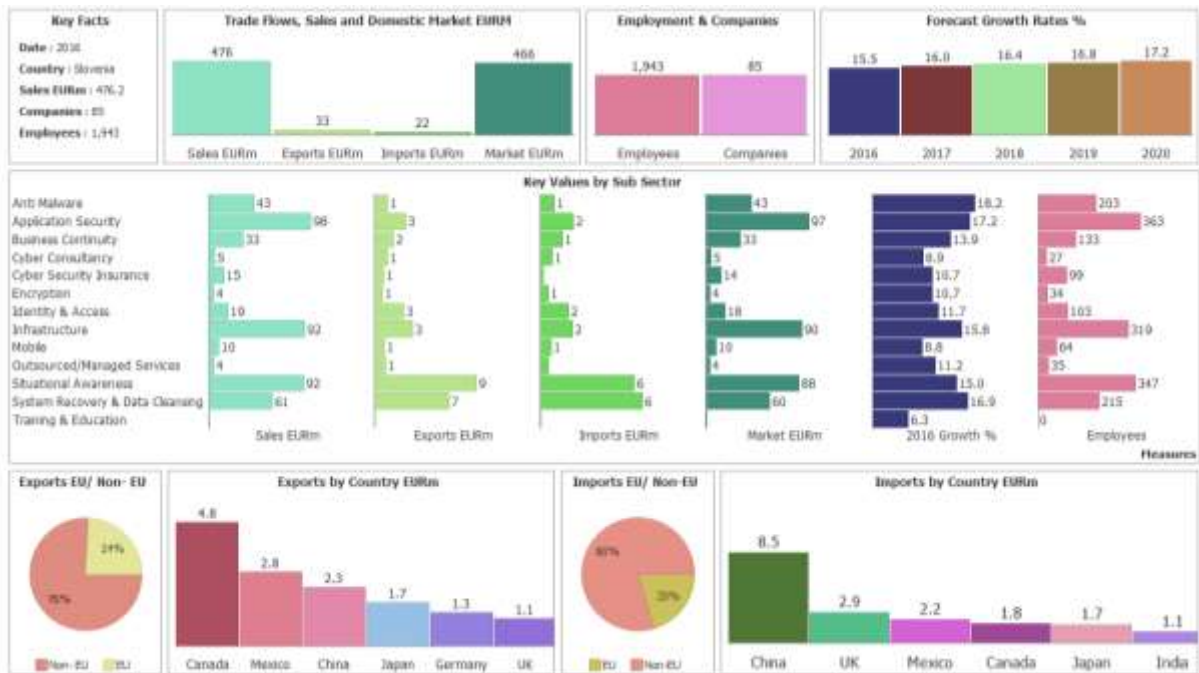
1.1.100 Romania



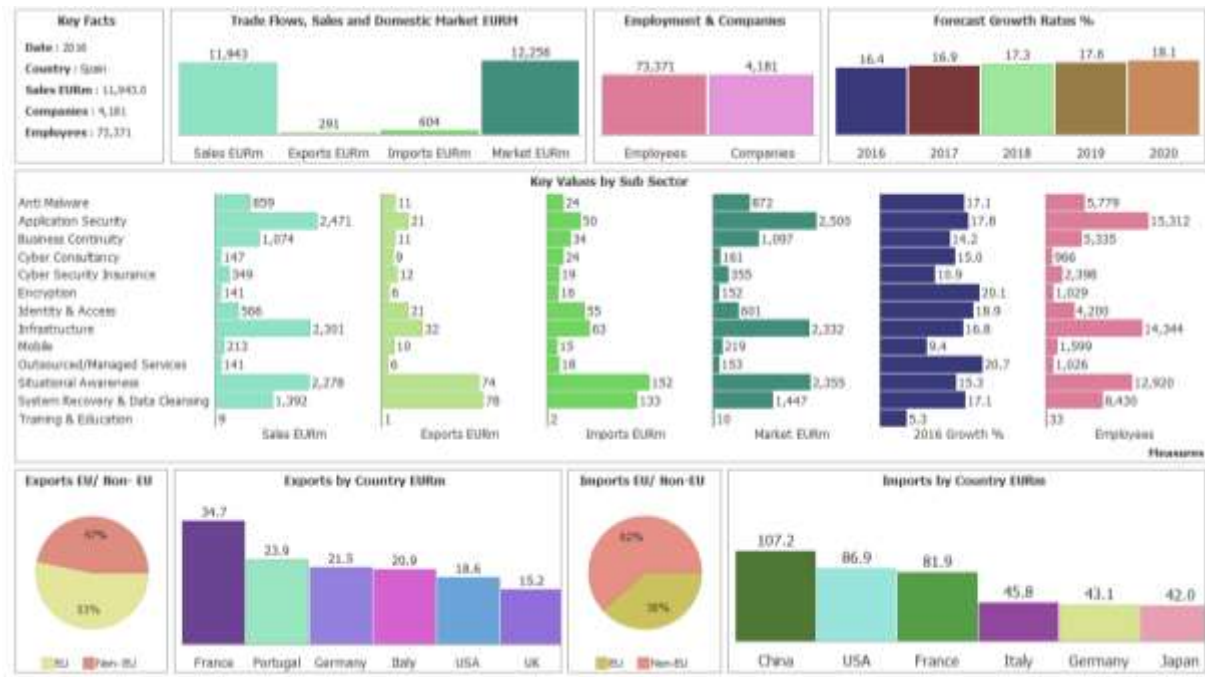
1.1.101 Slovakia



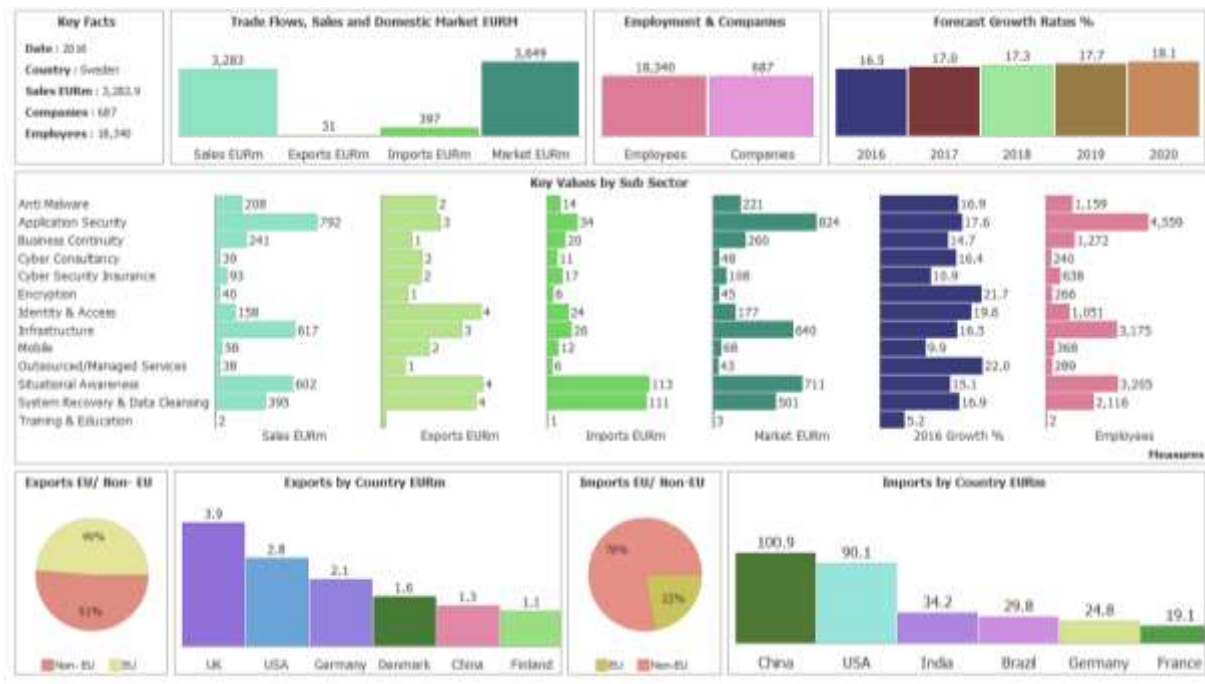
1.1.102 Slovenia



1.1.103 Spain



1.1.104 Sweden



1.1.105 UK



Appendix F : Trade Flows by Sub-sector

EU28



USA



China



Japan



India



Appendix G : Research Methodology Confidence Levels

All data values in this draft report are created by the intelligent use and transformation of primary and secondary data sources (selectively listed above). Data sources are carefully managed by measurement and rating of their accuracy and reliability over time, and by excluding sources that are outdated or without a measurable track record. No less than seven qualified sources are ever used and often, as is the case for this research, the final list of sources is much higher than this. A mean value is then calculated from these selected values and assigned a confidence level. Our aim is for an average confidence level of 85%.

The summary results are shown below in Figure 58, Figure 59 and in Table 44. Confidence levels are calculated for all product and service activities and for all countries but for convenience have been aggregated in the following charts at either country or sub-sector level.

The conventions for the bubble charts below are: horizontal axis= Sales Confidence Levels, vertical axis= Sales Growth Confidence Levels. Growth confidence levels are based upon trading over the next 24 months.

Figure 58 : EU Confidence Levels Sales and Sales Growth by Country

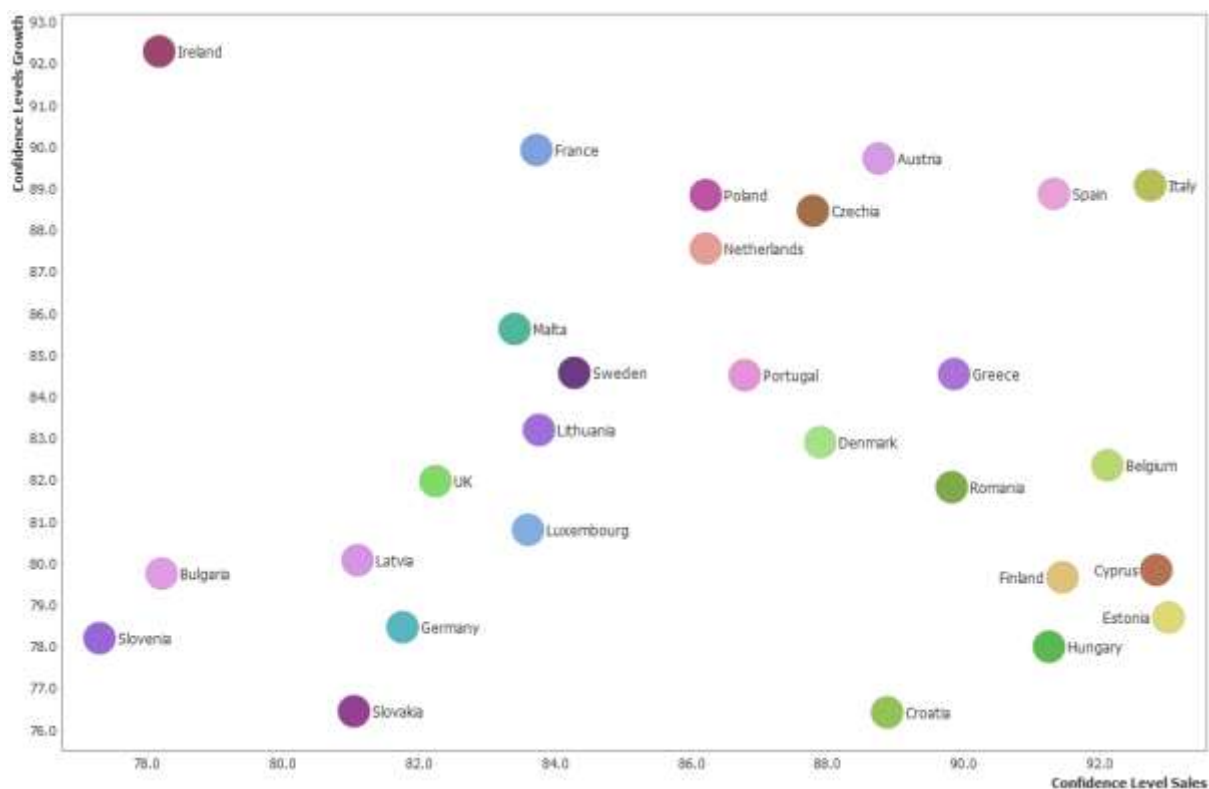
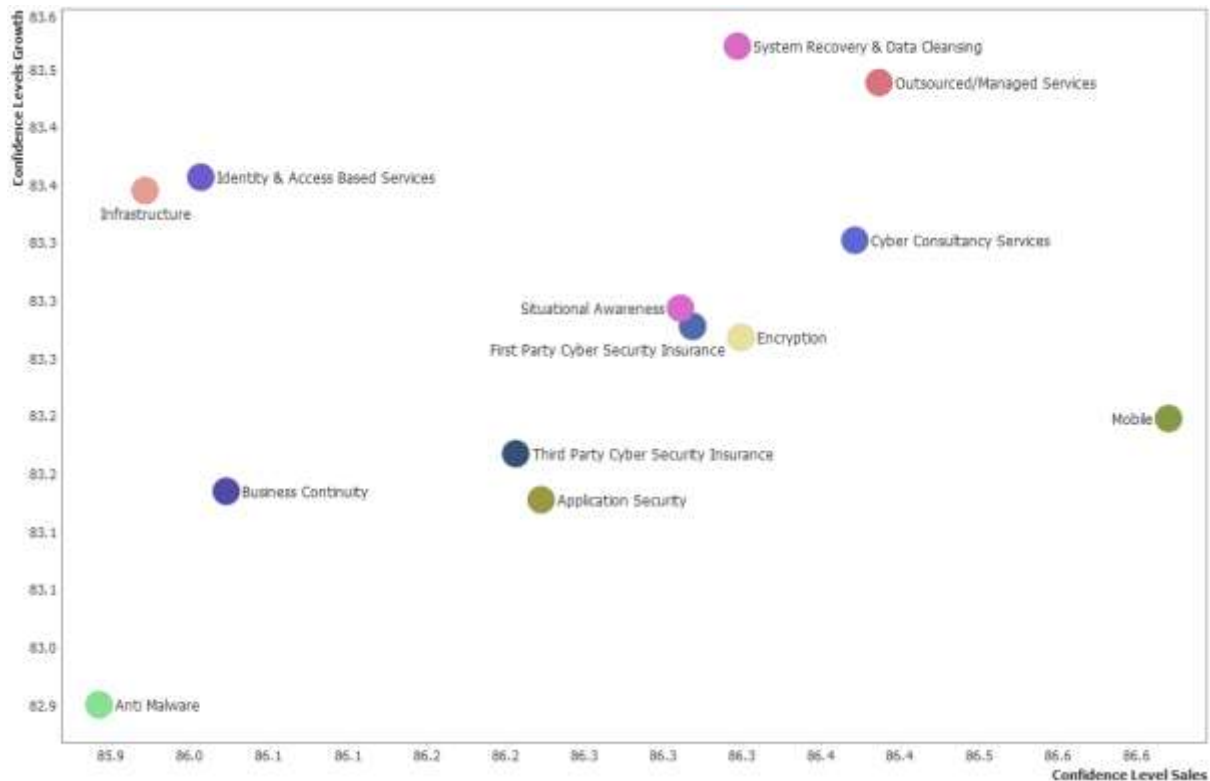


Figure 59 shows confidence levels for EU Sales and Sales Growth by country. The mean value for the sales confidence level is 86% and for sales growth is 83%. Figure 50 shows that confidence levels for individual countries varies between 76- 93%, reflecting the differing qualities of data and sources available for each country.

Figure 59 shows confidence levels for EU Sales and Sales Growth by sub-sector. The mean value for the sales confidence level is 86% and for sales growth is 83%. Figure 51 shows that confidence levels for individual sub-sectors vary between 82- 86%, reflecting the differing qualities of data and sources available for each sub-sector.

Figure 59 : EU Confidence Levels Sales and Sales Growth by Sub-sector



As an extension of the analysis in Figure 43, Table 44 shows confidence levels for EU sales and sales growth.

Table 44 : Confidence Levels EU Sales and Sales Growth

Country	Sales	Sales Growth
Austria	89.0	89.5
Belgium	91.9	82.5
Bulgaria	78.2	79.8
Croatia	88.7	77.0
Cyprus	92.8	79.7
Czech Republic	87.6	88.4
Denmark	87.7	82.7
Estonia	93.2	79.0
Finland	91.3	79.6
France	83.8	90.1
Germany	81.9	78.3
Greece	90.0	84.8
Hungary	91.5	77.6
Ireland	78.0	92.6
Italy	93.2	88.9
Latvia	80.7	80.2
Lithuania	84.1	83.4
Luxembourg	83.6	80.7
Malta	83.3	85.7
Netherlands	86.0	87.6
Poland	86.1	88.8
Portugal	87.0	84.4
Romania	89.8	81.9
Slovakia	81.0	76.7
Slovenia	77.4	78.4
Spain	91.3	88.5
Sweden	84.3	84.9
UK	82.6	82.4

Appendix H : Taxonomy – Cybersecurity Data Level 2 – 4 Definitions

Anti Malware

Anti Spam Solutions
Anti Spam Solutions
Anti Virus/Worm
Anti Virus/Worm
Malware
Malware
Specialist Anti Malware

Development of Software for Anti Spam Solutions
Supply of Software for Anti Spam Solutions
Development of Software for Anti Virus/Worm
Supply of Software for Anti Virus/Worm
Development of Software for Malware
Supply of Software for Malware
Malware Forensics

Application Security

Application Code Security
Application Code Security
Content Filtering & Monitoring
Content Filtering & Monitoring
Patch Management
Patch Management
Vulnerability Assessment
Vulnerability Assessment
Vulnerability Assessment
Vulnerability Assessment
Vulnerability Assessment
Vulnerability Assessment
Vulnerability Assessment

Development of Software for Application Security
Supply of Software for Application Security
Development of Software for Content Filtering & Monitoring
Supply of Software for Content Filtering & Monitoring
Development of Software for Patch Management
Supply of Software for Patch Management
Automated Alert Correlation
Automated Attack Trend Analysis
Automated Causality Analysis
Automated Vulnerability Analysis
Cyber Vulnerability Data
Development of Software for Vulnerability Assessment
Manual Vulnerability Analysis
Supply of Software for Vulnerability Assessment

Business Continuity

Business Continuity/Recovery
Business Continuity/Recovery
Business Continuity/Recovery
Business Continuity/Recovery
Business Continuity/Recovery
Computer Forensics
Computer Forensics
Computer Forensics
Computer Forensics
IT/Cyber Forensics
IT/Cyber Forensics
IT/Cyber Forensics

Development of Software for Business Continuity/Recovery
Email Recovery
Operating System Recovery
Supply of Software for Business Continuity/Recovery
Virtualisation Recovery
Computer Hardware Forensics
Development of Software for Computer Forensics
Provision of Computer Forensics Services
Supply of Software for Computer Forensics
Automated Forensics
Forensic Data Recovery
Manual Forensics

Cyber Consultancy

Access Management
Anti Spam Solutions
Anti Virus/Worm
Application Code Security
Business Continuity/Recovery
Computer Forensics
Content Filtering & Monitoring
Corporate Services
Corporate Services
Corporate Services
Corporate Services
Corporate Services
Corporate Services
Corporate Services
Encryption/PKI/Digital Certificates
Firewalls
Identity Management
Intrusion Detection
Malware
Messaging Security
Mobile Security/Device management
Patch Management
PC/Mobile/End Point Security
Vulnerability Assessment
Wireless Security
Cyber Consultancy

Consulting Services for Access Management
Consulting Services for Anti Spam Solutions
Consulting Services for Anti Virus/Worm
Consulting Services for Application Security
Consulting Services for Business Continuity/Recovery
Consulting Services for Computer Forensics
Consulting Services for Content Filtering & Monitoring
Audit
Governance, Risk & Compliance
Insider Threat
Legislation & Standards
Security Policy
Strategy - business
Strategy – govt
Training a & Awareness
Consulting Services for Public Key Infrastructure
Consulting Services for Firewalls
Consulting Services for Identity Management
Consulting Services for Intrusion Detection
Consulting Services for Malware
Consulting Services for Messaging Security
Consulting Services for Remote Access Management
Consulting Services for Patch Management
Consulting Services for PC/Mobile/End Point Security
Consulting Services for Vulnerability Assessment
Consulting Services for Wireless Security
Cyber Consultancy

Cyber Security Insurance

Business Interruption from Network Downtime
 Business Interruption from Network Downtime
 Business Interruption from Network Downtime
 Cyber Extortion
 Cyber Extortion
 Cyber Extortion
 Cyber Extortion
 Investigation of Privacy Breach
 Loss of Third Party Data
 Loss of Third Party Data
 Loss of Third Party Data
 Loss of Third Party Data
 Loss of Third Party Data
 Loss of Third Party Data
 Loss or Damage to Digital Assets
 Loss or Damage to Digital Assets
 Multi-Media Liability
 Multi-Media Liability
 Multi-Media Liability
 Multi-Media Liability
 Reputational Damage
 Security and Privacy Breaches
 Security and Privacy Breaches
 Security and Privacy Breaches
 Security and Privacy Breaches
 Security and Privacy Breaches
 Theft of Money and Digital Assets
 Theft of Money and Digital Assets
 Third Party Breach Notification

Business Interruption from Network Downtime
 Degradation in Service from network downtime
 Network Failures
 Cyber extortion through data release
 Cyber extortion through false communications to obtain personal information
 Cyber extortion through network damage
 Cyber extortion through network restriction
 Investigation by regulators Insurance
 Compensation for Data Errors
 Compensation for Denial of Access
 Compensation for Software Failure
 Compensation for System Security Failure
 Liability for Data/Information Corruption
 Liability for Data/Information Loss
 Data Loss or Damage
 Software Loss or Damage
 Breach of Privacy
 Defamation
 Infringement of third party Intellectual Property
 Negligence in Publication of any Content in Electronic or Print Media
 Data protection breach reporting
 Breach of Employee Privacy or Confidentiality
 Breach of Third Party Privacy
 Failure of Outsourced service provider
 Security breaches
 Transmission of Malicious Code
 Electronic theft of funds/money
 Theft of computer equipment
 Customer Notification Expenses

Encryption

Digital Signatures
 Encryption/PKI/Digital Certificates
 Encryption/PKI/Digital Certificates
 Encryption/PKI/Digital Certificates
 Storage Security, including Cloud

Digital Signature Software
 Certificate Generation
 Development of Software for Public Key Infrastructure
 Supply of Software for Public Key Infrastructure
 Storage Security Localised

Identity & Access

Access Management
 Access Management
 Authentication
 Authentication
 Identity Management
 Identity Management
 Identity Management
 Identity Management
 Identity Management
 Intrusion & Anomaly Prevention
 Intrusion & Anomaly Prevention
 Messaging Security
 Messaging Security
 Messaging Security

Development of Software for Access Management
 Supply of Software for Access Management
 Physical /Virtual Authentication
 Single Sign On/Security Tokens
 CAPTCHA testing
 Chip and Pin
 Development of Software for Identity Management
 PIN sentry
 Supply of Software for Identity Management
 Anomaly Detection & Prevention
 Intrusion Prevention
 Abuse Mailbox Information
 Development of Software for Messaging Security
 Supply of Software for Messaging Security

Infrastructure

Data Management
 Firewalls
 Firewalls
 Infrastructure Monitoring
 Infrastructure Resilience
 Infrastructure Resilience
 Intrusion Detection
 Intrusion Detection
 Intrusion Detection
 Intrusion Detection
 Intrusion Detection
 Intrusion Detection
 Intrusion Detection
 Outsourced/Managed Services
 Storage Security, including Cloud

Data Leakage Prevention
 Development of Software for Firewalls
 Supply of Software for Firewalls
 Content Monitoring/Filtering
 Penetration/Vulnerability testing
 Secure Disposal
 Automated Intrusion Detection Systems Host Based IDS
 Automated Intrusion Detection Systems Network Based IDS
 Automated Intrusion Response
 Development of Software for Intrusion Detection
 Manual Intrusion Detection Systems Host Based IDS
 Manual Intrusion Detection Systems Network Based IDS
 Supply of Software for Intrusion Detection
 Cloud Security
 Storage Security Cloud

Mobile

Mobile Security/Device management
 Mobile Security/Device management
 PC/Mobile/End Point Security
 PC/Mobile/End Point Security
 PC/Mobile/End Point Security
 VPN
 Wireless Security
 Wireless Security

Development of Software for Remote Access Management
 Supply of Software for Remote Access Management
 Development of Software for PC/Mobile/End Point Security
 Mobile Device Recovery and Memory Card Recovery
 Supply of Software for PC/Mobile/End Point Security
 VPN Mobile Device
 Development of Software for Wireless Security
 Supply of Software for Wireless Security

Outsourced/Managed Services

Access Management
 Anti Spam Solutions
 Anti Virus/Worm
 Application Code Security
 Business Continuity/Recovery
 Content Filtering & Monitoring
 Cyber Services
 Cyber Services
 Encryption/PKI/Digital Certificates
 Firewalls
 Identity Management
 Intrusion Detection
 Malware
 Messaging Security
 Mobile Security/Device management
 Patch Management
 PC/Mobile/End Point Security
 Vulnerability Assessment
 Wireless Security

Management Services for Access Management
 Management Services for Anti Spam Solutions
 Management Services for Anti Virus/Worm
 Management Services for Application Security
 Management Services for Business Continuity/Recovery
 Management Services for Content Filtering & Monitoring
 Managed Services
 Security Services
 Management Services for Public Key Infrastructure
 Management Services for Firewalls
 Management Services for Identity Management
 Management Services for Intrusion Detection
 Management Services for Malware
 Management Services for Messaging Security
 Management Services for Remote Access Management
 Management Services for Patch Management
 Management Services for PC/Mobile/End Point Security
 Management Services for Vulnerability Assessment
 Management Services for Wireless Security

Situational Awareness

Darkweb
 Darkweb
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 External Cyber Threat Intelligence
 High Level Situational Awareness
 High Level Situational Awareness
 High Level Situational Awareness
 High Level Situational Awareness
 High Level Situational Awareness
 High Level Situational Awareness
 High Level Situational Awareness
 Internal Cyber Threat Intelligence
 Internal Cyber Threat Intelligence
 Internal Cyber Threat Intelligence
 Internal Cyber Threat Intelligence
 Low Level Situational Awareness
 Low Level Situational Awareness
 Media Monitoring
 Proactive Cyber Surveillance
 Proactive Cyber Surveillance
 Proactive Cyber Surveillance
 Proactive Cyber Surveillance
 Proactive Cyber Surveillance

Darkweb investigation Services
 Darkweb Software
 Commercial Cyber Intelligence Feeds
 Cyber Law Enforcement
 Cyber Security Industry Associations
 Cyber Security Researchers
 GEOIP Data
 Hash Databases
 Underground Cyber Security Forums
 Manual Alert Correlation
 Manual Attack Trend Analysis
 Manual Causality Analysis
 Manual Damage Assessment
 Manual Intrusion Response
 Manual Taint and Information Flow Analysis
 Training Services for Digital Rights Management
 Cyber Security Event Data
 Fraud Investigation
 Human Intelligence
 Sandboxes
 Automated Damage Assessment
 Automated Taint and Information Flow Analysis
 Social Media Monitoring
 Brand Monitoring
 DNS Monitoring
 Honeynets
 P2P Monitoring
 Watch List Monitoring

System Recovery & Data Cleansing

Data Recovery Services	Database Recovery
Data Recovery Services	Desktop Recovery
Data Recovery Services	Digital Photo Recovery
Data Recovery Services	Flash Drive Recovery
Data Recovery Services	Hard Drive Recovery
Data Recovery Services	Laptop Recovery
Data Recovery Services	RAID Recovery
Data Recovery Services	Server Recovery and Network Storage Recovery
Data Recovery Services	Solid State Drive Recovery
Data Recovery Services	Specialised Recovery Services
Data Recovery Services	Tape Recovery
Manual Data Cleansing	Data De-Duplication (removal of duplicate records)
Manual Data Cleansing	Data Formatting
Manual Data Cleansing	Data Updation
Manual Data Cleansing	Data Validation
Manual Data Cleansing	Data Verification
System Recovery & Data Cleansing	Data De-Duplication (removal of duplicate records)
System Recovery & Data Cleansing	Data Formatting
System Recovery & Data Cleansing	Data Updation
System Recovery & Data Cleansing	Data Validation
System Recovery & Data Cleansing	Data Verification

Training & Education

Access Management	Training Services for Access Management
Anti Spam Solutions	Training Services for Anti Spam Solutions
Anti Virus/Worm	Training Services for Anti Virus/Worm
Application Code Security	Training Services for Application Security
Business Continuity/Recovery	Training Services for Business Continuity/Recovery
Computer Forensics	Training Services for Computer Forensics
Content Filtering & Monitoring	Training Services for Content Filtering & Monitoring
Encryption/PKI/Digital Certificates	Training Services for Public Key Infrastructure
Firewalls	Training Services for Firewalls
Identity Management	Training Services for Identity Management
Intrusion Detection	Training Services for Intrusion Detection
Malware	Training Services for Malware
Messaging Security	Training Services for Messaging Security
Mobile Security /Device management	Training Services for Remote Access Management
Patch Management	Training Services for Patch Management
PC/Mobile/End Point Security	Training Services for PC/Mobile/End Point Security
Vulnerability Assessment	Training Services for Vulnerability Assessment
Wireless Security	Training Services for Wireless Security

Appendix I : Data Sources

21CT	3SDL Ltd	405Labs
41st Parameter	6Point6 Limited	6Scan
7Safe Ltd	Abeonet SA	Above Security
Absolute Software	Accellion	AccelOps
Accuvant	Acuity Risk Management	Acunetix
Adallom	Additional Country by country data sources	Advanced Content Services Inc (ADCS)
Advanced Systems International	Advent IM	Aegify
AfreecaTV Co Ltd (067160)	Agari	Agilience
AGS	AhnLab	AhnlabInc
AirbusGroup Ltd	Airport Operators' Association	AirTight
Akamai Technologies	Alert Enterprise	Alert Logic
AlgoSec	Alien Vault	AllClear ID
Allegro Software	Allgress	AlphaGuardian
AMA Research	Amarium Technologies Inc	Ambersail Ltd
American firearms Association	AnchorFree	Antiy Labs
AnubisNetworks	Apperion	Appicure Technologies Ltd
Applied Cyber Solutions	AppRiver	Arbor Networks
Area 1 Security	Arson Prevention Bureau	Arxan
Ascentor	ASD	AsgentInc
Aspect Security	ASPG	Association for Payment Clearing Services
Association of British Insurers	Assure Technical	AT&T Network Security
Auconet	Aujas	Authenticate
Autonomic Software	Avast	Avatier
Avecto	AVG Technologies	Aviation International
Avira	AXON Ghost Sentinel	Axway
B3System SA	BAE DETICA	BAE Systems
BAE Systems Applied Intelligence	BAE Systems Research	Banff Cyber
Barclay Simpson	Barclay Technologies Holding AG	Barracuda Networks
BART International	Bay Dynamics	Bayshore Networks
BDO LLP	Becrypt	Beijing VenustechInc
Beijing VRV Software Corp Ltd	Berkeley Varitronics Systems	Bespacific

Beyond Security	Biodata Information Technology AG	Bird & Bird LLP
Bit9 + Carbon Black	BitArmour	Bitdefender
Bitglass	Black Duck Software	Black Lotus
Blue Coat	Blue Lights Digital Ltd	Blue Sun Media Inc
Bluedon Information Safe Technology Co Ltd	Blueliv	Boldon James
Booz Allen	borwell	Bradford Networks
Brainloop	Brainzsquare	Breakingpoint Ltd
BRI - Business Risk Intelligence	Brinqa	British Airport Services and Equipment Assoc
British Approval for Fire Equipment	British Retail Consortium (BRC)	BSIA
BT	BT Security	Bugcrowd
Bullzi Security Inc	Bwise	C2B2
C3IA Solutions	CA Technologies	CAaNES
CACI	Cambridge Intelligence	Card Watch
Carnegie Mellon Software Engineering Institute	Caspida	Catbird
Cavirin	CBEMA	CBR
CDEX Inc	Cecurity.com	Celestix
CenterTools Software	Centrify	Centripetal
CenturyLink	CertainSafe	Charlton Networks
Check Point Software	Checkmarx	China Mulans Nano Technology Corp Ltd
CIA	Cienaga Systems	Cigital
Cimcor	CipherCloud	Cisco Systems Inc
Citicus	Citrix	Clearswift
Clearwater Compliance	Clef	Click Security
CloudHASH Security	CloudLink	CloudLock
CloudPassage	Coalfire	Code Dx
Code42	Codenomicon	Cognosec GmbH
Collective Software	Com-Guard.com Inc	Commissum
Community Care	Computer Sciences Corporation	Confederation of European Aerospace Societies (CEAS)
Confer	Consumers Defence Association.	ContentKeeper
Context Information Security Ltd	Contrast Security	Core Security
Corero Network Security PLC	CoSoSys	CounterTack
Courion	Coverity	CrowdStrike
Crypteia Networks	Cryptomathic	Cryptovision

Cryptzone	CSC	Cyactive
Cyber Crime Investigation	Cyber Operations Inc	Cybersecurity Associates
Cybersecurity Canada	Cybera	CyberArc
CyberDefender Corp	Cyberis Ltd	CyFIR
Cylance	CYREN	Damballa
Daon	Darktrace	Data monitor
DATASHIELD	DB Networks	DBAppSecurity
DeepNines	Deep-Secure	Defence Intelligence
Defence Manufacturers Association	Defense Point Security	Deja vu Security
Dell SecureWorks	Deloitte LLP	Delta ID
DEMA	Denim Group	Designing Out Crime Association (DOCA)
DeviceLock	DFLabs	DigiCert
Digital Arts Inc	Digital Assurance Consulting Ltd	Digital Defense
Digital Guardian	Digital Info Security Co	Digital Shadows
Digital Shadows Ltd	Dionach Ltd	Distil Networks
Domain Tools	D-RisQ	Druva
Duo Security	E C Council USA	EADS
Eagle Eye Networks	Earthport PLC	Eastcompeace Smart Card Co Ltd
Easy Solutions	ECSC Ltd	EdgeWave
Eid Passport	Elastica	E-Monee.com Inc
ENCODE	Encription Limited	Endace Ltd
Endgame	Enforcive	Entersekt
Entrust	ePlus Security	ERPScan
eSentire	ESET	ESNC
Euro monitor	European Regions Airline Association	Evident.IO
Exabeam	Exercise3	Exobox Technologies Corp
Exonar Limited	Extol MSC Bhd	F5
FARA	Farmwatch Limited	Farsight Security
Fasoo	Federation of Drug and Alcohol Professionals (FDAP)	FEMA
Ferris Research	Finmeccanica UK Limited	Fire and Security Association
FireEye Inc (FEYE)	FireMon	Forecast International
Forensic Innovations	ForeScout	ForgeRock
Forrester Research	Fortinet Inc	Fortscale
Forum Systems	FoxT	Freight Transport Association (FTA)

Frost & Sullivan	Frescoers	F-Secure OYJ
Fulcrum Biometrics	Future Tense Central	Futurex
Gartner	Gemalto	Gemalto NV
GenemenInc (GNMN)	General Dynamics Corporation	GFI
GhostMail	Gibio Co Ltd	Gigamon
Gigya	GiveADay.co.uk	Glimmerglass
Globalscape	GlobalSign	Good
Google	Gotham Digital Science	Greenfield Computers
Greenleaf Technologies Corp	GreenSQL	GreyCastle Security
Grid 32 Security	Groundworks Technologies	Guardian Analytics
GuardiCore	GuidePoint Security	GuruCul
Hangzhou Shunwang Technology Co Ltd	HansolNexG Co Ltd (081970)	Harris
Haystax	Hedgehog Security Ltd	Herjavec Group
Herne Hill Consulting Ltd	Hewlett Packard Company	Hex Security Limited
Hexis	HID Global	highbeam
Hillstone Networks	Homeland Security Research	Hortonworks
Horus Security Consultancy	HP Information Security UK Ltd	Hyperion Gray
HyperSecur Corp	HyTrust	IASME Consortium
IBM	iboss	ICSPA
ID Experts	Identity Finder	Igloo Security Inc
IKANOW	Imperva	Imprivata
Indelible Data	Industry Research group	Infloblox
Info Express	Info4Security	Infocyte
InfoGard	INFOSEC	Infotechnics research
INITECH Co Ltd	InnovaSec	Innove
INSIDE Secure	Institute for Defense& Government Advancement (IDGA)	Integralis AG
Intel Security Group	Intellect UK	Intelliagg
IntelSecure	Intercede Group PLC	International Air Transport Association (IATA)
International Business Strategies	International Compliance Association (ICA)	International institutes of technology
International Universities	Intersect	Intrusion Inc
Ionic Security	IpasInc	irm
IRM PLC (Information Risk Management PLC)	IronKey	ISA Holdings Ltd
iSIGHT Partners	i-Sprint	IT Governance Ltd
IT Security Inc.	itWatch	Ixia
Jane's Information Group Ltd	JUMPSEC Ltd	Juniper Networks

Juniperresearch	Kaspersky Lab	Key Pasco
Keynote	KEYW	Klockwork
Krimmeni Technologies	Kroll	Kryptnostic
L-3 Communications Holdings	Lancop	LANDesk
Lastline	LaunchKey	Leidos
Lieberman Software	LIFARS	LIGATT Security International Inc
Light Cyber	Light Point Security	Link11
Linoma Software	Lockheed Martin Corporation	LockPath
LOGICA	LogRhythm	Lookingglass
Lookout	Lumension Security	Lynx Software Technologies
Malcovery Security	Malwarebytes	ManageEngine
Mandalorian Security Services	Mandiant	Marble Security
Market Research	MASS	MBD
MCSI	MDSec Consulting Ltd	Mega AS
Messageware	MetricStream	Microsoft
MicroStrategy	Mimecast	MindPoint Group
Minereye	Mint Technology Corp	Mobile Active Defense
Mobile Content Management Solutions Ltd	Mobile Vault Inc	MobileIron
Mobilityone Ltd	Mocana	Modulo
Monterey Technology Group	Morphick	MSI Reports Ltd
MTI Technology Ltd	MWR Infosecurity Ltd	Mycroft
NACOSS (National Approval Council Of Security Systems)	Napatech	National Community Safety Network (NCSN)
National Electrical Manufacturers Association (NEMA):	National Plant and Equipment Register Limited (TER)	NCC Group PLC
NEMA	Neoarenalnc (037340)	NetFort
NetIQ	NetScout	Netskope
Nettitude Ltd	Network Connections	Newmark Security PLC
Nexbis Ltd	NexDefense	NexG Co Ltd
Nice D&B Co Ltd	Nicstech Co Ltd	NokNok Labs
Norse	Northrop Grumman Corporation	Northrop Grumman UK
Nowcom Co Ltd	NowSecure	NS8 Corp
N-Stalker	NT OBJECTives	NTA Monitor Ltd
Ntrepid	NuData Security	Nuix
nwStor	Oberthur Technologies	Obrela Security Industries
Odyssey Technologies Ltd	Okta	Onapsis
OneLogin	ONSLOT Ltd	OnWire

OpenDNS	OPSWAT	OSPL
Osterman Research, Inc.	OullimElsesInc	outlier Security
Overland Storage Inc	Overlap Groupe	Ovum
Oxford Biochronometrics	PA Consulting Group	PacketSled
Paladion	Palo Alto Networks	Panda Security
Paraben	Patrior	Patron Systems Inc
PegasusBridge Finance Ltd Corporate	Pen Test Partners Consulting LLP	Penango
Pentura Ltd	Perspecsys	Perspective Risk Ltd
PGI Strontium Ltd	PGP	PhishLabs
Pindrop Security	Ping Identity	PivotMail
PivotPoint Security	PixAlert	pixicloud
PKWARE	Plantynet Co Ltd	Plimsoll
Portcullis Computer Security Ltd	Portnox	PortSwigger
Prelert	Prevalent Networks	PrimeKey Solutions
Privacy Analytics	PrivateCore	Procad SA
Procheckup Ltd	Promisec	Proofpoint
Protected Networks	Protectimus	Proteus Security
PUNCH	PWC	Pwnie Express
PyeongAhn Trading Inc	Q1 Labs	Qihoo 360 Technology Co Ltd
Qinetiq Ltd	Qosmos	QSGI Inc
Quality Guild	Qualys	QuintessenceLabs
Quotium	Radiant Logic	Radware
RahaxiInc	RandomStorm	Rapid7
Raytheon Company	Recorded Future	Red Canary
Red Lambda	RedOwl	RedSeal
Report Linker	ResearchandMarkets	Reservoir Labs
Resilient Systems	Reuters	Ripjar
Riscure	Risk Based Security	Risk I/O
RJD Technology Ltd	Road Haulage Association (RHA)	Rohde and Shwarz
root9B	RSA EMC	Rsam
RSD	S4E SA	Safe Net
SAIC	SailPoint	Saint Corporation
Sandettie	Sanitas Data Security	SDS
SEC-1 Ltd	SECFORCE Ltd	Seclore
Seclytics	SECNOLOGY	SecSign
SecuavailInc	SecuEra Technologies	Seculert
Secunet Security	Secunia	Secure Access Technologies

Secure Decisions	Secure Digital Inc	Secure Digital Solutions
Secure Fortress PLC	SecureAuth	Secured By Design (SBD)
Secured Services Inc	SecureLogix	Security Alliance Ltd
Security Compass	Security Industry Authority (SIA)	Security Park
Security Sales International (Brazil, Russia, China, India)	Security Systems and Alarms Inspection Board (SSAIB)	Securonix
Selex ES	Senetas Corp Ltd	Sensato
SensePost UK Ltd	SentinelOne	SENTRIX
SentryBay	Sera-Brynn	Seven Technologies Group Ltd
Shape Security	Siemens Government Technologies	Silent Circle
Silobreaker	SilverSky	Sirrix AG
Skybox Security	Skycure	Skyhigh Networks
Smoothwall	SMTP Inc	SnoopWall
SoftForum Co Ltd	Solarwinds	Soliton Systems KK
Solutionary / NTT	Sonatype	Sonic Wall
Soonr	Sophos	Sorinteq Limited
SourcefireInc	Spam Titan	Spector Soft
Spikes Security	Splunk	Sqrrl
StillSecure	Stonesoft OYJ	Strikeforce Technologies Inc
StrongAuth	STS Group	Sumo Logic
Sungard AS	Surevine Limited	SurfRight
SurfWatch Labs	Swivel Secure	Sword and Shield
Syferlock	Symantec Corp	Synack
Syncplicity	SynerComm	Syntegrity Networks
Sypris	SysAid	Taia Global
Tanium	Tapestry Technologies	TargetProof
TechGuard	Technical Communications Corp	Tectia OYJ
Telecommunications UK Fraud Forum	TeleSign	Templar Shield
Tenable Network Security	TeraDact	Tevora
Thales France	Thales Group	Thales UK Ltd
The Association for Biometrics	The Association of Security Consultants	The Atlantic Alliance of Aerospace and Defence Associations.
The Bharat Corporation	The Boeing Company	The British Airport Services & Equipment Association
The British Fire Protection Systems Association	The British Security Industry Association	The European Biometrics Forum

The Fire Protection Association	The Friendly Nerd	The Institute of Security Management
The International Institute of Security	The International Professional Security Association	The International Security Industry Organization
The Master Locksmiths Association	The National Fire Protection Association	The National Security Inspectorate
The Networking People Ltd	The Police Federation Of England and Wales	The Radicati Group Inc
The Security Industry Authority	The Security Industry Training Organisation	The Security Institute
	Thomson Reuters	Threat Stack
ThreatConnect	ThreatMetrix	ThreatSim
ThreatStream	Thycotic Software	Timo E&M Co Ltd
Timo Technology Co Ltd	Titania	TMC Security Solutions Ltd
Transol Corp Ltd	TrapX Security	Trend Micro Inc
Trend Micro Inc/Japan	Tripwire	Triumfant
TrulyProtect	TRUSTe	TrustedSec
Trustwave UK Ltd	Unisys	Universe Group PLC
University of Maryland	Untangle	UtimacoSafeware AG
Vanguard Integrity Professionals	vArmour	Varonis
VASCO Data Security	Vaultive	Vectra Networks
VEEDog	Vehicle Security Installation Board	Venafi
Venture Cybersecurity	Veracode	Verint
Veris Group	VeriSign Inc	VERISIGN JAPAN KK
Verizon Business Security Solutions	Vidder	Viewfinity
Virtru	Virtual Forge	Visiongain
VisiTrend	Vistrionix	VivoSecurity
Vkansee	V-Key	VMware
Voltage Security	Vormetric	VSS Monitoring
VSUS Technologies Inc	VU Security	Wandera
WatchDox	WatchGuard	Waterfall
Wave Systems	Webroot	Websense
Wetstone Technologies	White Ops	WhiteHat Security
WildPackets	Win Magic	Windtalker Security
wolfSSL	Wombat Security Technologies	Wontok
WWPass	Xbridge	Xceedium
XO Communications	Xyone Security	Your Internet Defender Inc
Zenedge	Zentek Forensics Ltd	ZeroFOX

Ziften	ZixCorp	Zscaler
Zybert Computing Ltd		

Appendix J : List of Acronyms

This chapter includes the list of acronyms used in the study.

Table 45 : List of acronyms of the 28 Member States

Country	Acronym
Austria	AT
Belgium	BE
Bulgaria	BG
Cyprus	CY
Czech Republic	CZ
Germany	DE
Denmark	DK
Estonia	EE
Spain	ES
Finland	FI
France	FR
United Kingdom	UK
Greece	GR
Croatia	HR
Hungary	HU
Ireland	IE
Italy	IT
Lithuania	LT
Latvia	LV
Malta	MT
Member State(s)	MS(s)
The Netherlands	NL
Poland	PL
Portugal	PT
Romania	RO
Sweden	SE
Slovenia	SI
Slovakia	SK

Appendix K : Top 500 Global Cybersecurity Companies by growth (alphabetical order)

European companies are marked in **Red**.

Company	Cybersecurity Sector	Corporate HQ
A10 Networks	DDoS Cyber Attack Protection	San Jose, CA
Absolute	Mobile Device Management & Security	Austin TX
Accellion	Secure Mobile File Sharing	Palo Alto CA
Accenture	Enterprise Security Strategy	New York City NY
Acunetix	Web Vulnerability Scanner	Kingston Upon Thames, UK
Agari	Real-Time Cyberthreat Detection	San Mateo CA
AhnLab	Internet Security Solutions	Gyeonggi-do, South Korea
AIRBUS Cybersecurity	Cyber Threat Defense	Paris, France
Akamai Technologies	Secure Cloud & Mobile Computing	Cambridge MA
Alert Logic	Security-as-a-Service Solutions	Houston TX
AlgoSec	Security Policy Management	Boston MA
AlienVault	Threat Detection & Response	San Mateo CA
AlClear ID	Identity Protection Service	Austin TX
AnchorFree	End-to-End Information Security	Mountain View CA
Anodot	Automated Anomaly Detection	Ra'annana, Israel
Anomali	Threat Intelligence Platform	Redwood City CA
Antiy Labs	Anti-Virus Engine & Solution	Beijing, China
Appdome	Mobile App Security	Tel-Aviv, Israel
Apperion	Mobile App Security	Boston MA
Applied Risk	Industrial Cybersecurity	Amsterdam, The Netherlands
Appthority	Mobile App Security	San Francisco CA
Arbor Networks	DDoS Attack & Threat Protection	Burlington MA
Argus Cyber Security	Automotive Cybersecurity	Tel Aviv, Israel
Arxan	Application Security Products	Bethesda MD
Assured Enterprises	Managed IT Security Services	Austin TX
AT&T Network Security	Managed Security & Consulting	Bedminster NJ
AttackIQ	Security Infrastructure Testing	San Diego CA
aurionPro	Enterprise Security Solutions	Mumbai, India
Auth0	Identity for Developers	Bellevue WA
Avanan	SaaS Security Platform	New York City NY
Avast	Anti-Virus Protection for MACs	Prague, Czech Republic
Avecto	Endpoint Security Software	Cheshire, UK
Avira	Antivirus & IT Security Software	Munich, Germany
Axway	Secure Email & File Sharing	San Jose CA
BAE Systems	Cybersecurity Risk Management	Surrey, UK
Baffle	Data Security & Encryption	Santa Clara CA
Balabit	Privileged Account Security	Senningerberg, Luxembourg
BankVault	Anti-Hacking Software	Perth, Australia
Barracuda Networks	Email & Web Security Appliances	Campbell CA
Bastille Networks	Internet of Radios Security	San Francisco CA
Bay Dynamics	Information Risk Intelligence	San Francisco CA
Bayshore Networks	Internet of Things Security	New York City NY
Becrypt	Mobile Device & Data Security	London, UK
Behaviosec	Behavioral Biometrics	Stockholm, Sweden
BeyondTrust	Privileged Access Management	Phoenix AZ
Biocatch	Behavioral Biometrics	New York City NY
Bio-key	Fingerprint Biometric Identification	Wall NJ
BIOWATCH	Wristwatch Vein Authentication	Martigny, Switzerland
Bitdefender	Anti-Virus & Endpoint Security	Bucharest, Romania
Bitglass	Data Protection & Breach Discovery	Campbell CA
BitSight	Security Rating Platform	Cambridge MA
Black Duck Software	Open Source Software Security	Burlington MA
BlackBerry	Mobile & Data Security	Waterloo, Canada
BlackStratus	Security & Compliance Management	Piscataway NJ
BlueCat	Secure DNS Services	Toronto, Canada
Blueliv	Cyber Threat Analysis	Barcelona, Spain
Bomgar	Identity & Access Management	Ridgeland MS
Booz Allen	Cybersecurity Solutions & Services	New York City NY
Bradford Networks	Network Security Automation	Boston MA
Brainloop	Secure Document Management	Munich, Germany
Bromium	Endpoint Security	Cupertino CA
BSI Cybersecurity	Cybersecurity Services	Dublin, Ireland

Company	Cybersecurity Sector	Corporate HQ
BT	Security & Risk Management Solutions	London, UK
Bugcrowd	Crowd Sourced Security Testing	San Francisco CA
Bwise	IT Governance, Risk & Compliance	Rosmalen, The Netherlands
CA Technologies	Identity & Access Management	New York City NY
CACI	Intelligence, Defense & Federal Security	Ballston VA
Carbon Black	Endpoint & Server Security Platform	Waltham MA
Cato Networks	Cloud Network Security	Tel-Aviv, Israel
CBI	IT Risk Management	Ferndale MI
Cellebrite	Mobile Forensics Technology	Petah Tikva, Israel
Centrify	Unified Identity Management	Santa Clara CA
Centripetal	Cyber Threat Intelligence	Herndon VA
Check Point Software	Unified Threat Management	Tel Aviv, Israel
Checkmarx	Software Development Security	Tel-Aviv, Israel
Cimcor	Governance, Risk & Compliance	Chicago IL
CipherCloud	Cloud Visibility & Data Protection	San Jose CA
Cisco	Threat Protection & Network Security	San Jose CA
Citrix	Secure Remote Access	Fort Lauderdale FL
Claroty	OT Security Platform	Tel-Aviv, Israel
Clavister	Network Security	Ornskoldsvik, Sweden
Clearswift	Data Loss Prevention	Reading, UK
Clearwater Compliance	Risk Management and Compliance	Nashville TN
CloudFlare	Web Performance & Security	San Francisco CA
CloudPassage	Cloud Infrastructure Security	San Francisco CA
Coalfire	Cyber Risk Management	Louisville CO
Cobalt Labs	Penetration Testing & Bug Bounty	Paris, France
Code Dx	Software Vulnerability Management	Northport NY
Code42	Data Management & Protection	Minneapolis MN
Comodo	Endpoint & Internet Security	Clifton NJ
Continuum GRC	IT Governance, Risk & Compliance	Scottsdale AZ
Contrast Security	Application Security Software	Palo Alto CA
Core Security	Identity & Access Management	Westborough MA
Corero	DDoS Defense & Security Solutions	Hudson MA
CoroNet	Enterprise Commjacking	Be'e Sheva, Israel
CounterTack	Real Time Attack Intelligence	Waltham MA
Cronus Cyber Technologies	Continuous Penetration Testing	Haifa, Israel
CrowdStrike	Breach & Endpoint Protection	Irvine CA
Cryptomathic	Cloud, Mobile & Network Security	Aarhus, Denmark
Cryptzone	File & Data Encryption Platform	Waltham MA
CSC	IT Security Services	Falls Church VA
Cyber adAPT	Network & Mobile Security	Half Moon Bay CA
CyberArk	Cyber Threat Protection	Petach-Tikva, Israel
Cyberbit	SOC Automation & Orchestration	Ra'anana, Israel
Cybereason	Endpoint Protection & Hunting Engine	Boston MA
CyberX	Industrial Network Security	Tel-Aviv, Israel
Cybric	Security-as-a-Service	Boston MA
Cyence	Cyber Risk Modeling	San Mateo CA
CyFIR	Digital Forensics & e-Discovery	Manassas VA
Cylance	Cyber Threat Intelligence	Irvine CA
Cymmetria	Enterprise Cyber Deception	Tel Aviv, Israel
Cyphort	Malware Detection & Prevention	Santa Clara CA
CYREN	Web, Email & Mobile Security	McLean VA
Daon	Identity Assurance & Biometrics	Washington DC
Darktrace	Cyber Threat Prevention	London, UK
Dataguise	Big Data Security	Fremont CA
DB Networks	Intelligent Continuous Monitoring	Fremont CA
DBAPPSecurity	Database & Web Application Security	Fremont CA
Deloitte	Global Risk Management Services	New York City NY
Denim Group	Secure Software Development Services	San Antonio TX
DeviceLock	Endpoint Data Leak Prevention	San Ramon CA
DFLabs	Automated Incident & Breach Response	Lombardy, Italy
DigiCert	Digital Certificate Provider	Lehi UT
Digital Arts	Web & Email Filtering Software	Tokyo, Japan

Company	Cybersecurity Sector	Corporate HQ
Digital Defense	Managed Security Risk Assessment	San Antonio TX
Digital Guardian	Data Loss Prevention	Waltham MA
Digital Shadows	Cyber Intelligence Feeds	East Sussex, UK
Distil Networks	Malicious Bot Detection & Prevention	Arlington VA
DomainTools	Cybercrime Investigation & Prevention	Seattle WA
Dragos Security	Industrial Control Systems Security	San Antonio TX
DriveLock SE	Endpoint Security Solutions	Munich, Germany
Druva	Endpoint Data Protection & Governance	Sunnyvale CA
Duo Security	Cloud Based Two-Factor Authentication	Ann Arbor MI
E8 Security	Agent less Security Intelligence	Redwood City CA
EastWind Networks	Breach Detection	Salt Lake City UT
Easy Solutions	Electronic Fraud Protection	Doral FL
Eclectic IQ	Threat Intelligence Analysis	Amsterdam, The Netherlands
EdgeWave	Military Grade Internet Security	San Diego CA
Elastic	Open Source Cloud Security	Mountain View CA
ENCODE	IT Security & Digital Risk Management	Athens, Greece
Endgame	Security Intelligence & Analytics	Arlington VA
enSilo	Exfiltration Prevention Platform	San Francisco CA
Entersekt	Authentication & Fraud Protection for Banks	Stellenbosch, South Africa
Entrust	Authentication & Identity Assurance	Dallas TX
ePlus Security	Infosecurity Services & Products	Herndon VA
ERPScan	SAP Security Solutions	Palo Alto CA
eSentire	Threat Detection & Prevention	Cambridge, Canada
ESET	Multi-Device End Point Security	Bratislava, Slovakia
ESNC	Security for SAP Applications	Munich, Germany
EverCompliant	Transaction Laundering Prevention	Tel-Aviv, Israel
Evident.io	Cloud Security for AWS	Dublin CA
Exabeam	User Behavior Intelligence	San Mateo CA
EY	Cybersecurity Consulting & Advisory	New York City NY
F5	Cloud & Data Center Security	Seattle WA
Factom	Blockchain Technology	Austin TX
Fasoo	Data & Software Security	Seoul, South Korea
FFRI, Inc.	Cybersecurity R&D	Tokyo, Japan
Fhoosh	Data Security & Encryption	La Jolla CA
Fidelis Cybersecurity	Cyber Attack Defense	Waltham MA
Fingerprint Cards AB	Fingerprint Biometrics	Gothenburg, Sweden
Finjan Holdings	Cybersecurity IP Licensing	East Palo Alto CA
FireEye	Advanced Threat Protection	Milpitas CA
Fireglass	Enterprise Network Security	Tel Aviv, Israel
FireMon	Network Security Management	Overland Park KS
Flexera Software	Software Vulnerability Management	Itasca IL
Forcepoint	Insider, Cloud & Network Security	Austin TX
ForeScout	Network Security & Access Control	Campbell CA
ForgeRock	Open Source Identity Management	San Francisco CA
Fortinet	Enterprise Security Solutions	Sunnyvale CA
Fortscale	Big Data Cyber Analytics	San Francisco CA
Forum Systems	Secure Cloud Gateway	Newton MA
Fox Technologies	Network Security & Assess Management	San Jose CA
F-Secure	Internet Security for All Devices	Helsinki, Finland
Future Tense Central	Phone & Mobile Device Security	Opelika AL
Gemalto	Digital Identity Management	Meudon Cedex, France
General Dynamics	IT Cybersecurity Solutions	Fairfax VA
GFI	Email & Network Security Solutions	Durham NC
Gigamon	Data Center & Cloud Security	Milpitas CA
GigaTrust	Secure Content Collaboration	Herndon VA
Globalscape	Secure File Transfer	San Antonio TX
GlobalSign	Authentication & Identity Service Provider	Portsmouth NH
GM Security Technologies	Managed Security Services	San Juan, Puerto Rico
Good Harbor	Cyber Risk Advisory	Washington DC
Google	Project Shield for News Sites	Mountain View CA
GrammaTech	Software Code Security	Ithaca NY
GreatHorn	Automated Threat Detection	Belmont MA

Company	Cybersecurity Sector	Corporate HQ
GreyCastle Security	Information Security Consulting	Troy NY
Guardian Analytics	Behavioral Analytics for Fraud Prevention	Mountain View CA
GuardiCore	Data Center Security	Tel-Aviv, Israel
Guidance Software	Endpoint Data Security	Pasadena CA
GuidePoint Security	Information Security Services	Reston VA
GuruCul	Security Risk Intelligence	Los Angeles CA
HackerOne	Bug Bounty Platform	San Francisco CA
HanSight	Big Data Security	Beijing, China
Harris	Cybersecurity for Federal Agencies	Melbourne FL
Haystax	Advanced Threat Analytics	McLean VA
Herjavec Group	Information Security Services	Toronto, Canada
HID Global	Secure Identity Technology	Austin TX
Hillstone Networks	Data Analytics Firewall Protection	Sunnyvale CA
Hortonworks	Big Data Security Analytics	Santa Clara CA
HPE	Cybersecurity for Public Sector & Defense	Palo Alto CA
HYPR	Biometric Security	New York City NY
HyTrust	Cloud Security Automation	Mountain View CA
IBM Security	Enterprise IT Security Solutions	Waltham MA
iboss	APT Defense, Web & Mobile Security	San Diego CA
Illumio	Adaptive Security Platform	Sunnyvale CA
Illusive Networks	Deception Technology	Tel-Aviv, Israel
Immunisweb	Continuous & On-Demand Web Security	Geneva, Switzerland
Imperva	Data & Applications Security	Redwood Shores CA
Imprivata	Security for Healthcare Providers	Lexington MA
Indegy	Industrial Systems Cybersecurity	Tel Aviv, Israel
Infoblox	Automated Network Control & Security	Santa Clara CA
Infocyte	Intrusion Assessment Platform	San Antonio TX
INFOSIGHT	Cyber Advisory & Training	Miami Lakes FL
Innové	Managed Security Services	Boerne TX
INSIDE Secure	Smartphone & Mobile Device Security	Aix-en-Provence, France
Inspired eLearning	Security Awareness Training	San Antonio TX
Intel Security Group	Anti-Virus, Malware & Threat Protection	Santa Clara CA
InteliSecure	Network Security Services	Greenwood Village CO
Intersect	Threat Detection & Prevention	Ottawa, Canada
Intralinks	Cloud Security & Compliance	New York City NY
Ionic Security	Data Privacy & Protection	Atlanta GA
IronNet Cybersecurity	Threat Detection & Mitigation	Fulton MD
IRONSCALES	Automated Phishing Response	Ra'annana, Israel
i-Sprint Innovations	Identity & Access Management	Chai Chee, Singapore
Israel Aerospace Industries	End-to-End Cybersecurity	Tel-Aviv, Israel
Ivanti	Enterprise Endpoint Security	South Jordan UT
Ixia	Network Visibility, Security & Testing	Calabasas CA
Juniper Networks	Threat Intelligence & Network Security	Sunnyvale CA
Kaspersky Lab	Malware & Anti-Virus Solutions	Moscow, Russia
Kenna	Vulnerability Threat Management	Chicago IL
Keypassco	Multi-Factor Authentication	Gothenburg, Sweden
KEYW	Cyber Defense & Digital Forensics	Hanover MD
KnowBe4	Security Awareness Training	Clearwater FL
KPMG	Cyber Risk Management	London, UK
Kroll	Cybersecurity Services	New York City NY
Kudelski Security	Managed Security Services	Lausanne, Switzerland
L-3	National Security Solutions	Reston VA
lastline	Security Breach Detection	Redwood City CA
Leidos	Anti-Terrorism & Homeland Security	Reston VA
Level 3	Network & Managed Security Services	Broomfield CO
Lexumo	Open Source Security	Cambridge MA
Lieberman Software	Privileged Identity Management	Los Angeles CA
LIFARS	Digital Forensics & Cyber Intelligence	New York City NY
LifeLock	Identity Theft Detection	Tempe AZ
Link11	DDoS Mitigation Solution Provider	Frankfurt, Germany
Linoma Software	File Security & Data Encryption	Ashland NE
Lockheed Martin	Cybersecurity Solutions & Services	Bethesda MD

Company	Cybersecurity Sector	Corporate HQ
LockPath	IT Governance, Risk & Compliance	Overland Park KS
LogRhythm	Log Management & Security Analytics	Boulder CO
LookingGlass	Cyber Threat Intelligence Management	Arlington VA
Lookout	Mobile Security for Android & iOS Apps	San Francisco CA
Lynx Software Technologies	Real Time Threat Detection	San Jose CA
Magnet Forensics	Digital Forensics Tools	Waterloo, Canada
MailControl	Anti-Spymail Solutions	Chicago IL
Malwarebytes	Malware Detection & Protection	San Jose CA
Masergy	Managed Security Services	London, UK
MedCrypt	Medical Device Security	Encinitas CA
Menlo Security	Malware Detection & Protection	Menlo Park CA
MetricStream	IT Governance, Risk & Compliance	Palo Alto CA
Microsoft	Datacenter to Endpoint Protection	Redmond WA
MicroStrategy	Mobile Identity Platform	Tysons Corner VA
Mimecast	Email Security	Watertown MA
MindPoint Group	IT Security Solutions	Springfield VA
Mitek	Mobile Identity Verification	San Diego CA
Mitnick Security	Penetration Testing & Training	Las Vegas NV
MobileIron	Mobile Device & App Security	Mountain View CA
Mocana	Mobile & Internet of Things Security	San Francisco CA
Mojo Networks	Wireless Intrusion Prevention	Mountain View CA
Morphick	Advanced Threat Protection Services	Cincinnati OH
Mosaic 451	Cyber Security Services	Phoenix AZ
MPrest	Building & Control Systems Security	Petach Tikva, Israel
NCC Group	Information Assurance Services	Manchester, UK
N-Dimension	Managed Security Services	Richmond Hill, Canada
Nehemiah Security	Cyber Threat Detection	Tyson's Corner VA
NetFort	Network Security Monitoring	Galway, Ireland
NetIQ	Security Management & Intelligence	Houston TX
NetScout	Situational Awareness & Incident Response	Westford MA
Netskope	Cloud Application Security	Los Altos CA
Netwrix	Hybrid Cloud Security	Irvine CA
NexDefense	Automation & Control Systems Security	Atlanta GA
Nexthink	Anomaly & Behavior Analytics	Prilly, Switzerland
neXus	PKI, Access & Identity Management	Hagersten, Sweden
Nexusguard	Cloud Enabled DDoS Mitigation	Hong Kong
NNT	IT Security & Compliance	St. Albans, UK
Nok Nok Labs	Unified Authentication Infrastructure	Palo Alto CA
Northrop Grumman	Cyber & Homeland Security Services	McLean VA
Novetta	Cyber Security Analytics	McLean VA
NowSecure	Mobile Device & App Security	Oak Park IL
Nozomi Networks	Industrial Control Security	Mendrisio, Switzerland
NSFOCUS	DDoS Mitigation & Protection	Hong Kong
Ntrepid	Secure Network & Online Computing	Herndon VA
NTT Security	Managed Security Services Provider	Omaha NE
NXT-ID	Biometric Security Solutions	Oxford CT
Oberthur Technologies	Digital Security for Mobility	Chantilly VA
Observable Networks	Endpoint Modeling	St. Louis MO
Okta	Enterprise Identity Management	San Francisco CA
Onapsis	ERP Cybersecurity Solutions	Boston MA
OneLogin	Enterprise Identity Management	San Francisco CA
OPSWAT	IT Infrastructure Security & Management	San Francisco CA
Optiv	Information Security Services	Denver CO
Oracle	Identity Security Operations Center	Redwood City CA
Osirium	Privileged User Management	Berkshire, UK
Paladion	Cybersecurity Testing & Monitoring	Bangalore, India
Palantir	Cybersecurity Analytics and Cyber Fraud	Palo Alto CA
Palo Alto Networks	Threat Detection & Prevention	Santa Clara CA
Panda Security	Anti-Virus & Internet Security Software	Bilbao, Spain
Panopticon Labs	Online Game Security	Columbus OH
Paraben	Digital Forensics & Data Recovery	Ashburn VA
Phantom	Security Automation & Orchestration	Palo Alto CA

Company	Cybersecurity Sector	Corporate HQ
Phirelight	Cyber Threat Intelligence	Ottawa, Canada
PhishLabs	Cybercrime Detection & Prevention	Charleston SC
PhishMe	Phishing Attack Defense	Leesburg VA
Pindrop Security	Phone-Based Fraud Prevention	Atlanta GA
Ping Identity	Identity & Access Management Platform	Denver CO
PKWARE	Data Encryption & Security	Milwaukee WI
PortSwigger	Web Application Security Testing	Knutsford, UK
Praetorian	Cybersecurity Consulting & Services	Austin TX
Precise Biometrics AB	Mobile Identity Authentication	Lund, Sweden
Prevalent Networks	Third-Party Risk Management	Warren NJ
PrimeKey Solutions	PKI & Digital Signature Solutions	Solna, Sweden
Proficio	Managed Security Services	Carlsbad CA
Promisec	Endpoint Security Intelligence	Needham MA
Proofpoint	Security-as-a-Service	Sunnyvale CA
Protegrity	Enterprise Data Security	Stamford CT
Protenus	Health Data Security	Baltimore MD
Prot-On	Encryption & File Security	Madrid, Spain
PulseSecure	Enterprise Mobile Security	San Jose CA
PwC	Cybersecurity Consulting & Advisory	London, UK
Pwnie Express	Enterprise Threat Detection	Boston MA
Qihoo 360	Internet & Mobile Security	Beijing, China
QinetiQ	Cyber Consulting & Services	Farnborough, UK
Qosmos	Real-Time Data Security	Paris, France
QuadMetrics	Cyber Risk Measurement	Ann Arbor MI
Qualys	Cloud Security & Compliance	Redwood City CA
Quann	Managed Security Services	Republic of Singapore
Quick Heal Technologies	IT Security Solutions	Maharashtra, India
QuintessenceLabs	Data Security Technology	Deakin, Australia
Radiant Logic	Enterprise Identity Management	Novato CA
Radware	Application Security & Delivery	Tel Aviv Israel
Rapid7	Security Data & Analytics Solution	Boston MA
Raytheon Cyber	Cyber Security Services	Waltham MA
Recorded Future	Real-Time Threat Intelligence	Somerville MA
Red Canary	Threat Detection & Response	Denver CO
RedOwl	Data Analytics for Risk & Compliance	Baltimore MD
RedSeal	Cybersecurity Analytics	Sunnyvale CA
Reservoir Labs	Real-Time Threat Visibility	New York City NY
Resolver	GRC & Incident Management	Toronto, Canada
Ridge-Schmidt Cyber	Executive Cyber Solutions	Washington DC
Risk Based Security	Cyber Risk Analytics	Richmond VA
RiskIQ	Digital Threat Management	San Francisco CA
RiskSense	Cyber Risk Management	Albuquerque NM
RiskVision	Integrated Risk Management	Sunnyvale CA
Rogue Wave Software	Source Code Analysis	Louisville CO
Rohde & Schwarz Cybersecurity	Encryption & IT Security	Munich, Germany
root9B Holdings, Inc.	HUNT & Cyber Operations	Colorado Springs CO
RSA	Intelligence Driven Security	Bedford MA
Rsam	IT Governance, Risk & Compliance	Secaucus NJ
Rubicon Labs	IoT Security & Identity	San Francisco CA
SafeBreach	Data Breach Protection	Tel Aviv, Israel
SAIC	Cybersecurity Professional Services	McLean VA
SailPoint	Identity & Access Management	Austin TX
Saint Corporation	IT Security Risk & Compliance	Bethesda MD
SaltDNA	Enterprise Mobile Security	Belfast, UK
Sangfor	Network Security & Optimization	Shenzhen, China
SAS Institute	Fraud & Security Analytics	Cary NC
Saviynt	Cloud Identity Management	Los Angeles CA
Savius	Network Analytics & Forensics	Walnut Creek CA
SDS	Multi-Platform Encryption	Minneapolis MN
SECDO	Incident Investigation & Response	Ra'annana, Israel
Seclore	Digital Rights Management	Mumbai, India
SecuAvail	MSSP & Log Analysis	Osaka, Japan

Company	Cybersecurity Sector	Corporate HQ
Secure Digital Solutions	Infosecurity Consulting Services	Saint Louis Park MN
SecureAuth	Secure Access Control	Irvine CA
SecuredTouch	Mobile Identity Verification	Tel-Aviv, Israel
SecureKey	Identity & Authentication Solutions	Toronto, Canada
SecureMySocial	Social Media Security	New York City NY
SecureRF	IoT Security	Shelton CT
SecureStrux	Compliance & Vulnerability Management	Arlington VA
SecureWorks	Managed Security Services	Atlanta GA
Security Compass	Software Development Security	Toronto, Canada
Security Innovation	Application Risk Management	Wilmington MA
SecurityScorecard	Security Ratings & Assessments	New York City NY
Securonix	Security Analytics Technology	Los Angeles CA
Senrio	Enterprise IoT Security	Portland OR
SentinelOne	Endpoint Protection Platform	Mountain View CA
SentryBay	PC, Mobile & IoT Security	London, UK
Sentryo	Industrial IoT Security	Villeurbanne, France
Sera-Brynn	Cyber Risk Management	Suffolk VA
SEWORKS	Mobile App Security	Seoul, South Korea
Shape Security	Website Attack Prevention	Mountain View CA
Siemens Government Technologies	Cybersecurity for Federal Government	Arlington VA
Siemplify	Security Orchestration & Incident Response	New York City NY
Signifyd	e-Fraud Detection & Prevention	San Jose CA
Silent Circle	Enterprise Privacy Platform	Geneva, Switzerland
Silverskin	Penetration Testing & Training	Helsinki, Finland
SimpliflDed	Multi Platform Biometrics	Madison WI
Sixgill	Dark Web Intelligence	Netanya, Israel
Skybox Security	Risk Analytics for Cybersecurity	San Jose CA
Skycure	Mobile Device Protection	Tel Aviv, Israel
Skyhigh Networks	Cloud Access Security	Cupertino CA
Skyport Systems	Application Security	Mountain View CA
Smoothwall	Unified Threat Management	Leeds, UK
SnoopWall	Mobile Device Security	Nashua NH
Socure	Social Biometrics	New York City NY
Sonatype	Enterprise Application Security	Fulton MD
SonicWall	Network & Mobile Security	Santa Clara CA
Sophos	Anti-Virus & Malware Protection	Abingdon, UK
Spam Titan	Email Security Appliances	Galway, Ireland
SparkCognition	Cognitive Security	Austin TX
Spirion	Data Discovery & Protection	New York City NY
Splunk	Big Data Security	San Francisco CA
Sqrrl	Cyber Defense Analytics	Cambridge MA
SSH Communications	Privileged Access Control	Helsinki, Finland
Star Lab	Embedded Security	Washington DC
StrongAuth	Enterprise Key Management Infrastructure	Sunnyvale CA
Stroz Friedberg	Cyber Intelligence & Risk Management	New York City NY
Sumo Logic	Big Data Security Analytics	Redwood City CA
Sungard AS	Managed Security Services	Wayne PA
Sure ID	High-Assurance Identity Management	Hillsboro OR
SurfWatch Labs	Cyber Risk Intelligence Analytics	Sterling VA
Swimlane	Security Automation & Orchestration	Louisville CO
Swivel Secure	Risk Based Authentication	Wetherby, UK
Sword & Shield	Managed Security Services	Knoxville TN
Symantec	Endpoint, Cloud & Mobile Security	Mountain View CA
Synack	Crowd Security Intelligence	Redwood City CA
Syncplicity	Secure File Storage	Santa Clara CA
Synopsys	Software Integrity Platform	Mountain View CA
Tanium	Security & Systems Management	Emeryville CA
Tapestry Technologies	Cyber Defense Services	Chambersburg PA
TeleSign	Mobile Identity Verification	Marina Del Rey CA
Telos Corporation	Risk Management & Compliance	Ashburn VA
Tempered Networks	Network Security	Seattle WA
Tenable Network Security	Vulnerability Scanning	Columbia MD

Company	Cybersecurity Sector	Corporate HQ
Thales	Secure IT Solutions	Paris, France
The Chertoff Group	Global Risk Management	Washington DC
ThetaRay	Big Data Security Analytics	Hod HaSharon, Israel
Threat Stack	Cloud Infrastructure Security	Boston MA
ThreatConnect	Cyber Threat Intelligence Platform	Arlington VA
ThreatMetrix	Online & Mobile Fraud Protection	San Jose CA
ThreatQuotient	Threat Intelligence Platform	Reston VA
Thycotic	Privileged Account Management	Washington DC
TowerSec	Automotive Cyber Security	Ann Arbor MI
Transmit Security	Programmable Biometric Authentication	Tel-Aviv Israel
TrapX Security	Threat Detection & Prevention	Tel-Aviv, Israel
Trend Micro	Server, Cloud, and Content Security	Tokyo, Japan
Tripwire	Advanced Cyberthreat Detection	Portland OR
Trusona	Authentication Platform	Scottsdale AZ
TRUSTe	Data Privacy Management	San Francisco CA
TrustedKnight	Malware Detection & Protection	Annapolis MD
TrustedSec	Information Security Consulting	Strongsville OH
Trustlook	Artificial Intelligence Security	San Jose CA
Trustwave	Managed Security Services	Chicago IL
Tufin	Security Policy Orchestration	Tel Aviv, Israel
Twistlock	Container Security	San Francisco CA
Unisys	Endpoint & IT Infrastructure Security	Blue Bell PA
Untangle	Network Security Appliance	San Jose CA
Uppguard	IT Visibility & Risk Management	Mountain View CA
Uplevel Security	Incident Analysis & Response	New York City NY
ValiMail	Automated Email Authentication	San Francisco CA
Vanguard Integrity Professionals	Cybersecurity Consulting & Training	Las Vegas NV
vArmour	Data Center Security	Mountain View CA
Varonis	Data Security & Analytics	New York City NY
VASCO Data Security	Authentication & e-Signature Solutions	Marlborough MA
Vaultive	Cloud Data Encryption	Boston MA
Vectra Networks	Cyber-Attack Detection & Management	San Jose CA
Venafi	Trust Protection Platform	Salt Lake City
Veracity	Industrial Network Security	Aliso Viejo CA
Veracode	Application Security Testing	Burlington MA
Veriato	Employee Monitoring Software	Palm Beach Gardens FL
Verint	Security Intelligence & Compliance	Melville NY
VeriSign	Internet Security Solutions	Reston VA
Verizon Enterprise	Network & Data Security	Basking Ridge NJ
Verodin	Cyber Attack Simulations	Reston VA
Virgil Security	Key Management & Cryptography	Manassas VA
Virtru	Secure Email & Digital Privacy	Washington DC
Virtual Forge	SAP Application Security	Heidelberg, Germany
VirtualArmour	Private Cloud Infrastructure	Centennial CO
Vkansee	Fingerprint Sensors for Mobile Security	Beijing, China
VMRay	Malware Detection & Analysis	Boston MA
VMware	Mobile, Data Center & Cloud Security	Palo Alto CA
Votiro	Zero-Day Exploit Detection	Tel-Aviv, Israel
Wallarm	Automated Vulnerability Detection	Menlo Park CA
Wandera	Secure Mobile Gateway	London, UK
WatchGuard	Threat Management Appliances	Seattle WA
Waterfall	Cybersecurity for NERC-CIP Compliance	Rosh Ha'ayin, Israel
Webroot	Security Analysis & Threat Detection	Broomfield CO
Wetstone Technologies	Cybercrime Investigations & Digital Forensics	Cortland NY
White Ops	Bot Fraud Detection & Prevention	Brooklyn NY
WhiteHat Security	Web Application Security	Santa Clara CA
Wickr	Secure Ephemeral Messaging	San Francisco CA
WinMagic	Full-Disk Encryption Software	Mississauga, Canada
wolfSSL	Open Source Internet Security	Edmonds WA
Wombat Security Technologies	Cybersecurity Education & Training	Pittsburgh PA
Zenedge	Web Application Security	Los Angeles CA
ZeroFOX	Social Risk Management	Baltimore MD
Ziften	Unified Security & Management	Austin TX
Zimperium	Mobile Threat Defense	San Francisco CA
ZixCorp	Email Encryption & Data Protection	Dallas TX
Zscaler	Security-as-a-Service Solutions	San Jose CA

Appendix L : Participant organisations in the CIMA workshops

(in alphabetical order)

Company	Type	Originating - Operating Member State
11Paths - TELEFONICA DIGITAL ESPAÑA, SLU.	LE	Spain
ABIT GmbH	SME	Germany
ACAPELLIS	SME	France
ACCENTURE SA/NV	LE	Belgium
Acerodocs	SME	Spain
AEI Ciberseguridad	Association	Spain
Aenor	LE	Spain
Airbus	LE	Germany
AIRBUS Defence & Space - CyberSecurity (Airbus DS CyberS	LE	France
aizoOn SRL	SME	Italy
Akamai	LE	Poland
Akquinet	SME	Poland
AllThingsTalk	SME	Belgium
ALTRAN	LE	Belgium
ANSSI - Agence Nationale de la Sécurité des Systèmes d'Inf	GOV	France
Arthur's Legal B.V.	SME	Netherlands
ASPISEC SRL	SME	France
ASTOR sp. z o.o.	SME	Poland
Atos	LE	Spain
Autek Ingeniería	SME	Spain
AVL List GmbH	SME	Germany
AVS Automotive	LE	Greece
BAE Systems	LE	France
BDR - Bundesdruckerei GmbH	LE	Germany
BICS	LE	Belgium
Bit4Id	SME	Italy
BKA - Federal Chancellery of Austria	GOV	Austria
BlackBoxSecu	SME	France
BlockMark	SME	UK
BLUE energy Sp. z o.o.	SME	Poland
Bochum Wirtschaftsentwicklung	RTO	Germany
Bosch	LE	France
BT - British Telecommunications Public Limited Company	LE	UK
BusinessForensics	SME	Netherlands
BYTE Computer SA	SME	Greece
Caixabank / Fundación APWG.eu	LE	Spain
CALS	LE	Spain
Capgemini	LE	Spain
CARMAO GmbH	SME	Germany
CCI Nice Cote D'Azur	Association	France
CCI Vacluse	Association	France
CDTI [Centre for the Development of Industrial Technology	GOV	Spain
CDTI [Centre for the Development of Industrial Technology	GOV	Spain
Ceenetworks	SME	UK
Centre for European Policy Studies - CEPS	Association	Belgium
Charlton Networks	SME	UK
CINI - Consorzio Interuniversitario Nazionale per l'Informat	RTO	Italy
Ciptor	SME	Belgium
Ciptor	SME	Sweden

Círculo de Inteligencia	RTO	Spain
Civis Polska Holding	LE	Poland
CLICKALBA Seguridad de la Información S.L.	SME	Spain
Compumatica	SME	Netherlands
CONCEPTIVITY sàrl	SME	Switzerland
Connexion Libre	SME	France
Conseil Régional de Bretagne	GOV	France
Containpro	SME	Germany
Countercraft	SME	UK
Cracow University of Economics	RTO	Poland
Cryptomage SA	SME	Poland
CSA	Association	Spain
Cubewise	SME	Belgium
CY4GATE	SME	Italy
Cyber Noesis	SME	Greece
Cyber Services	SME	Hungary
Cyber Services Plc.	SME	UK
Cybersprint	SME	Netherlands
D2RT - Délégation Régionale à la Recherche et à la Technol	RTO	France
DCMS - Department for Digital, Culture, Media and Sport	GOV	UK
De Montfort University	SME	UK
Deep Secure	SME	UK
Deloitte Advisory	LE	Spain
Department for International Trade British Embassy Wars	GOV	Poland
DETACK GMBH	SME	Germany
Dialoog	SME	Spain
Digital Catapult (DIGICAT)	SME	UK
Dimension Data	LE	Belgium
Docupress media	Association	Spain
Dustin AB	LE	Sweden
Easy Global Market	SME	France
ECO	Association	Germany
EEMA - The European Association for e-Identity & Security	Association	Belgium
Emma Philpott - IASME / UK Cyber Forum	SME	UK
EMTech P.C.	SME	Greece
Enamor International	SME	Poland
ENCODE	SME	Greece
Engineering Ingegneria Informatica S.p.A.	LE	Italy
Enthalpy LTD	SME	Greece
EOS	Association	Belgium
EPUNTO Interim Management	SME	Spain
Ericsson	LE	Sweden
ETSI	Association	France
EU policies	GOV	Spain
EURECAT	RTO	Spain
Eurobits	SME	Germany
European Cyber Security Organisation - ECSO	Association	Belgium
EVANT	SME	Netherlands
Everis	LE	Spain
EVERIS Aerospace and Defence S.L.U. (AEDE)	LE	Spain

EY	LE	Italy
Finnish Information Security Cluster FISC ry	Association	Finland
Forcepoint	LE	Belgium
ForgeRock	SME	Belgium
FORMAVOLUCION	SME	Spain
F-Secure Corporation	SME	Finland
Fujitsu	LE	Spain
Future Intelligence	SME	Greece
G&D - Giesecke & Devrient GmbH	LE	Germany
Gemalto	LE	France
Gemalto	LE	Netherlands
GET [Grupo Estudios Técnicos]	SME	Spain
Gipuzkoa Council - Diputación Foral de Gipuzkoa, Gipuzkoa	GOV	Spain
Global Cyber Alliance Belgium - GCAB	Association	Belgium
GMV	LE	Spain
Goethe-Universität Frankfurt	RTO	Germany
GS2X	SME	France
GUARDTIME	SME	Estonia
High Tech Bristol & Bath	SME	UK
Huawei Technologies Belgium N.V.	LE	China
IBM - Ireland Product Distribution Limited	LE	Ireland
ibm security	LE	Netherlands
IDENTT sp. z o.o.	SME	Poland
IFIS Institut für Internet-Sicherheit)	RTO	Germany
iMinds - IMEC	RTO	Belgium
Immersive Labs	SME	UK
IMT - Institut Mines-Télécom	RTO	France
INCIBE	Association	Spain
Independent	SME	UK
Independent	SME	UK
Independent DPO	SME	Belgium
Independent Free Lance DPO	SME	Belgium
INDRA	LE	Spain
ING	LE	Belgium
InnoTec System	LE	Spain
INNOVALIA - Association de Empresas Tecnológicas INNO	RTO	Spain
InnovaSec	SME	UK
Innovation Bridge Consulting	SME	UK
INRIA - Institut national de recherche en informatique et e	RTO	France
Inria Sophia Antipolis	RTO	France
Institut Mines Telecom	SME	France
Intel Corporation SA	LE	Belgium
Intrinsic-ID	SME	Netherlands
Isdefe	LE	Spain
Isdefe	LE	Spain
Iwecloud	SME	France
John Douglas - Information Age	SME	UK
Kahuna Managing Security BV	SME	Netherlands
KETS Quantum	SME	UK
KI - The Kosciuszko Institute	RTO	Poland

Kommerskollegium [Foreign Trade]	RTO	Sweden
Kontron	SME	France
KPMG Advisory	LE	Belgium
KPN/NB/Security	LE	Netherlands
Krause IT Consulting	SME	Germany
KU Leuven	RTO	Belgium
KUNST LLC	SME	Greece
LEET Security	SME	Spain
Leonardo S.p.a. - Leonardo-Finmeccanica-Società per azioni	LE	Italy
LIKTA - Latvijas Informācijas un komunikācijas tehnoloģijas	Association	Latvia
Lloyds Bank	LE	UK
LogPoint	SME	Sweden
LSEC	Association	Belgium
LuJam Security	SME	UK
Maruta Wachta	SME	Poland
Microsoft Corporation	LE	US
MINETAD [Ministry of Energy, Tourism and the Digital Agency]	GOV	Spain
Ministry of Digital Affairs, Poland	GOV	Poland
MiSE - Ministry of Economic Development, Italy	GOV	Italy
MNEMO	LE	Spain
MSB	RTO	Sweden
n-Auth	SME	Belgium
NCDR Demokritos	RTO	Greece
Neowave	SME	France
Nextel S.A.	SME	Belgium
NextVision Ibérica	SME	Spain
NOKIA	LE	Belgium
NOKIA BELL LABS FRANCE	LE	France
Norwegian University of Science and Technology - Center for Cyber Security	RTO	Norway
NRD CS UAB - NRD Cybersecurity	SME	Italy
NRW.BANK Venture Center	SME	Germany
NTT DATA Italia	LE	Italy
Nunsys	SME	Spain
Oracle Hellas	LE	Greece
Oracle Polska	LE	Poland
ORION INNOVATIONS P.C.	SME	Greece
PESI	RTO	Spain
Physec GmbH	SME	Germany
Piaggio Aerospace	LE	Italy
Plegma Labs S.A	SME	Greece
Poste Italiane	LE	Italy
Prosegur	LE	Spain
PwC Belgium	LE	Belgium
PwC Italy	LE	Italy
Quorum	SME	France
RadarServices Smart IT-Security GmbH (TSMC)	LE	Germany
RBS	LE	UK
RedSocks Security BV	SME	Netherlands
Rohde & Schwarz Cybersecurity	LE	Spain
RSA	LE	Sweden

RSCS - Rohde & Schwarz Cybersecurity GmbH	LE	Germany
Ruhr Universität Bochum	RTO	Germany
S2 Grupo de Innovación en Procesos Organizativos S.L. (S2 G	LE	Spain
S21SEC - Grupo S21SEC Gestión S.A.	SME	Spain
Safelayer	SME	Spain
SAS	LE	Poland
Satways Ltd	SME	Greece
Securactiva	SME	Spain
SecuRing	SME	Poland
Security Brokers	SME	Italy
SETSI - INCIBE - CDTI	Association	Spain
Shepd	SME	UK
Sngular	LE	Spain
SOFOKLEOUSIN.GR	SME	Greece
Sogei SpA	LE	Italy
Sophos	LE	Belgium
Sophos	LE	UK
SPECFILE Project	SME	Poland
STM - STMicroelectronics International N.V.	LE	Belgium
STM Solutions Sp. z o.o. Sp. L	LE	Poland
Swedish Agenc for Growth Policy Analysis	GOV	Sweden
SWEEPATIC.COM	SME	Belgium
Symantec Polska	LE	Poland
Systematic Paris-Region-SPR	Association	France
Tages Solidshield	SME	France
Tecnalía	RTO	Spain
TECNALIA - Fundación Tecnalía Research & Innovation	RTO	Spain
Teknikföretagen	Association	Sweden
Telecom Italia S.p.A.	LE	Italy
Telefónica	LE	Spain
TERRA SPATIUM SA	SME	Greece
Texplained	SME	France
THALES	LE	Spain
The FundingBox Group	SME	Poland
ThreadStone Cyber Security	SME	Netherlands
TimeLex	SME	Belgium
TNO - The Netherlands Organisation for applied scientific r	RTO	Netherlands
Trecom	SME	Poland
Trustweave	SME	UK
UBITECH - GIOUMPITEK Meleti Schediasmos Ylopoiisi kai Po	SME	Greece
UK Cyber Forum	SME	UK
UL TS B.V.	SME	Netherlands
United Technologies Research Centre Ireland, Ltd. (UTRC)	RTO	Ireland
Université Nice Sophia Antipolis	RTO	France
University of Genoa	RTO	Italy
University of Piraeus	RTO	Greece
Unomaly	SME	Sweden
Vasco	LE	Belgium
Vip Protection Group	SME	Greece
Vitrociset	LE	Italy

Vmware	LE	Spain
VoIP Secure	SME	Belgium
VÖWG - Verband der öffentlichen Wirtschaft und Gemeinwirtschaft (Association of Public Services and Public Enterprises Austria)	Association	Austria
VTT Technical Research Centre of Finland	RTO	Finland
Vulnex	SME	Spain
WatchGuard Technologies Inc.	LE	Poland
Waterfall Security Solutions	SME	Canada
Wayra	SME	Spain
Wheel Systems	SME	Poland
WIBU-SYSTEMS AG	SME	France
WISeKey	SME	France
Wooxo	SME	France
Xeridia SL	SME	Spain
Xolido Systems	SME	Spain
Zenit GmbH	SME	Germany
Zion Security	SME	Belgium

Appendix M : Results from workshops

Workshop Recommendations Summary

1.1.106 Fragmentation and reliance on imports

Focus group participants noted that Cybersecurity is still an immature market so fragmentation is not surprising. There are a lot of innovative small companies and a growing M&A activity, which can be both good and bad. For example, it appears difficult to develop and grow EU companies in fields such as Encryption: acquisitions of SMEs by, for example, US companies is an ongoing issue, just as it is in other fast developing sectors such as Electric Vehicles. Differences in culture which drive investment (e.g. US venture capital funding associated with a strong risk-taking culture, Government-driven innovation funding programmes in Asia) give international competitors a competitive advantage compared to Europe, but this applies more widely than Cybersecurity.

There are also major barriers to the growth of start-ups in Europe. Failure by start-ups is culturally acceptable in the US but not in the EU, where entrepreneurs find it difficult to get financial backing if previous business ventures have been unsuccessful. Selling is difficult for start-ups and immature SMEs as users are very risk averse. Other barriers for start-ups include a need for lawyers (IP, employment, etc) which is very time consuming and distracts from the core growth aims of the business.

There may also be fragmentation in research projects and activities, with similar research happening in Spain, Germany and other parts of Europe. If this was combined or better coordinated a larger impact could be created, e.g. similar to research in defence, such as for the US Joint Strike Fighter.

It is recognised that it is very difficult for large players to link to innovative SMEs, particularly as timescales for projects and funding budgets are very different. A good model is SystemX in France (<https://www.universite-paris-saclay.fr/en/university/member/irt-system-x>) in which universities, start-ups and Large Enterprises (LEs) define a project and work together to develop a prototype with state funding. This supports exchange of personnel from the companies to work at the research centres. The functioning of the Institute is based on two fundamental aspects:

1. The co-localization of its talents: the Institute brings together in one place all the project partners, thus creating a melting pot of interaction between stakeholders of public and industrial research.
2. The pooling of skills and platforms: by reaching a critical mass, SystemX is able to provide a platform through the pooling of many skills and technological bricks.

One of the four focus areas is: “Internet of Trust” or digital trust in the “Internet of Everything” with research programmes on Cognitive and Cybersecurity algorithms for intelligent control and optimal management of the networks of the future.

It is also difficult for large companies and SMEs to cooperate effectively across new developing value chains. For example, in Industry 4.0 connecting elements together to form a new value chain has security implications and requires large and small companies to cooperate across sectors, which is very challenging.

1.1.107 Standards / Certification

Focus group participants generally agreed that there was a need for EU-wide Cybersecurity product standards that apply in all MS. For example, the following exist: Common Criteria (international viewpoint but organising body based in US) which uses a ‘scope set’, CPA - Commercial Product Assurance in the UK that uses security characteristics (e.g. for Firewalls, Smart Meters), a new set of

standards in Germany, etc. Agreement on ‘what is good in a Cybersecurity product’, e.g. the equivalent of an EU ‘crash test’ (like Euro NCAP for cars) for Cybersecurity products and services, could allow countries to run their own schemes built on a common agreement. National-only standards are not useful to exporters, hindering inter-MS trading, and could be thought of as anti-competitive.

Participants were divided on whether this would support EU competitiveness. There appears to be added value from certification making sales and especially exports easier, and raising user awareness and confidence. However, there are negative effects related to the time and cost of approvals. For example, the existing common criteria take a very long time to get certified, and are only affordable for large players. In the UK, the cost (from EUR 50 thousand to EUR 500 thousand) for national approvals is prohibitive and stifles innovation. Getting separate MS testing and approval to sell across Europe is a big burden, especially for SMEs.

Concerns were raised about differences between MS on certification and it was felt that the EU can play a role in harmonising standards. The EC should develop a single set of approval criteria for Cybersecurity products and services that applies across EU MS. It was also felt that if there was such a set of common standards then there would be a reasonable chance of getting agreement with the US.

1.1.108 Regulation / Legislation

Focus group participants were divided on whether this would support EU competitiveness. Those in favour cited the example of the US and the PCI/DSS regulation, that led to a significant boost in training requirements together with the development of vulnerability products in the US. Others mentioned the GDPR, which is a European regulation, but all the US security vendors specialized in data protection have seemed to benefit from this development, while the EU is lagging behind in this technology. It was also mentioned that legislation may be a business opportunity for the security industry, but for those EU companies that are subjected to it, it is a burden.

ECSC members noted that the new NIS directive will stimulate EU critical infrastructure sectors to address Cybersecurity and this will create an opportunity for EU Industry, as well as supporting ENISA to set up a certification centre.

1.1.109 Role of Government / Pre Competitive Procurement (PCP)

All focus group participants were clear on the need for national governments and the EU to lead by example. The US built up its leading ICT market position through military funding. Cybersecurity is not seen as a strategic defence capability in the EU unlike in the US. Industry needs to be supported with a strategic view at EU level.

While governments are policy makers and supporters of the competitiveness of national companies, products are also bought from outside their region and Europe. Current EU Public Procurement policies which focus on the best price are not conducive to building up national champions and markets, e.g. Thales and Leonardo tried to develop firewalls but stopped as it was not commercially beneficial. Public Procurement could be split into two: (1) for commodity purchasing, (2) strategic with an industrial policy. The use of Defence funds could also be considered.

PCP instruments are largely unknown to Cybersecurity focus group participants. Innovative procurement could be considered in order to stimulate faster acceptance of technology.

The UK is seen as a global innovation hub. Growth of companies in Cybersecurity in Europe could be helped by learning lessons from UK initiatives such as CyLon, Wayra and ICURE.

- CyLon (<https://cylonlab.com>), which is Europe’s first Cybersecurity accelerator, offers GBP 15 thousand funding for a 3% equity stake. Cylon offers a 13-week intensive training/mentoring

programme for start-ups, culminating in the opportunity to pitch their product to over 100 investors and customers at a Demo Day.

- Wayra (<https://wayra.co.uk/gchq>) supports the GCHQ Cyber Accelerator which is a collaboration between the UK Government, the Government Communications Headquarters (GCHQ), Wayra UK, part of Telefónica Open Future_, and the National Cybersecurity Centre (NCSC). Successful applicants will gain access to GCHQ's world-class personnel and technological expertise to allow them to expand capability, improve ideas and devise cutting-edge products to outpace current and emerging threats. A roster of best-in-class coaches and mentors from GCHQ and the wider Telefónica Group – including O2 and ElevenPaths – will provide support. Start-ups will also receive a financial grant, and access to work space.
- The ICURE Innovation-to-Commercialisation programme piloted by the SETsquared Partnership (<http://www.setsquared.co.uk/research-commercialisation/cyber-security-icure-programme>) and Innovate UK, is funded by the Department for Business, Environment and Industrial Strategy (BEIS). ICURE offers university researchers with commercially-promising ideas up to GBP 50 thousand to 'get out of the lab' and validate their ideas in the marketplace.

Competitions to attend and be sponsored at exhibitions and trade events such as InfoSec, UKTI Singapore, are also very useful.

1.1.110 Clusters

Cybersecurity clusters exist in a number of Member States and represent the views of and support small and large business and academia. These provide brokerage for collaborative projects and links as well as access to professional services (see EC Framework 7 'Facilitate Industry and Research in Europe' (FIRE) project reports, <http://www.trustworthyictonfire.com>). Ecosystems cannot be artificially created but need nurturing and sustaining beyond normal political cycles. Many of the EU clusters were stimulated by national or regional financial support and some have become self-sustaining through subscription models, etc. It was noted by participants that the US ecosystem is more sustainable as DARPA, DHS etc publish longer-lasting innovation pipelines/roadmaps.

The high density of strong academic institutions working in Cybersecurity located near Industry companies requiring access to this expertise is an EU strength (e.g. compared to Asia), as is the quality and low cost of education in the EU (e.g. compared to the US).

1.1.111 Competence Centres

Focus group participants also suggested setting up a centre of Cybersecurity excellence, such as NIST in the US, with the best people from the different Member States government agencies. One suggestion was that ENISA could fulfil this role, widening its activities beyond reports and studies.

Participants also strongly supported the need for one or more champions at EU level to combine innovative ideas and economic policies need to be developed to encourage this, e.g. like an Airbus for Cybersecurity. These could be based around one of the major EU companies, acting as the hub linking to research institutes and SMEs.

This page was intentionally left blank.

Appendix N : Cybersecurity Research Methodology 2017

Introduction to Research Methodology

1.1.112 Introduction

This document describes the quantitative research methodology adopted as part of the CIMA project. It aggregates the different techniques and processes applied to different project tasks and deliverables that include:

- Global market quantification
- Supplier and purchaser analysis
- Country analysis
- Market forecasting
- International trade flows
- Company analysis

The methodology describes in detail, using examples drawn from Security and Cybersecurity, the research methods and processes employed in generating quantitative analysis of the European Cybersecurity market.

1.1.113 Quantitative Research Process

The Quantitative Research methodology (described in more detail in Section 0) relies on a core analytical system called Profiling. This is based upon a 30- year international research programme that started in Harvard University and was subsequently developed in countries across Europe. Profiling is used to track technology and market change and uses “big data” techniques, analytical data grids, business case studies and industry- level research to provide probabilistic and measurable evidence about how companies/ economies adapt to and perform within changing market conditions.

The methodology reflects best practice in private sector research processes like market competitive and competitor intelligence gathering and analysis- as well as more traditional public sector economic assessment methodologies. It has developed from long term experience of selecting, monitoring, evaluating, triangulating and then analysing multiple unstructured and semi- structured data sources to produce structured values, forecasts and economic/ industrial indicators with explicitly measured data confidence levels.

This approach is suited to providing multi- sourced "big data" solutions to define and quantify previously unobserved or "difficult-to-measure" markets where standard industrial classification systems are non- existent, restricted or rapidly out- dated. This includes previously and currently researched sectors like the Low Carbon Economy, Digital & Creative Industries, Geo- Located Services, Life Sciences, Space Technology, Carbon Markets, Weather & Climate Services, Climate Change Adaptation, Agri- technology, Marine Environment and Security/ Cybersecurity. Some of these markets/ sectors have a planning horizon (a measure of market change) as short as six months and are experiencing rapid growth and development, so it is not surprising if national systems fail to capture their emerging value.

This approach is most often employed within the public or private sector when:

- An emerging or newly “discovered” market needs to be defined and quantified
- An existing market needs a more flexible and detailed segmentation than Standard Industry Classifications can provide
- International market information and national benchmarking are required and cannot be provided due to differences in international industry coding systems
- A financial business case needs to be made for supporting a new market/ sector through robust quantification of the current economic baseline and future market opportunities.

In these circumstances, the methodology provides: Internally consistent global research, based upon market intelligence sources and rules rather than national statistics, that can be used to measure economic sectors that are not well represented by Standard Industrial Classification (SIC) codes or industry bodies and provides a flexible/ adaptable data structure with multiple levels of detail and multiple measures that are consistent across international boundaries.

1.1.114 Different Approaches to Market/ Sector Quantification

There are three distinctive approaches to economic market/ sector analysis and each has its own merits. They are the:

- National statistical approach
- Trade/ industry approach (including survey techniques)
- Multi- sourced approach.

In the UK, the Office of National Statistics (ONS) reports economic activity using Standard Industry Classifications (SIC) codes. Most nations have their equivalent systems i.e. NACE, NAICS etc. The national statistical approach can be generic, slow moving, structurally rigid and objective as befits its role as a national score- keeping system. It has longevity, consistency, credibility, availability and a widely- experienced base of analysts and users’ familiar with its interpretation and application. But it suffers the limitations and inaccuracies of self- classification against a list of generic product/ service descriptions that do not fit with most company's experience of the global market. For this reason, despite its "dependability" it has an inherent level of inaccuracy that is almost impossible to measure and it is rarely a good tool to measure emerging or difficult-to-define market sectors. So, while companies may be required to report their activities using systems like SIC, they would not use SIC (due to its inflexibility) as the basis for their own market research or planning.

The Trade/ Industry approach generally has the advantage of agreed sector boundaries (that may be different to SIC definitions), higher levels of accuracy within those boundaries (i.e. is internally consistent), annual collection and may include some benchmark standards for performance against competing nations and their flagship companies (i.e. can be outwardly focused). The limitations are that data collected in this way takes many years to achieve consistency and credibility, is only available where strong associations exist, is subjective (collected and reported for the benefits of its membership) and has no reason or basis to define or measure new or emerging sectors or to generate performance standards for this new collection of activities (i.e. it is inherently conservative or self-interested). Trade/ Industry data is generally provided on a confidential basis, and can be difficult to verify externally. Also, it may be collected on a selective basis, from "prime" companies and excluding

supply chain companies, which means that it provides a limited ability to "drill-down" into the supporting activities provided by lower- tier companies.

The multi- sourced approach (employed for this research) has the advantage of being flexible, rapid, objective and can operate in areas where the above two approaches either do not exist or are poorly aligned with the sector/ market under investigation. The experimental nature of the multi- sourced approach can create definition and analysis where neither existed previously and can generate new levels of market awareness and debate. The limitations are that this approach is not directly comparable with traditional statistics (numbers are created, not just collected), is inherently complex and, therefore, difficult for others to replicate, does not have an existing or immediate body of industry support (or trained users) and can lack a continuous commitment to funding once its initial objective is achieved. The multi- sourced approach is, however, an early flavour of what the "big data" explosion can bring to the sector and market analysis party in terms of the structured use of unstructured or semi- structured data, leading to detailed segmentation and bespoke/ rapidly updating market definitions.

Often, the multi- source approach is only considered when all other efforts have failed to adapt/ extend existing data sources or to successfully extrapolate and estimate new markets by adding assumptions to the existing statistical data. For this reason, the multi- source approach can suffer from incredulity ("can't be done"), scepticism ("can't be verified") or protectionism (can't be allowed to compete).

The other and quite legitimate problems with the multi-source approach is that it is derived from primarily non- economic sources and must develop (over time) economic characteristics that enable its outputs to be compared with traditional data sources. While it is legitimate to talk about and assemble figures about "sales" from an industry or market intelligence perspective, public sector economist and statisticians will require this to be converted to terms like Gross Value Added (GVA) before it can be absorbed into the economics mainstream.

While it is possible to map multi-source solutions and outputs to existing classification systems and to existing economic metrics, this can be a time- consuming and exhaustive process and can often conflict with the initial requirement for a rapid, and internally consistent, assessment of a new sector/ market. Recent examples, where similar research mapped 3,000 products and services from its Green Economy definition to SIC, NACE and NAICS codes, demonstrated that as little as 10% of green activities were captured by specific industry codes in any of the three systems and that the remaining 90%+ of activities disappeared into "general manufacturing" and other equally generic (and unhelpful) codes. A similar exercise would produce even worse results for Cybersecurity.

Case Study 1: Comparing Approaches to Sector Measurement

In a recent experiment (2014), the UK commissioned the collection of Low Carbon company- level data (not using SIC) using standard survey techniques via a non- Industry source.

The advantages of this methodology were that it could sustain a sector definition that by-passed limitations in SIC but at the same time provided a legitimacy to Low Carbon activities by subjecting them to the same rules that are applied to SIC coded businesses.

The disadvantages of this approach (drawn from the recent research itself) were that only limited performance data could be obtained (typically, more valuable and sensitive data like growth, exports etc. is only trusted to trade bodies), only a limited number of companies were identified (due to size), extrapolations about activities (based upon SIC coded data), employment and company distributions etc. were based solely upon the companies that a) could be seen and b) volunteered for the survey. The limitations in the survey approach (when compared with the multi-sourced approach) were: loss of granularity (analysis only available at sub-sector level), loss of supply chain analysis (replaced with standard multipliers), loss of usable metrics like forecast growth and loss of international comparisons and measures of competitive performance.

Allowing for some small differences in definition the estimated size of the UK Low Carbon sector using the survey approach (GBP 128 billion) was almost identical to contemporary multi-sourced research (GBP 134 billion).

There are a few examples where the multi-sourced approach has generated the business case for investment in new sector infrastructure and networks, which in turn generated new industry associations and knowledge, which in turn created a better understanding of how national statistics could be adapted (over time) to measure future sector activities. These examples include:

- Low Carbon Economy (above)
- Space Technologies (where the research launched the business case for the UK Industry network that now conducts its own research into Earth Observation Satellite markets), and
- Climate Services, where the research is part of a Horizon 2020 consortium preparing to deliver a European Market Observatory

The case study, and other examples enacted across different European countries and global cities, demonstrates that the quantitative multi-sourced approach can produce early and robust quantitative market assessments that can subsequently be validated and mainstreamed using more traditional research methods.

Defining Cybersecurity

1.1.115 Introduction

The current Cybersecurity research is based upon a programme that started in the UK in 2006 and has reported to national government on the global Security market for 10 years and on Cybersecurity for five years.

An initial Cybersecurity definition was created in 2010, updated in 2013 and in 2014 to reflect significant changes in the content and reporting of Cyber activities. This history reflects the constantly changing nature of an emerging sector. Cybersecurity is defined as an industry that responds to the escalating challenges of maintaining the confidentiality, integrity, availability and resilience of Cyberspace and to counter "deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or network or the information and/ or programmes resident in or transiting these systems or networks."

Key points about the Cybersecurity definition used for this report are:

- The current definition has evolved since its first introduction in 2010 and will continue to evolve i.e. at any point, the definition is a “freeze- frame” on what is happening in the industry
- Any proposed changes to the definition are investigated to ensure that they are quantifiable and additions to the definition are “run backwards” to ensure that data history and trend analysis is maintained
- Data is structured to enable multiple coding, filtering and reporting of the data without changing the underlying data structure. In this way, definitions can be “dynamic” without losing content and context and can be re-purposed for “themed” security activities like – events, borders, transport.

An example of how the Cybersecurity dataset can be coded for comparative and analytical purposes is included at Appendix H, where the structure and content of the current CIMA dataset is compared with an alternative taxonomy to test the comprehensiveness and completeness of the research data.

The current definition includes 12 sub-sectors of Cybersecurity. These are:

- Anti- Malware
- Application Security
- Business Continuity
- Cyber Consultancy
- Cyber Insurance
- Encryption
- Identity and Access Control
- Infrastructure
- Mobile
- Outsourced
- Situational Awareness
- Systems Recovery

These sub-sectors are described in more detail in Table 46 (below). For the purposes of the analysis in the CIMA report First and Third- Party Insurance have been merged into a single “Cyber Insurance” category.

Table 46 : Cybersecurity Sub-sectors

Anti- Malware	Includes development, supply, management, training and consulting for anti-malware, anti- spam, firewall, antivirus/ worm and forensic software/ services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Application Security	Includes development, supply, management, training and consulting for application code security/ patch management/ content filtering & monitoring/ vulnerability assessment software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Business Continuity	Includes development, supply, management, training and consulting for business continuity & recovery/ IT & Cyber forensics/ computer forensics software and services (manual and automated) for corporate/ small business/ public/ cloud/ smart communications and other networks.
Cyber Consultancy	Includes consulting for cyber audit/ insider threat/ security policy/ risk & compliance/ training & awareness/ legislation, standards and strategy for threat avoidance, threat detection and compliance

Encryption	Includes development, supply, management, training and consulting for identity management/ digital signature/ digital certificate/ storage security correction/ detection/ prevention software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
First Party Cyber Insurance	Includes loss or damage to digital assets, business interruption from network downtime, cyber extortion (through data release, network damage, network restriction or false communication), reputational damage and theft of money or digital assets.
Identity & Access Based Services	Includes development, supply, management, training and consulting for access management/ intrusion detection & response/ intrusion & anomaly prevention/ messaging security software and services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Infrastructure	Includes development, supply, management, training and consulting for infrastructure monitoring/ data management/ network security/ infrastructure resilience testing/ security applications/ web services security/ enterprise risk assessment for corporate/ small business/ public/ cloud/ smart communications and other networks.
Mobile	Includes development, supply, management, training and consulting for mobile endpoint security/ mobile device management/ VPN/ Wireless security software and services (local/ remote access) for corporate/ small business/ public/ cloud/ smart communications and other networks.
Outsourced/ Managed Services	Includes development, supply, management, training and consulting for cyber threat/ internet platform/ systems access/ mobile systems/ network & hub/ systems integration/ cloud services for corporate/ small business/ public/ cloud/ smart communications and other networks.
Situational Awareness	Includes development, supply, management, training and consulting for high & low level situational awareness/ internal & external cyber threat intelligence/ proactive cyber surveillance/ social media monitoring/ deep web investigations software and services (automated and manual) for corporate/ small business/ public/ cloud/ smart communications and other networks.
System Recovery & Data Cleansing	Includes development, supply, management, training and consulting for system recovery/ data recovery/ data cleansing/ data validation & verification software and service for corporate/ small business/ public/ cloud/ smart communications and other networks.
Third Party Cyber Insurance	Third Party Cyber Insurance includes security and privacy breaches, investigation of privacy breach, third party breach notification, multi- media liability and loss of third party data (loss, corruption, denial of access, software failure, data error and systems failure).

1.1.116 Structuring the Data

A seven- digit coding system is used for the full Cybersecurity sector dataset. At Level 5, there are 3,800 discrete LCEGS products and services and they are aggregated at Levels 4:

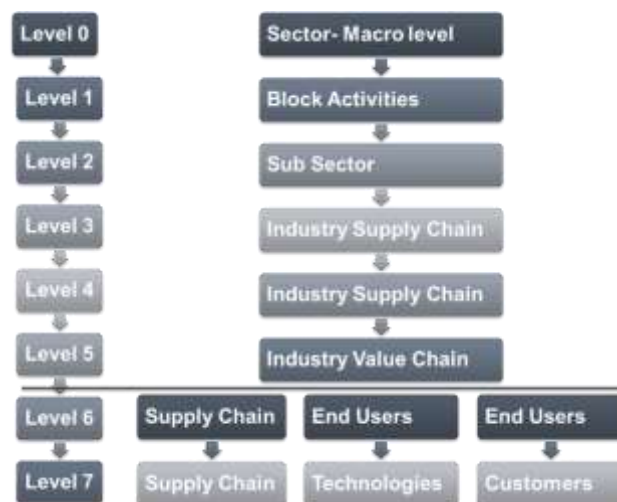
- Level 1 Cybersecurity
- Level 2 12 sub-sectors
- Level 3 51 sub sub-sectors
- Level 4 225 product and service categories
- Level 5 1,100 product and service activities.

In reality, there are seven different data levels behind Cybersecurity, but not all product or service activities can be defined at seven levels. Level 5 is the compromise between too little and too much data, with most reporting conducted at Levels 2 and 3. Where the additional levels of data become important is when:

- Specific “deep dives” are required for individual companies to identify markets for their products and services
- To identify end-user groups for specific products and services, or at the transactional level, for specific customers.

The multi- layered data model is shown at Figure 60, with each data level annotated to describe in broad terms what it contains/ how it can be applied. The terms at each level can vary according to the sector under investigation, can be foreshortened for service- only sectors and even increased to reflect very long supply chains like automotive and aerospace.

Figure 60 : Multi- Layered Data Model



The Cybersecurity data set used for this research includes 1,100 products and services, aggregated (by supply or value chain activity) into four data levels and then reported for the 12 sub-sectors. The current sector definition includes the widest possible range of cyber- related activities on the principle that it is easier to filter- out activities for any specific analysis than it is to add them to the data set at a later point. The data is arranged hierarchically, with the data being aggregated at five levels, where Level 5 is the most granular and Level 1 refers to the sector. The data hierarchy is illustrated in Table 47.

Table 47 : Data Hierarchy Example

Level 1	Level 2	Level 3	Level 4	Level 5
Cyber	Application Security	Application Code Security	Supply of Software for Application Security	Large Corporate Networks
				Small Business Networks
				Cloud Services Networks
				Public Sector Networks
			Management Services for Application Security	Smart Comms Networks
				General Applications
				Large Corporate Networks
				Small Business Networks
		Patch Management	Development of Software for Patch Management	Cloud Services Networks
				Public Sector Networks
				Smart Comms Networks
				General Applications
			Consulting Services for Patch Management	Large Corporate Networks
				Small Business Networks
				Cloud Services Networks
				Public Sector Networks
			Management Services for Patch Management	Smart Comms Networks
				General Applications
				Large Corporate Networks
				Small Business Networks
				Cloud Services Networks
				Public Sector Networks
				Smart Comms Networks
				General Applications

Organizing Cybersecurity activities into a usable taxonomy involves two tasks:

- The first is to try and adapt the "language" of products and services created from different industrial sectors so that they describe and fit with the defined Cybersecurity activities (see Section 0)
- The second is to then attempt to group those activities together in a meaningful hierarchical relationship for analytical and reporting purposes.

The hierarchical structure of the Cybersecurity sector activity base means that products and services are aggregated into sensible groupings within each sub-sector. Grouping 150 activities against a single sub-sector without intermediate levels of aggregation would create a reporting nightmare.

Figure 61 : Grouping Activities



The description and grouping of activities within sub-sectors varies according to the nature of the Cybersecurity process (see Figure 61 : Grouping Activities). In general terms, the taxonomy for "products" involves different levels of technology or integration i.e.

- "Access Control Systems"/ "Domestic Buildings"/ "Door Controls Data Systems" split into "Key Pad", "Swipe Card", "Proximity Devices", "Biometric" and "Other" at Level 5
- "Biometrics"/ "Manufacture"/ "Facial Traits Reading Systems" split into "Door, Gate and Barrier Access", "Computer Access", "Authorisation Systems", "Mobile Applications" and "ID Registration" at Level 5.

For services, the taxonomy is often less technology- based (less moving parts or assembly) and is more "user" focused. This means that many of the software, support, service tasks (i.e. most of Cybersecurity) at Level 5 are defined in terms of user networks i.e. Large Corporate, Small Business, Cloud, Public Sector, Smart Comms and General Applications (see Table 2).

A list of Cybersecurity activities (Level 2- 4) is included at **Appendix H : Taxonomy – Cybersecurity Data Level 2 – 4 Definitions**.

Geographic Analysis

1.1.117 Introduction

In Section 1.1.114 Different Approaches to Market/ Sector Quantification one of the benefits of the multi- sourced methodology was cited as its ability to operate across national boundaries. By not being bound to single national sources of data the Cybersecurity definition can be applied to multiple geographies by using multiple data sources that can operate independently of national boundaries. The process for doing so is described in more detail in Section 0, but in Section 0 the scope for geographical analysis is described. So, where Section 0 focused on sector definitions and boundaries, Section 0 performs the geographical equivalent.

The sector research has often been described/ used as an “overlay” system that can sit on top of various national industry classification systems, without having to disturb or change those reporting systems. In this regard, Cybersecurity can bypass the lengthy process of re- classification that would be required to achieve a measurable definition.

By using global data sources, it is possible to by- pass some of the weaknesses of the reporting systems for smaller countries by accessing external data. This use of internal/ external data also assists the measurement of trade flows between countries. By accessing global sources as part of the sector definition process it means that references to different products and services can be standardised in a descriptive way that is not dependent on any single country definition. This makes the Cybersecurity dataset truly scalable across multiple nations, cities and regions. The bad news is that it is not an exact fit with any of the classification systems, the good news is that comparison is possible without the time or resource required to adapt or change the underlying national systems.

1.1.118 Geographic Levels

The Cybersecurity data set is global and is defined at several levels:

- Global, Global Region and Global Sub Region
- Country (226 countries)
- Country Region (for Top 50 economies only and for EU NUTS Level 2)
- Country Sub Region (bespoke for specific countries only)
- City (Megacities and other larger cities across the globe).

The data in the Cybersecurity data set is geo- coded so that analysis can be aggregated or disaggregated to any of the above levels. There are several reasons why the data is defined at so many different levels:

- a. The Cybersecurity data is globally sourced i.e. we do not just use a country’s data about itself. To obtain a more complete picture in the absence of definitive national data we search globally. To understand the global data, which is interconnected through international trade, we need to build a global model
- b. Cybersecurity is still an emerging market with little firm data currently available. This means that affirming Cybersecurity data on a single national economy requires comparisons with activities in other national economies, both for Cybersecurity and for other significant

economic sectors that act as customers for Cybersecurity. This is also true at the regional and city level- without a single definitive and official source of data to rely upon, to be confident in measuring any single geographical unit, you need multiple comparisons to sense- check and verify the results.

- c. To achieve measurement of international trade, we need to compare data on both ends of the trade i.e. purchaser/ seller or importer/ exporter. To be able to measure and rank market share within a country market we need to quantify the import/ export relationships between multiple countries. In most cases this includes the Top 50 economies, who account for approximately 90% of all global trade. Beyond the Top 50, it becomes the law of diminishing returns and introduces very high levels of complexity, so we do not attempt to map the inter-trading between all 226 countries
- d. Most national statistics lack the necessary meaningful comparisons to quantify and rank competitive performance. This is due to the problems of comparing definitions, understanding the basis for different national statistics and aligning the economic assumptions they lay behind them. Because the Cybersecurity data set focuses on internal consistency across all countries, rather than consistency for any single country, it is appropriate to make national (and other) comparisons
- e. The quality of data varies significantly across countries. Therefore, for smaller countries, the best sources of data may be from international bodies, NGOs, trading partners or neighbours. The quality and number of sources of data at a country level is taken account of through our system of quantifying data confidence levels (described elsewhere) that are based upon the available data for the sector in question and compared on a country-by-country basis.

The Cybersecurity data set includes economic data on 226 countries and territories. This list includes the IMF's World Economic Outlook's 189 countries plus 37 territories and island economies for which data is available. The full list of countries is shown at Table 48 : List of Countries for Research Purposes where the less- reported territories are indicated in red.

Table 48 : List of Countries for Research Purposes

Afghanistan	Gaza Strip/West Bank	Niger
Albania	Georgia	Nigeria
Algeria	Germany	Niue
American Samoa	Ghana	Northern Marina Islands
Andorra	Gibraltar	Norway
Angola	Greece	Oman
Anguilla	Greenland	Pakistan
Antigua and Barbuda	Grenada	Palau
Argentina	Guadeloupe	Panama
Armenia	Guam	Papua New Guinea
Aruba	Guatemala	Paraguay
Australia	Guernsey	Peru
Austria	Guinea-Bissau	Philippines
Azerbaijan	Guyana	Poland
Bahamas	Haiti	Portugal
Bahrain	Honduras	Puerto Rico
Bangladesh	Hong Kong	Qatar
Barbados	Hungary	Reunion
Belarus	Iceland	Romania
Belgium	India	Russian Federation
Belize	Indonesia	Rwanda
Benin	Iran	Saint Kitts and Nevis
Bermuda	Iraq	Saint Lucia
Bhutan	Ireland	Saint Vincent and the Grenadines
Bolivia	Isle of Man	Samoa
Bosnia	Israel	San Marino
Botswana	Italy	Sao Tome and Principe
Brazil	Jamaica	Saudi Arabia
British Virgin Isles	Japan	Senegal
Brunei	Jersey	Serbia
Bulgaria	Jordan	Seychelles
Burkina Faso	Kazakistan	Sierra Leone
Burma/ Myanmar	Kenya	Singapore
Burundi	Kiribati	Slovakia

Cambodia	North Korea	Slovenia
Cameroon	South Korea	Solomon Islands
Canada	Kuwait	Somalia
Cape Verde	Kyrgyzstan	South Africa
Cayman Islands	Laos	Spain
Central African Republic	Latvia	Sri Lanka
Chad	Lebanon	St Helena
Chile	Lesotho	St Pierre and Miquelon
China	Liberia	Sudan
Colombia	Libya	Suriname
Comoros	Liechtenstein	Swaziland
Congo	Lithuania	Sweden
Democratic Republic of Congo	Luxembourg	Switzerland
Cook Islands	Macau	Syria
Costa Rica	Macedonia	Taiwan
Cote d'Ivoire/ Ivory Coast	Madagascar	Tajikistan
Croatia	Malawi	Tanzania
Cuba	Malaysia	Thailand
Cyprus	Maldives	Togo
Czechia	Mali	Tokelau
Denmark	Malta	Tongo
Djibouti	Marshall Islands	Trinidad and Tobago
Dominica	Martinique	Tunisia
Dominican Republic	Mauritania	Turkey
East Timor	Mauritius	Turkmenistan
Ecuador	Mayotte	Turks and Caicos Island
Egypt	Mexico	Tuvalu
El Salvador	Micronesia	Uganda
Equatorial Guinea	Moldova	Ukraine
Eritrea	Monaco	United Arab Emirates
Estonia	Mongolia	United Kingdom
Ethiopia	Montserrat	Uruguay
Falkland Islands	Morocco	USA
Faroe Islands	Mozambique	Uzbekistan
Fiji	Namibia	Vanuatu
Finland	Nauru	Venezuela
France	Nepal	Vietnam
French Guiana	Netherlands	Virgin Islands
French Polynesia	Netherlands Antilles	Wallis and Futuna
Gabon	New Caledonia	Yemen
Gambia	New Zealand	Zambia
	Nicaragua	Zimbabwe

Missing from this list are:

- Curacao and Sint Maarten (included under Netherlands)
- Holy See, Kosovo and South Sudan (insufficient sources of available data).

The Quantitative Research Methodology

1.1.119 Overview of Market/ Sector Research Process

This section describes the process for creating, populating and maintaining the Cybersecurity data set. It includes the top- level research model and an explanation of most of the key stages of the model. This section includes content about the general research methodology (how it is applied to all the applied research sectors) and the specifics of the process as it applies to Cybersecurity.

While the requirements for each market research project vary, the methodology and process always follows the same five key stages:

1. Define- Identify, select and group the target market activities, whilst conducting an initial check for the right volume and quality of data sources. This is the most resource intensive step as it involves:
 - Identifying available data sources for defining the market/ sector under investigation
 - Investigating other Market, Benchmark and Specialist data for populating the metrics
 - Creating and testing market taxonomy of product and service activities
 - Establishing metrics framework for market analysis

2. Assemble- Populate the data measures for each market activity, carefully filtering the core data sources to ensure that confidence levels are within bounds. This is the most data intensive step as it involves:
 - Defining geography for data population and market analysis
 - Running national and regional geographic filters to take account of local business mix and local chains of supply
 - Running metrics for all products and services for pilot analysis and checking (normally up to 5 countries)

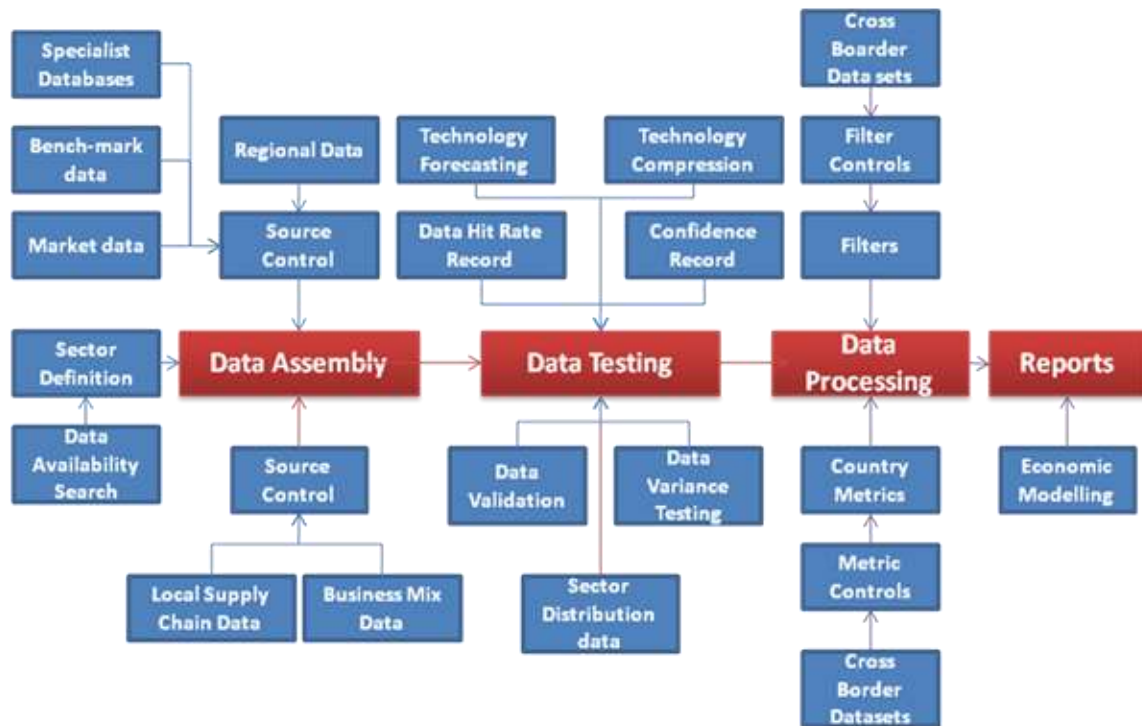
3. Check- Apply quality assurance checks to ensure data accuracy/ consistency across market activities and different countries and, in some cases, cross-check with different sector values. This includes:
 - Data validation through the evaluation of sources used to calculate data points and their corresponding data confidence levels
 - Variance Testing results against previous or related research
 - Checking forecast growth and other rates of change in relation to specific internal metrics for Technology Forecasting
 - Checking forecast growth and supply chain related change/ growth in relation to specific internal metrics for Technology Compression

4. Validate- Sense-check and spot-check market data values against specific projects/ authoritative sources/ expert knowledge/ customers or clients:
 - Final checks relating to the global roll-out of the data population beyond the pilot data
 - Application of cross- border filters and analysis to calculate national trade flows i.e. imports and exports

5. Publish- Recalculate, update confidence levels and publish research data set.

This process is illustrated by the generic Sector Research Model (Figure 62 : Market Research Model), where the numbers correspond to the process stages above.

Figure 62 : Market Research Model



The research model comprises distinct but iterative phases. This is because the data analysis needs to "create" its own data before it can analyse it. This is fundamentally different from any SIC or NACE-based sector analysis that takes its data as a "given."

Within the above model a range of different research methods are employed. Some aspects of the research system are semi- automated (necessary when dealing with large volumes of data), but the rule- sets and software algorithms are based upon many years' experience in compiling and reporting complex markets and all final decisions about reported outputs are subject to intense analyst scrutiny.

The research methods employed include:

- Desk research to define market/ sector content and determine market boundaries
- Industrial templates that identify core and supply chain activities in detail for inclusion in sector definition
- Data discovery tools to identify new data and sources relating to the defined sector activities
- Data coding systems to ensure that sector, company- level data and other classification systems are aligned for analysis and reporting purposes
- Data management techniques and systems to maintain existing source libraries and integrate them with new source materials

- Software systems with defined (but flexible) rule- sets to filter source content (i.e. Security v. Cybersecurity)
- Semi- automated processes for modelling and calculating data values from selected source lists
- Knowledge base of case study materials that can be accessed to help fill data gaps and provide industrial performance benchmarks
- Quality assurance processes and tools that check all values against a range of international, national and industrial comparators
- Data management and visualisation tools for presenting and reporting data

Survey and interview methods are only included when they are a specific requirement of a project and are mostly employed at the beginning of a project (definition) or at the end (value or possible application of the results) but are not employed as part of the data creation or data collection process.

A final comment on the research model, is that while it appears linear, it is highly iterative, with all research sub systems playing a role at the beginning, middle and end of each complex market/ sector research project.

1.1.120 Defining Sector Boundaries

Sector definitions are all about boundaries. Developing definitions for newly prioritised economic activities and markets involves a process of "revolution" (boundaries and taxonomies that generate debate) and evolution (boundaries and taxonomies that eventually generate an informed consensus). This cycle has occurred many times before and includes sectors like Information Technology, Digital Technologies, Biotechnology, Nanotechnology and the Low Carbon Economy/ CleanTech. Cybersecurity is, arguably, still in the revolutionary phase, where activities and applications (and their descriptions) are still emerging.

The first stage of any market research process is to define specific sector activities in line with an overarching definition. This may include:

- Starting from scratch (blank sheet formulation of a new market sector)
- Starting with an existing conceptual model (build on client view of an emerging sector)
- Adapting an existing sector model (build a bespoke view of a traditional sector).

Unlike some other sectors, Cybersecurity started as a blank sheet exercise in 2010/ 11 and has evolved since then based upon new needs and new sources of data. Defining Cybersecurity has been an iterative and incremental process that involves:

- Desk research to identify existing literature, industrial definitions, coding systems or experts
- Collation of existing sources (often fragmentary because they are prepared for a different purpose) to produce a comprehensive definition of the sector

- The creation of high level (sub-sector) headings under which the detailed product and service activities can be grouped
- Source- checking, to ensure that enough data sources can be found to produce robust metrics for each product/ service activity.

In the first case, as mentioned previously, there were no available taxonomies or dedicated sources of economic data for the original Cybersecurity research. Therefore, the research approach included several stages:

- Scoping the broader economic sectors of ICT, Defence, Telecommunications etc. within which Cybersecurity activities reside
- Isolating and then validating those activities from the broader sectors that fit with the proposed definition of Cybersecurity i.e. between data protection against deliberate rather than accidental threat
- Examining the data and sources within those sectors to construct an evidence base of sources that can be used to measure Cybersecurity
- Examining the data and sources further, to ensure that the Cybersecurity content of the sector activities can be clearly differentiated from economic activities that are generated due to other reasons
- The creation of decision trees/ rules sets and economic models to include supply and value chain activities that contribute to Cybersecurity products and services that may originate from other sectors

This was an iterative "bottom-up and top-down" process including firstly, the search for evidence that fits the "ideal" definition of Cybersecurity and secondly, the inclusion or omission of aspects of the "ideal" definition per the robustness of the available evidence. The result was a pragmatic definition that only includes economic activities for which multiple sources could be identified. These sources, eclectically drawn from a variety of sectors and a wide range of institutions, are listed at Appendix I.

One limitation of this research process is that a sector definition will only include product and service activities that have a traceable economic footprint i.e. a form of trading history. Publicly funded or academic research and any developments that have not yet reached the market are not included in the sector definition. This is partly due to our philosophy of only including measurable activities and partly due to the nature of the industry and market- focused sources that we access.

Managing Boundaries

Once the sector boundaries have been defined, the key issues become:

- How to ensure that only relevant activities are included (see Section 0)
- How to maintain the boundaries over time.

The process utilises data flags across a wide range of economic measures and performance benchmarks to track incremental and step change in Cybersecurity activities. This is an historical rather

than a forecasting process that measures change after it has happened and then flags the change so that a decision can be made to a) add to the current definition, b) re-group activities, c) monitor for further change or d) do nothing.

In the case of new activities (rather than increases in existing activities) then a rule- set is applied that questions:

- Is the new product/ service an immediate and beneficial replacement?
- Does the new product/ service provide robust short and medium term financial benefits?
- Does the new product/ service provide robust short/ medium term security benefits?
- Does the new product/ service provide a solution to new requirements in law or regulation?

Data to inform progress through the decision gates is then drawn from a variety of market, technology, supply chain and procurement sources. Applying the decision gates is a question of balance- too strict an application may substantially diminish the reported size/ value of the sub-sector and too lax an application may result in too little differentiation and over- reporting.

The decision on when to refresh sector boundaries and update definitions is generally conducted on an annual basis and is usually applied to the most current year and is back-dated to previous years when there is sufficient data to do so.

Creating a “Language”

The process of defining a new market/ sector quickly reveals the international differences in product and service descriptions and in Industrial Classification codes (assuming they are relevant). This is a significant barrier for traditional and new sectors alike. The international debate around defining the Green Economy is at least 15 years old (with no widely adopted and measurable definition agreed yet) and the Bio technology sector underwent several re-definitions in its first 10 years. This is due to both "boundaries" and "language."

To achieve a sector definition that is relevant, quantifiable and comparable on a global basis, the research process must:

- Identify the different product and service descriptions across different industries and international economies
- Group the different descriptions together
- Create (or adopt) a description or label that is universally applicable.

The search for a useable product/ service language often includes sources like Logistics, Shipping, Procurement, Insurance, Finance, Legal and Consulting applied to a wide range of vertically defined sectors- ICT, Transport, Electronics etc. For more mature sectors the product & service "language" is more developed and more widely accepted across different countries. For emerging sectors, this is less true and activity labels often need to be created.

The service "labels" that are carried forward into the current Cybersecurity taxonomy have, therefore, been adopted or constructed from available descriptions and have been made as relevant as possible to the underlying activities that each label includes- whether this is from a supplier or purchaser perspective. This is "bad" in that no single country or trading bloc (like the EU) can easily relate the descriptions to an existing classification system but it is "good" because it creates a data set with activities that are universally relevance and traceable.

Developing the Rule- Sets

Once the Cybersecurity activities were identified and then organised, the next stage was to generate the rule-sets and filters for the source data included in the development of the metrics. Rule- sets are important because they determine what economic activity is included in the sector analysis AND how the value of that activity is estimated. In some cases, this is straight forward and in other cases this may require the separation of Cybersecurity from Security or other services like ICT. One factor in developing and applying filters is that they improve over time, either through usage or through improvements in the data sources used as part of the filtering process.

Several filtering processes need to be employed in different combinations across the Cybersecurity definition if only relevant activities and values are to be included. This is where the multi- source approach has distinct advantages over industry classification systems that generally focus on "what" an activity is rather than "how," "why" or even "where" it is used. Multi- sourcing enables the use of additional data sources that can provide answers to these questions.

The first stage of filtration was to ensure that only activities clearly identified as Cybersecurity were included. The second stage of filtration was to find sufficient confirmatory evidence of "purpose or intent" (generally through data sources relating to procurement across the multiple sectors) to be able to determine whether a product or service has been used for Cybersecurity (rather than Cyber Defence). To derive usable data specifically about "purpose" often requires quite detailed disaggregation of product/ service data to ensure that only Cybersecurity activities are included and to exclude any over- reporting due to the inclusion of unrelated activity value.

Figure 63 : Disaggregation Model



This means researching activities often at deeper data levels (Level 6 to 7) to determine their more detailed characteristics (the "how", "where" or "why" answer), excluding unwanted activity values and then re-summarising the analysis at Level 5.

This double- filtration process addresses the issue of Cybersecurity activities being accounted for differently in different sectors.

The quality and appropriateness of data sources (once they were identified) varied widely in terms of not only what they included in their definition of Cybersecurity but also in their granularity of detail. In some cases, reported data was clear and Cybersecurity sales (for example) were accounted separately, however in others the sales figures reported included several other aspects not classified as Security (this is most often true of Cybersecurity activities). In cases such as this there is a need to triangulate with data sources outside of the Cybersecurity industry. Recording and reporting practices within the source materials varied on an industry-by-industry basis.

Cybersecurity activities are conducted by companies that are specialist to the Cybersecurity sector and by companies that are non- specialist but operate within the Cybersecurity supply chain. The source data, therefore, includes:

- Companies that solely provide Cybersecurity products and services (anywhere in the value chain)
- Companies who (amongst other activities) provide components or inputs into sub-assemblies or final assemblies of Cybersecurity products and services.

The "rule set" or threshold for including a company in the analysis is if at least 40% of sales activity can be directly attributed to the Cybersecurity sector (as defined within this methodology). In the case of larger companies this can often be extracted from financial reports, cross referenced to industry sources. For much smaller companies, it may be necessary to extrapolate the percentage of sales based on product range and turnover, tempered by more detailed case materials that we hold about the market performance of similar businesses. The exception to this 40% rule is for large companies where a small proportion of overall sales is a significant contribution to the Cybersecurity sector. However, this rule set can be changed at any time for different analytical requirements.

This threshold means that the sales, company numbers and employment figures published in the CIMA report focus upon the significant value- creating "core" of the Cybersecurity sector. This core is where true economic value is measured and this focus avoids (as far as is possible) any double counting of sales value within the supply chain.

Generating the Values

At the heart of the research methodology (Stage 2 of Figure 62 : Market Research Model) is a rigorous but flexible approach to measuring economic activity using multiple sources for multiple metrics. This methodology has been widely applied to both existing and "new" markets and sectors.

With no definitive sources of data or analysis as a starting point (as noted above), the key research task is to identify meaningful and multiple sources of transactional (and other) data and use this to a) construct and b) populate a detailed and segmented model of the market/ sector that transforms the available evidence from singular and fragmented insights into structured observations. The stages for this have been outlined above.

Much of this transactional and other data is already in the public domain, although it requires the corroboration of multiple sources and triangulation between different sources (financial, legal, academic, industry, trade association, procurement, government, etc.) before it can be validated and

transformed into usable data. This process (data triangulation and the use of "proxy" data) is at the heart of a "big data" research methodology that either:

1. Selects from multiple sources of pre-existing data (mature sectors)
2. Selects from more limited sources of pre-existing data and adds triangulated data to achieve more robust results, or
3. Finds no pre-existing sources and uses triangulated data to create the sources necessary for analysis (emerging sectors).

The Security dataset started at (2) and moved to (1) whereas Cybersecurity started at (3) and is moving towards (2).

Box 1: Triangulation Example

Corporate governance for climate change. The consulting sector data shows that in 2010/11 250 major corporates commissioned work (the consulting data rarely shows value for commercial reasons). Investor relations and fund management sector data shows that overall GBP 8.75 million was spent on work and in addition trade associations data reports independently that some GBP 9.2 million has been spent.

Triangulating data from the different sources makes it possible to arrive at highly accurate estimates of value and volume that are just not possible from consulting a single source, however authoritative that source may be within its own sector

In some cases, a single sub-sector may require all three approaches to capture the full range of economic activities. Box 1 summarises the triangulation process use for (2) and (3) i.e. how this involves identifying, evaluating, interpreting and transforming multiple data sources into new values that can then be tested, analysed, modelled and reported.

Market activities are only included within the Cybersecurity data framework when there are multiple sources of reliable data (nothing is single sourced- ever). These sources are screened to remove duplicate references to any single source and then shortlisted by removing outliers and unreliable sources. This shortlist is then screened again until some consistency in value is achieved. From the remaining sources, a value is then calculated and published. Values created in this way are then "reality tested" by comparing activity values within and across economic or industrial sectors, with recognised industry benchmarks and, ultimately, government statistics (if they are available). Example of this process are demonstrated as "deep dive" data examples (see below) and data triangulation is illustrated by Case Study 2, which is taken from a different sector but is a very good example of the triangulation process applied to an established product.

Case Study 2: Data Triangulation

We mentioned three methods for creating values previously ...

Rich sources of existing data	• Example= environmentally friendly water pumps • Lots of industry data sources but SIC codes do not fit • Multi- source, calculate mean value & confidence level • Triangulation of sources within a single metric
Some sources + Triangulation	• Example= domestic tanks • Some data on tank sales, but not "end-of-life"- SIC ≠ volume • Validate triangulated sources on repair etc and align with sales • Calculated mean etc by triangulating across limited metrics
Triangulation only	• Example= Road maintenance due to Climate Adaptation • Minimal data, Adaptation inferred rather than reported, no SIC • Validate triangulated sources across transport, insurance, finance, construction, procurement etc • Calculated mean etc by triangulating across many metrics

What is the environmental risk of leakage from single skinned domestic oil tanks and the costs/benefits of their replacement with new dual skinned tanks with leak- monitoring technology?

When there is no single source of information about the installed base that can be consulted

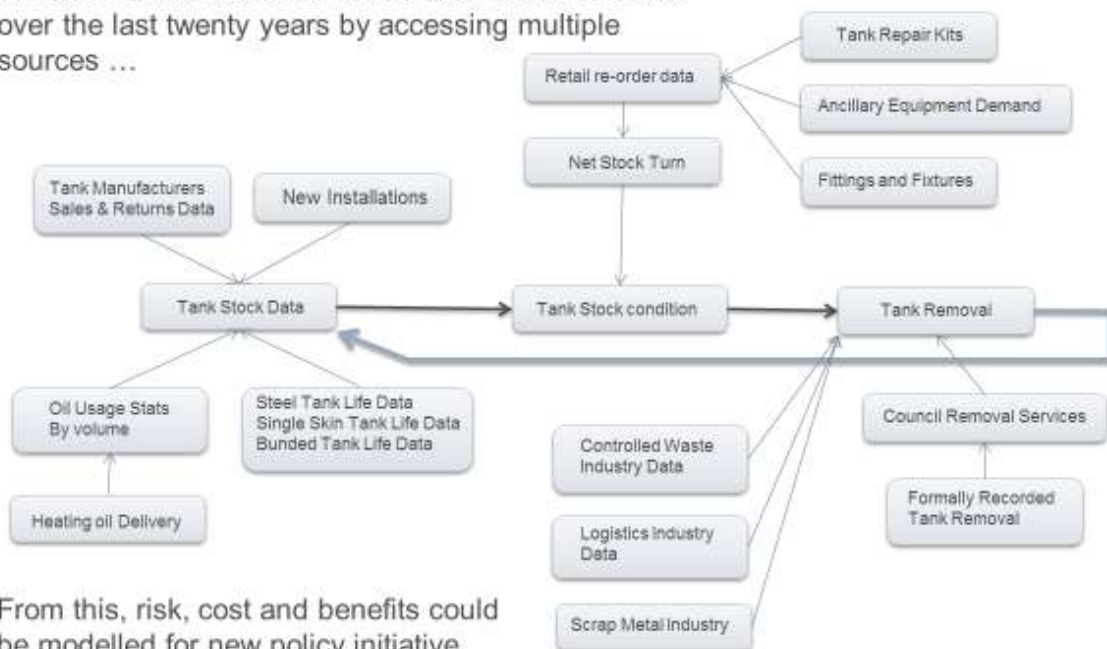
There is no industry body, so records are incomplete & fragmented

Current records are most accurate, but the least likely to reflect tank failures

There is no legal requirement to collect or share this information

There is no monitoring regime in place

We were able to estimate the installed base of tanks over the last twenty years by accessing multiple sources ...



From this, risk, cost and benefits could be modelled for new policy initiative

All research produced in this way is delivered with levels of data confidence assigned. Data confidence levels are a mathematical function of the spread of values across the range of sources that we include in our analysis. Confidence levels vary by activity, measure, geography and by forecast year. Typically, a confidence level of above 85% is achievable over time, which means that corroborative sources vary around the mean value by +/- 15% (see Section 0).

Data Sources

The underlying research methodology attempts to limit the risk and error behind the published numbers (whether historical or forecast) by multi-sourcing and monitoring a wide range of reliable and robust sources and then making the remaining range of uncertainty explicit. A full list of sources is provided in Appendix I of the Methodology but each analysis data template for Cybersecurity research calculates and publishes the number of sources used to compile the values for each row of market data for each country. Across the Cybersecurity research this figure averages 95 sources (ranging between 30 and 600 sources depending upon the market activity) for each line of data.

This source count, embedded in each data line, is representative of the volume of sources used- with the Sales value typically requiring the greatest number of sources. Other data points for the same product/ service will have their own source count, which may include a different number and mix of sources compared with other data points. Typically, sales, exports and growth forecasts use substantially different data sources for their calculation. For brevity, only the one source count is shown in the Cybersecurity data set. This combination of multiple sources means that the "formula" behind each data point is unique and that no single-source attributions are made within the data set.

Section 0 explains why the research uses multi-sources its quantitative data i.e. to offset the limitations of standard industrial codes. There are comprehensive internal and external quality assured processes for monitoring and rating data sources before they are included in the source management system. Across the various stages of analysis, checks and balances are employed that enable the capture of meaningful and multiple sources of transactional (and other) data that can be used to a) construct and b) populate a detailed and segmented model of the market/ sector and that transforms the available evidence from singular and fragmented insights into structured observations.

This data is collected from a very wide range of sources- some are core to the system whilst others relate to individual markets and sectors. They include:

- Company data- FAME, Dun & Bradstreet, Companies House, Hoovers Online, ICC, Thomson, Companies Online, OneSource
- Journals- Bloomberg, Forbes, Business 2.0, Economist, Wall St Journal, FT, Business Week
- Industry Associations- EEF, NTOs, Industry portals. CISP etc.
- Professional Bodies- Institutes, Chartered Bodies, Associations, Societies, Federations
- Market Research- Keynote, Data Monitor, FT, Reuters, Economist Intelligence Unit, Gartner, Frost & Sullivan, Mintel, OECD, IEA, World Bank
- Industrial Benchmark Information- Data Monitor, Windhaus, Integra, UCSD, DTM Corporation, analysts own benches, Harvard Business School, MIT Bench Series, Cranfield University etc.

Sector- specific sources vary and include additional academic, financial, professional, logistics, legal and transactional sources. The balance between general and sector- specific sources varies for each sector but is generally weighted strongly in favour of sector sources.

New sources emerge daily, but are subject to an incubation period within the source management system before they become active. This establishes the frequency and credibility of the source before it is used as part of any analysis. Typically, each annual data update may exclude some old sources and include some new sources (the number is monitored each year) but the volume of sources used ensures that source changes generally improve the quality of the data rather than introduce erratic effects in the year-on-year trend analysis. This is reflected in the annual improvements in data confidence levels. So, while the volume of sources used on an annual basis may not change significantly, the nature of the sources and their quality does change due to the regular housekeeping within source management.

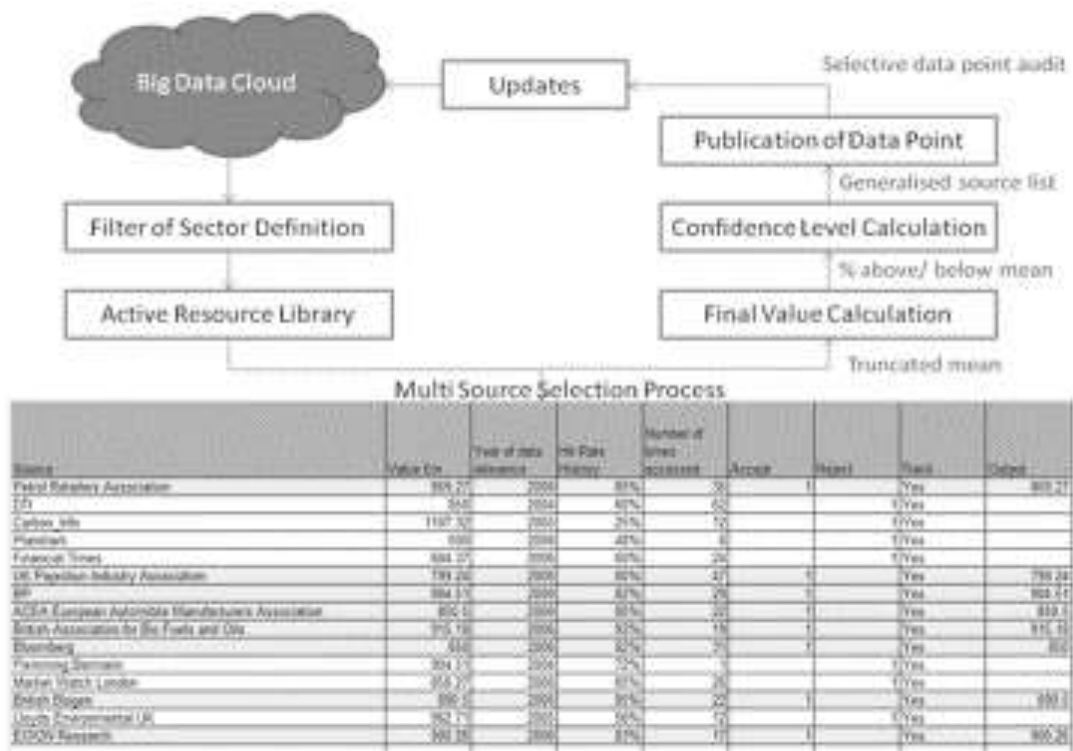
The use of sources to calculate specific data points was illustrated above, but the Cybersecurity data set contains a large volume of data points. To demonstrate how often specific data sources are used across a whole data set, an example is included at Section 0 to identify how often a source has been used, its “Hit Rate” and the economic metrics that it has been applied to. These source metrics give a sense of “preferred” or trusted sources and sources that have more general (rather than very specific) applications i.e. it gives some “weight” to how sources are used rather than “weighting” the sources themselves. The methodology does not “weight” sources by their name or reputation, nor does the system attempt to extract and analyse the assumptions behind the sources published values. Rather the multi- source methodology is based upon the volume of valid sources, the consistency in quoted values and the sources tested track record. It is, unapologetically, a case of quantity over quality, although quality does ensure that sources are used and re- used where they are appropriate.

Source Management

The source management system is shown at Figure 64. It tracks data sources over time. For each source, there is a history based upon source name, source value, year it relates to, the number of times used, “hit rate” (reliability) and whether it is to be accepted for a specific research purpose. The source data banks are fully transparent and auditable and relate to each calculated cell within any sector data set. These data banks are monitored closely internally and are routinely spot- checked each year by staff and clients as part of the peer- review audit.

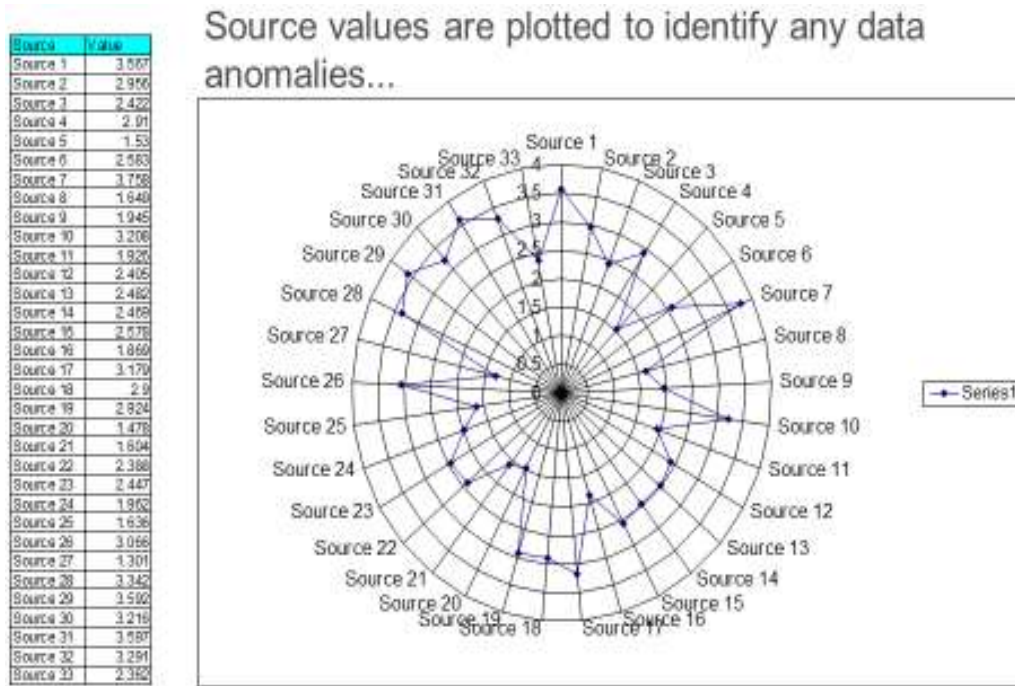
The Figure shows that data sources are filtered according to their relevance from a much larger data “universe.” The filtering process for Cybersecurity was described above, although it is possible to have multiple templates “in play” at the same time. The filtering process leads to sources being validated and accepted into the Source Management system *for that sector*. Sources can be relevant to many different sectors. Once accepted into the Source Management system, sources are tracked and assessed in preparation for, or between, uses. Those uses may be for a single or multiple data points that apply to single or multiple products and services in one or several countries.

Figure 64 : High Level Diagram of the Source Management System



Inclusion in the Source Management system does not mean that a source is automatically used. For each data point a set of sources are identified. This set of data sources is then assessed both automatically and by analyst intervention to determine the final set of sources/ values that will be used (see Figure 64). The values for each calculated data point are listed and visualised using radar diagrams that show the levels of variation in the values and it is at this point that the decision is made to include/ exclude sources, whilst ensuring that sufficient sources remain to provide a suitable spread of values.

Figure 65 : Sample Radar Diagram for Source Value Analysis



The radar and the associated list of values form the basis for the final data point calculation. This is taken as the mean value of those listed.

The confidence level for the value is then calculated by showing the variance between the mean value and the upper/ lower values in the final source list. This variance is shown as a percentage.

Source Usage

The sources that have been used to date for the Cybersecurity research are listed at Appendix I. This listing is for source names only. The source list illustrates a wide range of local, national and international sources that have commissioned/ undertaken and published relevant data and research. The sources include a cross section of different industry/ trade associations, financial institutions, market research organisations, environmental bodies, professional services, government agencies and some academic sources- amply illustrating the basis for multi- sourcing.

To illustrate how sources can be applied to the calculation of multiple data points, a “deep dive” example is enclosed at Section 0. The example includes only sources that have been used in the calculation of at least 11 metrics in the global data set. There are many other sources that did not meet this criterion that have been excluded from the list. Many of the sources included in the list will have been used to calculate more than 11 metrics, but for practical purposes we have reported the first 11 uses only.

Figure 66 : Example Sources

Source	Data Usage Type	Hit Rate for Metric	Metric	Times Used
A	International	91.90%	ROC	468
	Triangulation	81.90%	Head Count	
	Triangulation	60.00%	Head Count	
	International	71.10%	Available Market	
	International	Out of Range	ROS	
	International	95.60%	Import Value	
	Localised	75.20%	Sales	
	International	93.90%	ROS	
	Triangulation	73.30%	Growth	
	Triangulation	73.30%	ROS	
	Localised	68.40%	ROC	
B	Localised	88.90%	Sales	1550
	Triangulation	78.80%	ROC	
	Triangulation	65.90%	Import Value	
	International	71.60%	ROC	
	Localised	81.70%	ROC	
	Triangulation	75.50%	Available Market	
	International	75.30%	Head Count	
	Localised	94.60%	Available Export	
	International	79.70%	Head Count	
	Triangulation	89.30%	ROC	
	Triangulation	84.20%	Growth	
C	Triangulation	87.60%	ROS	262
	Triangulation	81.80%	ROS	
	International	62.90%	Sales	
	International	96.50%	ROC	
	Triangulation	97.40%	Import Value	
	International	64.80%	Available Export	
	International	72.00%	Head Count	
	Localised	72.80%	Sales	
	International	Out of Range	Available Export	
	Triangulation	75.40%	ROS	
	Localised	85.70%	Growth	

For each source and each of the listed metrics we have included Data Usage Type (3 options) and a hit rate (see three example sources at Figure 66). The Type category includes 3 options:

- Triangulation (as described in Case Study 2) is more of a complementary or “indirect” source that has been used to compensate for a lack of "direct" sources and can either be local or international
- Localised means that a source has been used at city or national level in conjunction with other sources of a like nature (i.e. no need to triangulate)
- International means that the source has been used in conjunction with other sources of a like nature (i.e. no need to triangulate) and may relate to a measure of international trade but may also be an international source used to calculate a localised measure

The "Hit Rate" is our measure of confidence in the source based upon historical usage and is specific to the metric in question. So, a single source can have multiple Hit Rates depending on context. An "Out of Range" statement shows where a source has been included for an initial calculation but was

subsequently rejected for the final calculation. A specific % value shows where the source is in- range. So, the “B” example in Figure 66 shows 11 metrics and Hit Rates between 71% and 94%. All three example sources are international, so the “Localised” count is low.

The “Times Used” column relates to the total historical uses of that source. The value in this column is significantly higher than the number of metrics shown for that source. This means that the source has been used for calculating the listed (and other unlisted) metrics for multiple countries. The range for “Times Used” is from 37 to 228.

The example “deep dive” provides greater transparency in how sources are used across data sets and acts as a guide for how sources are used in the Cybersecurity research. It shows that:

- Some sources are used more than others (Hit Rate = our confidence in the source compared with other sources)
- Sources are only used when they are relevant to a specific metric
- Sources may be used in different ways i.e. for triangulation in one calculation or as a “core” value in a different calculation
- Sources are rated per metric rather than across the board i.e. our use of them is discriminate
- Sources are always “context specific” i.e. that metric for that activity for that country.

While the example falls short of full disclosure of all sources and how they are used it does suggest a development path for further analysis of sources, in their own right, rather than as an input into specific data points. This “meta- data” analysis about sector sources would focus on the change in source volume and quality over time, change in the use of sources, changes in the rate of triangulation as new sources enter the market, reliability of specific sources in a specific activity/ country context and the impact of highly utilized sources on the data set.

Multi- Source Process for Deriving Values- an Example

The best way to illustrate the full process outlined in Sections 0 - 0 is through a detailed example. This example, using a single data point from within the 2015 Security & Cyber Sector statistics, demonstrates how the multi- source approach can be used to calculate sales, export, growth and other values²⁰. The multi- source approach includes six stages:

1. Select the data point
2. Identify the source data
3. Select sources for further analysis
4. Triage the sources to achieve a more consistent range of values

²⁰ This example was used in 2015 as part of the UK Government audit process for the 2015/ 16 Security “stats” release.

5. Calculate the mean value from the sources
6. Calculate the data confidence level.

Stage 1 involves selecting the data point. In this example, the data point is UK exports to the USA in Malware Forensics for Commercial Applications. This sits within the UK Export data set within the following data hierarchy: Security & Cyber>Cyber> Anti Malware>Specialist Anti Malware> Malware Forensics. It is one of five options for Malware Forensics: Commercial Applications, Public Organisations, Specialist Advisors, Specialist Research and Specialist Applications. This data point is one of 4,000 different products and services measured within the Security (including Cyber) Sector.

Stage 2 involves identifying the data sources that are relevant to the calculation of the data point. A full list of 260 sources were consulted for this data point. These sources are UK, USA and International and include research, company and other sources relevant to the investigation of Malware Forensics.

Stage 3 involves an initial sort and selection from the full list of sources to identify those of the most direct relevance. Forty- four sources were ultimately selected and these are shown at Table 4 and are labelled Source 1 through to Source 44 (in the original submission to UKTI these sources are named and not anonymised).

Table 49 : Data sources

Source	Nationality	Value Reported £ Sterling (converted)	Year of data	Hit Rate History 5 yrs %	Number of times accessed
Source 1	International	2.09	2015/16	81.9	52
Source 2	US	2.16	2015/16	87.6	78
Source 3	UK	2.86	2015/16	83	78
Source 4	UK	2.53	2015/16	87.6	100
Source 5	UK	3.03	2015/16	73	49
Source 6	US	2.68	2015/16	94.9	62
Source 7	UK	2.35	2015/16	69.8	87
Source 8	UK	2.48	2015/16	80.3	98
Source 9	UK	2.54	2015/16	91.8	67
Source 10	US	2.55	2015/16	73.7	42
Source 11	UK	2.62	2015/16	85.9	124
Source 12	UK	2.46	2015/16	75.6	21
Source 13	UK	2.51	2015/16	90.7	21
Source 14	US	3.02	2015/16	68.9	113
Source 15	US	2.27	2015/16	87.9	26
Source 16	US	2.12	2015/16	92.1	105
Source 17	US	2.20	2015/16	68.5	39
Source 18	International	2.46	2015/16	67.4	106
Source 19	US	2.17	2015/16	84	49
Source 20	US	2.87	2015/16	78.8	122
Source 21	UK	2.40	2015/16	81	45
Source 22	UK	2.19	2015/16	76.4	124
Source 23	UK	2.72	2015/16	77	91
Source 24	UK	2.35	2015/16	74.2	28
Source 25	UK	3.07	2015/16	72.4	62
Source 26	US	2.68	2015/16	91.4	111
Source 27	US	2.66	2015/16	78.4	111
Source 28	US	2.27	2015/16	78.9	75
Source 29	UK	2.88	2015/16	92.3	57
Source 30	UK	3.05	2015/16	89.1	28
Source 31	US	2.20	2015/16	69.8	124
Source 32	US	2.57	2015/16	80.6	95
Source 33	US	12.92	2015/16	36.1	30
Source 34	US	11.20	2015/16	43.4	88
Source 35	US	1.40	2015/16	25.2	11
Source 36	US	3.50	2015/16	42.8	122
Source 37	International	21.60	2015/16	31.1	8
Source 38	International	5.30	2015/16	44.9	9
Source 39	US	8.40	2015/16	23.5	47
Source 40	International	11.20	2015/16	29.5	95
Source 41	US	12.92	2015/16	37.7	73
Source 42	UK	1.10	2015/16	40.2	51
Source 43	US	12.92	2015/16	31.2	14
Source 44	US	12.92	2015/16	24.3	85

Their selection depends upon several factors stored within our source management system (columns 3-6 of Table 49). These are:

- Value- only sources showing proximate values are included
- Year of data- ideally sources should be current
- Hit rate over the past 5 years- level of assessed accuracy for this source over 5 years
- Number of times accessed- number of times this source has been used previously for this purpose i.e. same data point different years, identical data point different country etc.

The Table shows that the 44 sources were all current, with values between GBP 1 million and GBP 22 million, had hit rates of between 20 and 90% and had been accessed previously between 10 and 120 times each. All the values in the data set are unique, which means that multiple sources that may quote the same value (possibly from an identical source) are eliminated from the final selection.

Stage 4 of the process involves “smoothing” the results by excluding the outlier values from the final calculation. Table 50 shows that sources 45 to 63 were excluded from the analysis due to a combination of factors (shown as summary statements in column 9). These factors include:

- Value too high
- Value too low
- Low count (unsure of reliability)

Table 50 : Rejected Sources

Source 33	US	12.92	2015/16	36.1	30	NO	Out of range (definition error)
Source 34	US	11.20	2015/16	43.4	88	NO	Out of range
Source 35	US	1.40	2015/16	25.2	11	NO	suspect out of date
Source 36	US	3.50	2015/16	42.8	122	NO	Out of range investigate
Source 37	International	21.60	2015/16	31.1	8	NO	Out of range
Source 38	International	5.30	2015/16	44.9	9	NO	Out of range
Source 39	US	8.40	2015/16	23.5	47	NO	Out of range
Source 40	International	11.20	2015/16	29.5	95	NO	Out of range
Source 41	US	12.92	2015/16	37.7	73	NO	Out of range (definition error)
Source 42	UK	1.10	2015/16	40.2	51	NO	Out of range
Source 43	US	12.92	2015/16	31.2	14	NO	Out of range (definition error)
Source 44	US	12.92	2015/16	24.3	85	NO	Out of range (definition error)

The effect of these exclusions is shown using the radar diagrams at Figures 8 and 9. These are a feature of the QA system that quickly visualize possible data problems.

Stage 5 involves the calculation of the mean value from the final list of 32 sources, now ranging between GBP 2.09 million and GBP 3.07 million. This mean value is GBP 2.56 million the value quoted in the Security & Cyber Sector data set.

Figure 67 : Radar Diagram all 44 Sources

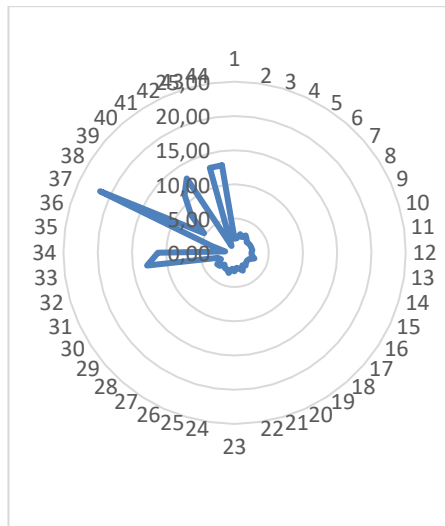
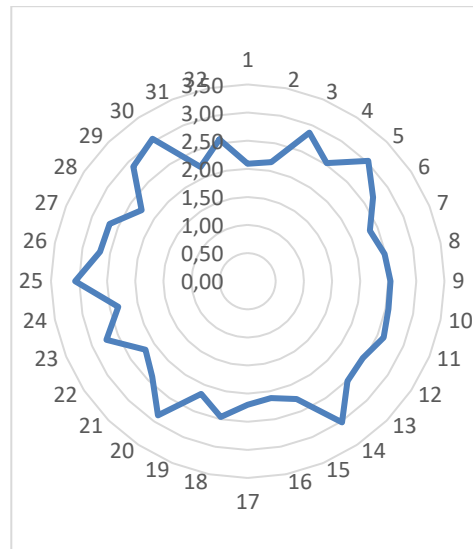


Figure 68 : Radar Diagram Final 32 Sources



Stage 6 calculates the confidence level for the data point. In this case it is the difference between the mean (2.56) and the highest and lowest values in the final data set. In this case the confidence level is 82% i.e. there is an 18% probability that the value could be as high as GBP 3.07 million or as low as GBP 2.09 million. Confidence levels for all values in the Security & Cyber sector data set are provided annually to UKTI to help ensure the accuracy of the research.

Stage 6, however, is not the final stage of analysis. Each data point that progresses through this process is then subject to further checks that ensure that the data point value is consistent with:

- Values in previous year's UK exports to the USA of the same service
- Comparative values of UK exports of same service to other countries
- Comparative analysis of export values as a proportion of UK Sales value of same service (over several years)
- Comparative analysis of export values when related to other Cyber services in the same category or family of services
- Analysis of historical growth trend in export value when compared with forecast growth values for exports
- Consistency in sales/ export trends over time
- Consistency in confidence levels over time.

Where any uncertainty about the final data point remains, this may be due to either market uncertainty or data uncertainty. In the case of market uncertainty, the value remains unchanged but is explained within the context of the Security & Cyber annual report. In the case of data uncertainty, then Stages 1-6 are repeated, but this time with additional or alternative data sources.

Because this process is so central to the methodology and how data values are created, a further three “deep dive” examples are included at Appendices for sales, employment and growth in France, Germany and Italy.

1.1.121 Data Alerts and Flags

All data points within the Source Management system, both new and old, are equipped with “data flags” that are activated every time data is updated. While every attempt is made to ensure that sources are robust and that calculations are accurate, abnormal figures can occur within the data set. This could be the result of error, the inclusion of new and more accurate sources or it could be an actual unusual event i.e. a significant uplift or decline in a value beyond the assigned parameters. Whatever the case, data flags provide another level of quality control, so that errors can be trapped or events recorded. Data flags can vary, but typically flags will capture the age of the data, the date that it was last updated and set a range within which we would expect values to fall. Exceptions that fall outside of the range are investigated individually.

Data flags enable us to identify and monitor incremental changes (weak signals) and trends (even across very large data sets) that might be early indicators of a change in market drivers or of a process step change in an industry. Typically, data flags provide early warning to corporate clients of changes in their industrial and competitive environment, but they can also be applied to sector level analysis—as identified in Section 0, where changes in activity can lead to the creation of new sub-sectors and the consolidation of fragmented activities.

1.1.122 Levels of Data Confidence

All the data values in the Cybersecurity research are created by the intelligent use and transformation of primary and secondary data sources (outlined above). Data sources are carefully managed by measurement and rating of their accuracy and reliability over time, and by excluding sources that are outdated or without a measurable track record. No less than seven qualified sources are ever used and often the final list of sources is much higher than this. As described above, a mean value is calculated from these selected values and this is assigned a level of data confidence based upon the variance in the final source list. The aim is for an average level of data confidence of 85%.

A level of data confidence is a balance between risk and reward. A very high data confidence level can be achieved by excluding most sources from the range or by conducting very high levels of source-search. A low data confidence level reflects either a legitimate high level of market uncertainty, very few available sources or a lack of rigour in the source analysis process. By aiming for an 85% data confidence level, supported by a significant number of sources, the intention is to maintain a balance between the range of sources and the consensus within those sources. The focus in the research process is to obtain an across-the board level of data confidence rather than attempt to achieve 100% confidence in any one set of numbers. This means that the search for sources for a specific data point will stop when it falls within the required range and that it continues for data points that fall outside the required range. So, the fact that so many levels of data confidence look similar is not an accident of the methodology, rather it is the desired outcome.

As each data point has its own set of sources, so each data point has its own level of data confidence. Data confidence levels can vary according to how mature/ emergent a product/ service is and how mature the reporting systems may be in/ for any given country. Developed nations typically have a wider range of robust sources to choose from. The minimum level of sources for emerging activities/ countries is seven (based upon years of research) and below that activities or countries tend to be excluded (but monitored over time for additional sources).

For the current Cybersecurity data, a full set of confidence levels have been provided by end- user industry and by EU country. Figure 69 show the aggregate level of data confidence for each sub-sector for two confidence levels- sales (horizontal axis) and forecast growth (vertical axis). The size of each bubble represents the relative value of the EU. The mean value for the sales confidence level is 86% and for sales growth is 83%. Figure 69 shows that confidence levels for individual sub-sectors vary between 82- 86%, reflecting the differing qualities of data and sources available for each sub-sector.

Figure 69 : Confidence Levels by Sub-sector

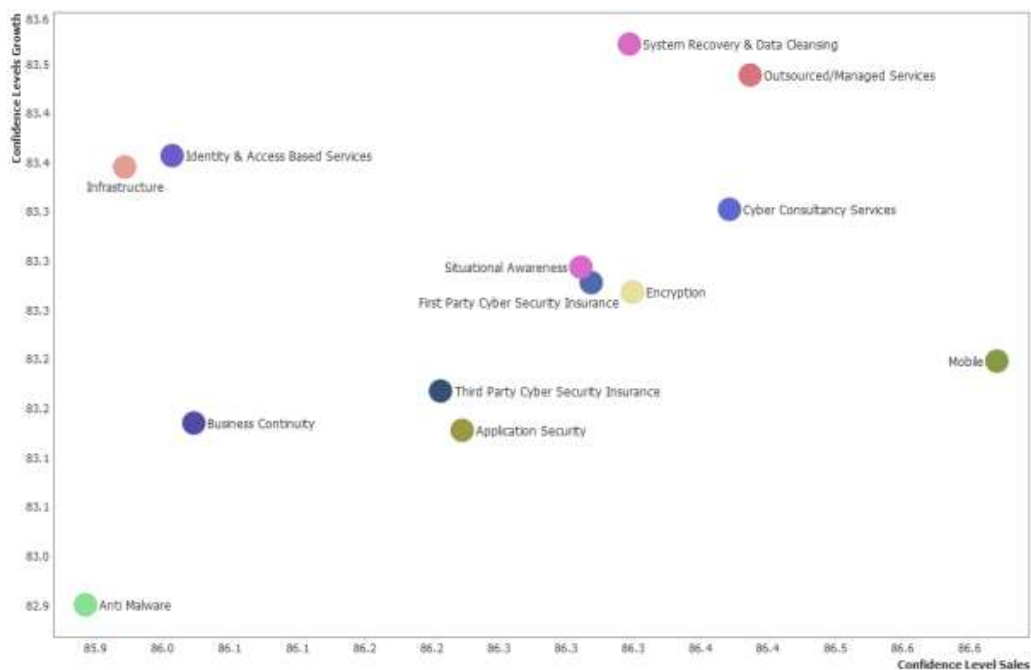
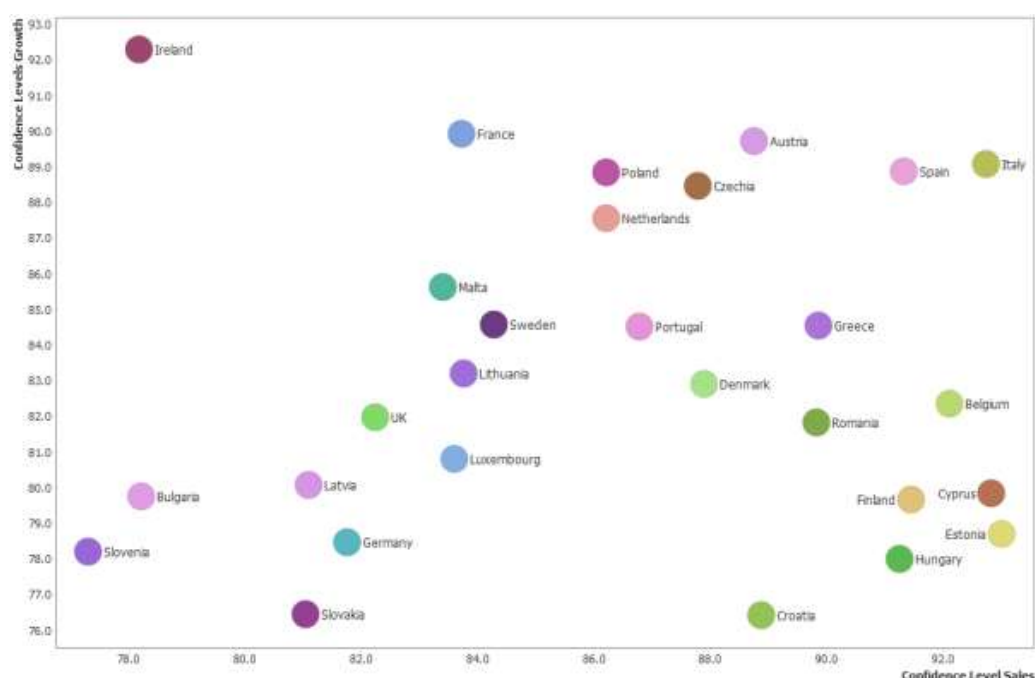


Figure 70 shows confidence levels for EU Sales and Sales Growth by country. The mean value for the sales confidence level is 86% and for sales growth is 83%. It shows that confidence levels for individual countries varies between 76- 93%, reflecting the differing qualities of data and sources available for each country.

Figure 70 : Confidence Levels by Country



1.1.123 Metrics

The research includes a wide range of metrics that have been developed and tested over many years. The full set of metrics are listed below in Table 51, with a title, a definition and a brief comment on when the metrics can be used. The metrics are divided into foreground metrics (to be analysed as part of the CIMA research) highlighted in red, and the background metrics (scanned for areas of interest and reported as necessary) in black. The values for each metric are all calculated using the multi-source methodology outlined in Sections 0 to 0.

Table 51 : Full List of Metrics

	Metric	Description	When to Use
Sector Related Metrics used for Economic	Sales (m EUR)	Measure of economic activity by identified companies and their supply chain within a defined country, based upon where the economic activity is delivered from rather than where it is reported.	Standard measures of sector economic performance by value, enabling comparison of activity values within a sector and comparison with other sectors.
	Available Market (m EUR)	Available market represents the proportion of the total market that is available for penetration at the normal cost of sales i.e. that is realistically available for penetration and is not currently dominated by major players.	
	Export (m EUR)	Measure of goods and services that travel from a source country to another country that may either be complete in their own right or become incorporated into a new product or service.	Economic values can be routinely updated to

			provide trend analysis and benchmarking with other countries
Export Available (m EUR)	Export available represents the proportion of the total export market that is currently not dominated by major exporters and therefore is available for market penetration at normal cost of sales.		
Export as % of Sales	A measure derived from the above that reflects the relative "export intensity" of different products and services market		
Imports (m EUR)	Measure of goods and services that originate from sources outside of the country that may either be complete in their own right or become incorporated into a new product or service.		
Domestic Market (m EUR)	Measure of the domestic market (i.e. consumption) within a country, based upon a formula of Sales - Exports + Imports		
Imports as % of Domestic Market	A measure derived from the above that reflects the relative "import intensity" of the domestic market for specific products and services		
Sales as a % of GDP	A measure derived by comparing sector sales with country GDP	Collectively, these measures "position" a country in terms of competitiveness and performance	
Global Market Share %	A measure derived from comparing country sales with global sales		
Global Share of Exports %	A measure derived from comparing country exports with global exports		
Exports by Country (m EUR)	Value of exports to a specific country	Collectively, these measures identify significant trade flows with other countries and identify strong export links.	
Imports by Country (m EUR)	Value of imports from a specific country		
Share of Country Exports %	Value of national exports to a specific country compared with total exports to that country. Can also be expressed as a % of the Domestic Market of that country		

Companies	Measure of the total number of companies in a country that are either core to the delivery of sector products & services or form an integral part of the supply chain	Along with Sales, these are the three key economic measures applied to domestic performance
Total Employment	Measure of the level of employment, in Whole Time Equivalents (WTEs), across core and supply chain companies involved in delivering sector products & services	
Management Employment	A proportion of total employment involved in managerial functions	Employment grouping relate to standard occupational classification. Rarely used in our analysis because of their generic nature. Where an occupation split is required on a national or regional basis, we generally create our own occupational/ skills profile at a more detailed level.
Supervisory Employment	A proportion of total employment involved in supervisory functions	
Admin Employment	A proportion of total employment involved in administrative functions	
Other Employment	A proportion of total employment involved in functions not listed above	
New Product Sales (m EUR)	The value of new products or services entering the market on an annual basis. This gives an indication of the rate of new technology adoption and the introduction of new concepts.	These two measures are often used to assess the market for new technologies. They also provide a better measure of possible early market penetration for start-up businesses
New Product Sales as % of all Sales	This helps give an indication of the flexibility of the market and its relative demand for new products/ services compared with other sector activities.	
Market Growth	Historical and forecast measure of the annual percentage rate of change in sales from one calendar year to the next. Currently, historical growth trends are recorded for a few the metrics above (Sales, Imports,	Growth is the fourth key economic measure. Mostly

	Exports, Employment) but forecast growth is only applied to Sales.	applied to sales, it can be a powerful indicator of the trajectory for different products & services. When used to estimate future sales it shows the changing impact of sector activities over time
Forecast v. Actual Growth	This is a retrospective analysis that compares actual year-on- year growth in Sales with the forecast levels of growth taken from previous years. This is a measure of how accurate and robust forecasts have been in the past and may be in the future.	
Average Critical Mass (m EUR)	This measures the average turnover that a company needs to achieve in its market place to withstand normal fluctuations in demand. Companies that reach the critical mass figure have much higher survival rates than those below.	These metrics appear in the economic data set because they have been used for specific purposes in previous studies-like measurement of market risk or success criteria for first time exporters.
Average ROS	ROS is used as a proxy measure of the average profitability that can be achieved from different markets and of an organisation's ability to re-invest in its own growth	
Average Spend on R&D as % of sales	A measure of the budget expended by businesses on research and development on an annual basis, expressed as a percentage of sales. This is a "push" measure for business innovation that we often compare with "pull" measures like % of new product.	They also typically appear as part of the company Profiling metrics (see below although they are not repeated below).
Transactions	An occasional measure often applied when investigating new service markets. It measures the volume (compared with the Sales Value) of trades/ transactions on an annual basis, Trend in transactions is a good indicator of an emerging market, where value may not yet be established. This metric is often linked with more detailed research into Top 20 suppliers/ purchases in key markets and also with pricing decisions within individual businesses.	This raises a general point, that metrics can be used for different purposes i.e. sector and/ or business analysis.

QA Metrics	No of Sources	Total number of data sources used to generate the values for each product/ service line in the data set. These sources are drawn from a current pool of circa 10,000.	QA metrics are generated for each product and service for each sector and for several of the key metrics. Confidence in Sales is generally higher than for employment or growth, but significant variations may apply especially in relation to mature v. new to market activities.
	No of Cases	Number of instances where we can identify and access case study organisations that provide comparable products/ services or have comparable capabilities, Case studies are drawn from a pool of circa 5m held by the Research Analysts.	
	Confidence Levels	Confidence levels are a mathematical function of the spread of values across the range of sources that we include in our analysis. Confidence levels are applied to all metrics but in particular, sales, employment, transaction levels and growth. Levels vary by activity, geography and by forecast year. Typically, a confidence level of above 80- 85% is achievable, which means that corroborative sources vary around the mean value by +/- 15- 20%.	
	The following set of metrics all apply to companies rather than sectors. They are generally more varied and more specialised. They can be loosely grouped into sub sets and can be combined with some of the economic metrics above. These metrics are drawn from the wider pool of Profiling measures and are best used at the individual product/ service market level i.e. they do not aggregate well, which is why they are rarely as part of our economic research. It should be stressed that these measured have been accumulated over time as part of the standard data set (for different reasons) and are not totally representative of how we would comprehensively review topic areas like markets, technology, innovation, operations etc. Metrics can be applied singly, as part of the "sets" grouped below or in any other combination, depending upon the brief.		
Company/ Industry Profiling Metrics & Benchmarks	Regionality of Markets	A newly developed suite of metrics that apply specifically to a company's ability to understand, adapt to and compete for substantial contracts in a specific country market.	Company and country specific measures that combine qualitative and quantitative analysis of industry sources and other evidence. Assembled due to a specific customer requirement and may be included
	Average project life cycle		
	Localisation of Chain	Collectively, these metrics assess the strength of existing industry supply chain "norms" on a national basis and consider the risk of attempting to enter existing supply chains or setting up new ones.	
	National Preferences		
	Supply Chain Loyalty		

	Complexity of Procurement		in future sector data sets.
	Level of lock-in of supply		
	Market Requirement for Brand Strength	This is measured as high medium or low, and is an indication of the need for brand strength for products in the marketplace based on competitive market data.	Collective measures of product/ service export potential.
	Brand strength required for Export Markets	This is measured as high, medium or low, and is an indicator of the level of need for brand strength in order to export successfully based on best case data.	Assembled originally as part of a UK programme to measures barriers to first time export.
	Product Transfer to Export Markets	This measure is in terms of low, medium and high transferability, to export markets. This gives us an indication of how ready products are for immediate export, e.g. low transferability might be because the product requires significant language translation work as would be the case with software for example.	Can be combined with market, products and economic measures to provide a rounded export market assessment
	Product Ability to Meet International Standards	This is measured as low, medium and high, and refers to industrial standards for products set by the industry on an international basis.	
	Average Product Range/ Spread- No. of products	This is measured in average number of products per business unit. A business unit is a business or part of a business engaged in a specific market area.	Measures included in original data set to assess product development, but have recently been used as a proxy for market innovation when combined with sales, growth and R&D measures (above).
	No. of New Products per annum	This is the number of new products or product sets introduced on average by businesses in each sub-sector on an annual basis.	
	New Product Success Rate %	New product success rate is a measure of the ability of a product to meet sales volume expectations in the market.	
	Average Time to Market for New Products	Time to market, the average time (for different sectors) taken to achieve market entry. This measure is often combined with "Time to Sales", as a reality check on the	

	average time it can take to achieve revenues in different markets	
No. of Products that equal 80% of Sales	This measure is in number of products that equal 80% of sales, which gives us an indication of the complexity of the business in terms of product management and also a measure of business risk (high dependency on small number of products)	
Market Sector Planning Horizon	Market sector planning horizon (in months) is the realistic horizon, based on available data, for business and operational planning. A measure of rate of market change that can be interpreted as either opportunity or risk.	A set of marketing metrics assembled for different purposes over time.
Number of Customers for 80% sales	Measured in number of customers and is an indication of the level of complexity of sales order management. Can also be a measure of risk i.e. dependency on too few customers.	Can be combine with product and economic measures to look at market opportunity and risk.
Average no of contracts for 80% of T/O	This measure is for organisations whose business is driven by securing contracts in the market place rather than selling products only. Therefore, this gives an indication of the critical reliance of the company on its contract portfolio.	
Average Annual Rate of New Contracts	This measure is for organisations whose business is driven by securing contracts in the market place rather than selling products only. This is a measure of the rate of new contract acquisition by a company (compared with the industry norm).	Benchmarks for these measures focus on industry/ market norms, how they differ for products/ services into different markets and provide a comparison point for company performance.
Average Contract Life	This measure is for organisations whose business is driven by securing contracts in the market place rather than selling products only. This measure is in months and is the average longevity of contracts within the industry, therefore giving an indication of the required rate of new contract acquisition by any company.	
Market Risk of Substitution	Measured as high, medium or low, this is the measure of the likelihood of alternative products or services emerging in the market place during the life cycle of the product or service delivered to market. This composite metric includes: Number of competitors	Can also be used to provide a risk profile for new market entry or for continued market presence.

	• Capital requirement to enter the market (where low the higher the risk) • Number of alternatives available • Number of technologies available • Number of service models (where product is a service) • Product life cycle • Time to market for new products	
Marketing Costs as % of Sales	These are the average industry costs for marketing activities measured as a percentage of sales per annum, based on best case data.	
Average Time to Maximum Sales	Measured in months, this is the average timeframe for new products to market to achieve plateau sales i.e. the average maximum sales per months for the life cycle of the product.	
No. of Competitors	Measure of significant competitors who are established in the marketplace and are achieving measurable sales figures.	
Technology Compression Rate %	In the production of all products and services the improvement of processes for either manufacture or delivery usually involves doing more value- added functions at a single point to reduce costs. As a result, quite often supply chains become shorter. This is known as technology compression. By understanding the rate of technology compression, we can better understand how the product will be delivered to market in the future and what the most likely cost and risk profile will be.	Three technology measures drawn from a wider suite (used specifically for technology assessment).
Technology Life Cycle	This is a composite measure of how technology change affects the product life cycle within each market. This measure includes an assessment of Technology compression (above) i.e. the rate at which product or service processes become obsolete.	In combination, these measures can be used to provide commentary on technology opportunity/ risk at the industry level- informing public investment decisions between industries.
Substitution Threat from New Technology	This measure looks at a specific technology and its ability to repel other technologies in other markets for its current applications. In addition, it looks at the likelihood of new technologies displacing the current technology, for example where margins are high and available market is in growth, R& D spend may indicate that high likelihood of new technology emergence and	At the company level, they

	therefore higher risk of replacement. The composite metric includes: • Number of alternative technologies either in or developing towards the market • Cost of technology relative to sales value and ROS • Time to market for new technologies • Product life cycle • Time to market for new product (that incorporates new technology)	identify and broadly measure risk within an industry
Delivery to promise %	This is a measure of the ability of the industry to deliver product to sales order promise, on a region by region basis.	A cross section of operational benchmarks drawn from a wide range of sources. Routinely produced as part of sector data sets to demonstrate the depth of our performance (as opposed to economic) data.
Percent sales returns %	Measured in per cent of total and is an indication of the number of products in percent terms returned faulty, by market and on an annual basis.	
Achievement of Regulatory Standards %	A measure of a products ability to achieve regulatory standards on a region by region basis. This measure is different to that of the ability of the product to meet international standards which really concentrates on the capability of the product, rather than legal requirements.	
Rate of Right First Time to Market (RFT) %	A measure of the rate of right first time to market, i.e. the ability of the sector to introduce new product without significant remedial expenditure.	
Average Pay Back	Measured in months, based on best case data, this is the measure of the time taken to achieve payback on investment for new products to market.	Typical use of these benchmarks is to show different performance requirements across industries and products/ services. This can be used with companies to identify current performance gaps or to assess future performance challenges for
Average Annual staff costs as % of Sales	Based on best case data for business with similar or identical product and service portfolios this is a measure of the total staff costs both direct and indirect per annum as a percentage of total sales.	
Cost of Engineering %	Measured in percentage of sales turnover, this is the total cost of engineering in manufacturing companies in order to deliver product to market on an annual basis.	
Cost of Quality %	Measured in percentage of sales turnover, this is the total cost of quality control, management and	

		assurance for both service and manufacturing companies to provide products and services to market.	new products/ markets.
Other Operating costs as a % of sales		Measured in per cent of sales turnover, this is the total cost of all other operational activities of the company excluding staff costs and primary operational costs.	
Production Scrap Rate %		Measured in per cent of sales turnover, this is the measure of scrap materials and componentry produced during the normal manufacturing process of product for supply to market.	
Plant Utilisation %		Measured in per cent of total machine time available. This is the measure of the amount of time that manufacturing or process plant is actually adding value to product rather than either idle, or in maintenance. This gives an indication of total plant efficiency and availability.	
No of Stock Turns per Annum		This is a measure of how many times per annum finished stock is replaced in the warehouse. This data amongst other data sets give an indication of the efficiency of manufacturing and production control and management and its relationship to sales and sales forecasting.	
Sector company Birth Rate % Total		Number of new start- up companies per annum based upon new company registrations and number of new balance sheets that we can see for this specific market, expressed as a percentage of the total number of companies.	A miscellaneous set of measures that have been used previously as part of a Porter five- forces analysis or as a general measure of competitiveness.
Sector company Death Rate % Total		Number of business failures per annum that we can see for this specific market, expressed as a percentage of the total number of companies	
Customer Power		Measured a high, medium or low this is a measure of the level of influence that the customer has on the chain of supply and the market place in which it operates. The composite metric includes: • Number of procurers (few procurers means higher customer power) • Regulatory controls (may give the customer increased power) • Level of influence the customer has on the end user market	Can be combined with market. product or economic measures to provide a general analysis of competitive barriers or performance.

Financial Entry Barriers	Measured as high, medium or low, this is a measure of identified barriers to entry in financial terms to the market for new businesses. This composite metric includes: • Cost of set up • Critical mass needed to reduce risk • Financial regulatory implications and the cost to comply • Scale of capital investment required to put delivery capability in place in relation to ROC • ROC • ROS • Local fluctuation of exchange rates
Operational Barriers to Entry	Entry and exit barriers is a compound measure (high, medium, low) of the level of competitiveness in a marketplace based upon the risks/ costs of effecting or maintaining a market presence. This composite metric includes: • Language barriers • Logistics capability and availability • Local restrictive regulations e.g. imports versus local supply • Limitations on raw materials availability • Limitations on skills availability • Restrictions due to contracted supply chains to competition

Some metrics are more important than others and more widely used and need to be described in additional detail. These metrics are shown in Table 52 : Description of Key Metrics.

Table 52 : Description of Key Metrics

Metric	Description
Sales	Sales is the estimate in (m EUR) of economic activity by identified companies in a defined region or country. The estimate of sales is based upon where economic activity takes place i.e. the location of the business rather than the location of the income earner. In calculating the sales value, the following factors are considered: • Turnover by sub-sector within postcode sets • Capital asset adjustment by sub-sector within postcode sets • GDP calculations • Supply chain procurement value sub-sector by sub-sector by postcode sets

	Sub-sector specific sales reporting where available Further adjustment is made on a sub-sector basis for both head office activities and virtual working organisations so that, <i>as far as is practical, sales is calculated based upon where it is conducted rather than where it is reported</i>. This applies to domestic and export sales. Sales figures are divided into Domestic Sales and Export Sales and combined into a Total Sales figure for reporting purposes
<i>Companies</i>	Companies is a measure of the total number of companies in the geographic region that match (or fit within) the activity headings for the sector. Because of the limitations in using traditional SIC codes to identify high technology and “new economy” businesses, companies are allocated to sector activity headings using the research methods identified above. The total number of companies is arrived at by a bottom-up analysis of company stock using a wide range of company sources. Having identified the total company stock in any given region, product and service outputs are identified and verified by accessing further databases that include: Institutional data sets, advertising and market data sets and reports and by web search.
<i>Employment</i>	Employment is a measure of the estimated employment numbers across all aspects of the supply chain. National, regional, city and other economic data sources have been used to estimate current employment levels for each sector activity. Where employment information is scarce, or where employment is estimated as a proportion of a company’s sales, a comprehensive range of case study materials are assessed to provide sensible industry- specific ratios and benchmarks. Following national statistics, employment figures are disaggregated into four streams- Management, Supervisory, Administrative and Other. Where further Skills analysis is commissioned, these four streams are disaggregated into much more detailed occupational groupings. The employment figures for each sector define the labour intensity of some market activities over others and help to identify the economic activities that are generating the highest levels of employment (but not necessarily value or growth).
<i>Market Growth Forecasts</i>	Market Growth Forecasts are a forward- looking indicator and have been measured for the short to medium term (five years) where there is a high level of confidence in the growth trend. This indicator enables the identification of the ongoing strength and potential of each economic activity relative to other sector activities and relative to growth rates across city and country markets. Growth forecasts are calculated in the same way as all other metrics using multiple sources, but with one exception. Sources for growth forecasts are “weighted” (the only metric that is) based upon previous “hit rates” i.e. levels of accuracy. Hit rates are measured in percentage terms and this percentage is applied to each forecast value as part of the final calculation. The “hit rate” is used for all metrics in determining that sources should be included in the analysis, but it is only use in one calculation i.e. the growth forecast.

Companies

1.1.124 Finding Cybersecurity Companies

Cybersecurity companies are difficult to find because they are generally coded in most official databases under different industrial headings. Company searches are based upon multiple sources of

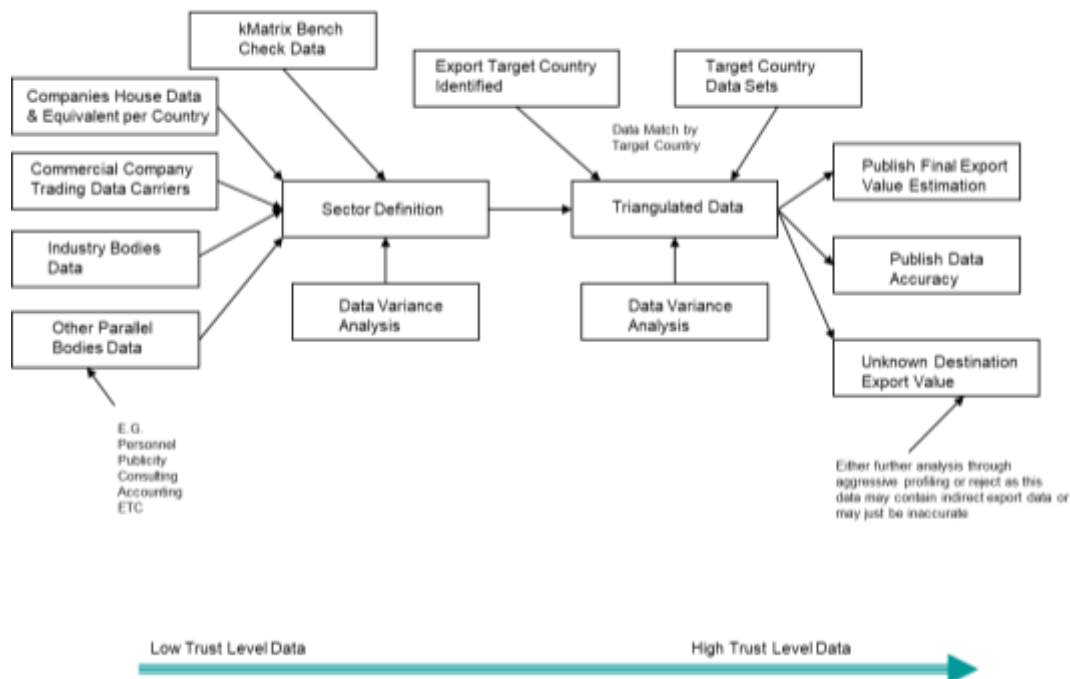
company data- official sources, industry sources, marketing directories, membership organisations etc. A small number of large companies are well documented (in the UK) by sources like FAME, Dun & Bradstreet, Companies House, Hoover, ICC, Thomson etc. (and their international equivalents) but most companies are smaller and harder to find. This requires detailed keyword searches of company data bases and web search engines. Currently, CIMA uses several highly trained “web-bots” to keep track of/ track down companies in Security and Cybersecurity. In the case of Cybersecurity, the process is more complex, as many suppliers are not actually Cybersecurity companies, but deliver services as part of a wider portfolio. So, data searches are not restricted to company data bases but require cross referencing, corroboration and triangulation between multiple sources of company, industry, procurement and other data to develop a realistic picture of trading on a global basis and within the EU. This process is closely aligned with private sector market and competitive intelligence techniques and reflects best practice in how companies themselves measure their own uncertain competitive landscape.

For the reasons given above, it is not always apparent from company websites or from national statistical sources that organisations are involved in the sale or Cybersecurity products and services. Therefore, more complex search processes are required, using an appropriately wide range of key words. A sequential process for identifying companies is identified in the 19 steps listed below:

1. Scan for Cybersecurity definition and associated definitions (as language and terminology differs) in both resident and new data sources
2. Decipher country- based industrial codes where relevant
3. Connect with central company registry per country
4. Connect with commercial company data holders where necessary
5. Identify products/ services that might include Cybersecurity for data search purposes
6. Associate each element with in-field data to look for trading activity
7. Look for project reports and commentary through established news routings as these usually identify who is involved so that we can then focus on organisations for more detail.
8. Scan for activity in commercial sectors
9. Scan for activity in sector and cross sector associations
10. Scan for activity in sector and cross sector Institutes
11. Scan for activity in the financial sector
12. Perform source evaluation as per our standard data reliability process
13. Apply data reliability process (data variance analysis)
14. Finalise source set post data reliability process.
15. Assembly Company names and financial activity
16. Establish operational base for each company identified
17. Data triangulation may be needed to define the Cybersecurity- relevant element of trading
18. Conduct manual data review to check for possible errors
19. Report process output.

This 19- step process is described as sequential, but in reality, it is iterative and is conducted within a sub- set of research routines contained within the wider research model, shown at Figure 71. This wider research model positions the specific data sources used within a wider universe of research routines and algorithms that cross check data against the Cybersecurity market definition, company case study and benchmarking data (reality checking of Cybersecurity data in relation to other market activities), other company and country data sets (to compare geographical trading patterns) in relation to what is known about Cybersecurity and, where appropriate, related or similar sectors.

Figure 71 : Company Search Model



It should be stressed that the quantitative research methodology as a whole is not BASED on company figures (because these are defined using SIC or their equivalent codes), but the research includes company data from traditional sources as a data "check." It is only when companies have been "coded" against Cybersecurity headings that they become useful as a meaningful source of data.

1.1.125 Classifying Companies

The company listings for Cybersecurity may then be used for several different purposes. Within the CIMA research these include:

- Reporting the company count and size ranges as key metrics in the market analysis
- Contributing to the calculation of activity values (domestic sales and exports) in the final research
- Specific listings- Top Cybersecurity companies, Top EU exporting companies, international exporters
- Tracing the sector of origin for some suppliers of Cybersecurity products and services
- Identifying end- users and end- user industries for Cybersecurity products and services

Typically, company listings are data coded for product and service outputs, industries that they serve, main industrial coding (i.e. not all Cybersecurity services are delivered by Cybersecurity companies) and geographic location(s). More complex codings are sometimes applied to more mature markets where core product and service offerings may contribute to multiple applications or customer

solutions. For emerging markets like Cybersecurity coding is more difficult as services are less well defined, under- reported and rapidly changing. This is reflected in earlier work conducted for UK Trade and Industry where the research identified significant changes in services, categories and in the branding of companies who may have started in ICT but had re-branded as Cybersecurity companies. These changes spanned the period 201- 2016 and are still not complete. Over time, however, data volume and quality have increased, providing more certainty and, therefore, enabling more complex market analysis and interpretation.

There is one further characteristic of emerging markets that applies to Cybersecurity and that is that early markets are often serviced by established companies exploring new opportunities. This means that services are provided as part of a wider portfolio, often on an ad hoc basis. This has been true for markets as varied as renewable energy and low carbon. As critical mass in the marketplace builds, services are provided by new entrants, spin- out companies and new business units of existing companies. The supply- side is, therefore, fragmented and difficult to define because many market players are only partially committed to the market and their contribution can be difficult to measure. This shows the importance of being able to search for service delivery into emerging markets by ranging across a broad base of companies operating in all industrial and service sectors

This makes the whole process of identifying, selecting and coding companies in emerging markets a complex and evolving process that requires multiple approaches or data sources and a degree of informed interpretation. In this respect Cybersecurity is not unique and can benefit from research methods used in other markets/ sectors, specifically those methods that attempt to differentiate, extract and quantify service values from a company's core offerings.

1.1.126 Accounting for Company Revenues

Companies can operate in many different territories and in many different sectors and may report their turnovers in different ways. It is therefore, challenging to identify and attribute Cybersecurity turnover to individual companies in specific cities or countries. This can only be done on a "best-efforts" basis by:

- Studying company results on a products and services basis to isolate a proportion of its turnover for Cybersecurity
- Researching where the product and service activities are conducted
- Referencing procurement data to account for where services might be purchased
- Referencing other sources of data as a "back- check" on product and service flows within and without the defined geography

Only then can an attribution of Cybersecurity turnover be made for an individual company (also see Sales and Company metrics description above). National reporting systems can indicate total company sales (although even this need interpreting) but it cannot provide an estimated value for Cybersecurity without these additional steps to filter the results. In many cases, even the companies themselves may be an unreliable source of data because emerging sales streams may not be monitored or accounted for. This process for attributing company sales has been tested/ audited in several emerging markets (blind testing with companies selected by clients) and the conclusion has been that initial client data can be unreliable and that external analysis of sales volumes in non- core markets is often the only means of quantifying these sales. This, of course, changes as an emerging market becomes more mainstream to a company's interests.

1.1.127 End- User Types and Markets

Both sales and company analysis processes are used to identify end- users for Cybersecurity products and services. Within the Cybersecurity taxonomy itself many markets are divided into Large Corporate, Small Business, Cloud, Public Sector, Smart Comms and General Applications, but this does not describe whether it applies to public or private sector clients. This is achieved through an additional research process that focuses on end- users. This was first introduced in 2012, where three broad types were identified:

- "Government" - including any department, organisation or agency that is security- specific and funded by government, For the UK that would including Home Office, UKTI, Police and public security organisations.
- "Other Public" - including any public funded not listed above i.e. local government and those responsible for security of public places (amongst other responsibilities).
- "Private Sector" - including a wide range of industries like Utilities, Manufacturing, Energy etc.

This research was based upon only those sources that already had a track record for the Security sector as a whole. Since then more detailed sources of Cybersecurity data have been identified and tested and a more accurate (but not complete) segmentation of end- user types is now possible for 2016.

This segmentation is based upon the US definition of Critical Infrastructure²¹ that includes 16 infrastructure types. 14 of these "Types" have been included in the CIMA research, two were excluded due to insufficient data sources (Dams and the Nuclear Industry) and two types have been added (Construction and Education). The 16 types used for analysis of end- users are:

• Chemical & Pharma Processing	• Other Utilities (Includes Energy)
• Commercial Facilities	• Government Facilities
• Communications	• Healthcare & Public Health
• Manufacture & Assembly	• Information Technology
• Emergency Services	• Education Sector
• Defence Industrial Base	• Transport & Logistics
• Financial Services	• Water & Wastewater Utilities
• Construction	
• Food & Agriculture	• Non- Traceable

Non- Traceable, "Other" activities account for 25%, which *relate to retail activities (10%), attributable activities (10%) and activities relating to sectors other than the 16 listed (5%)*. It is possible to apportion the non- traceable values to the other 16 "types" but by retaining and tracking this figure it should be possible to monitor improvements in data quality over time

A brief description of vertical or end- user markets for Cybersecurity products and services is included at Table 53.

²¹ US National Institute of Standards and Technology (NIST)

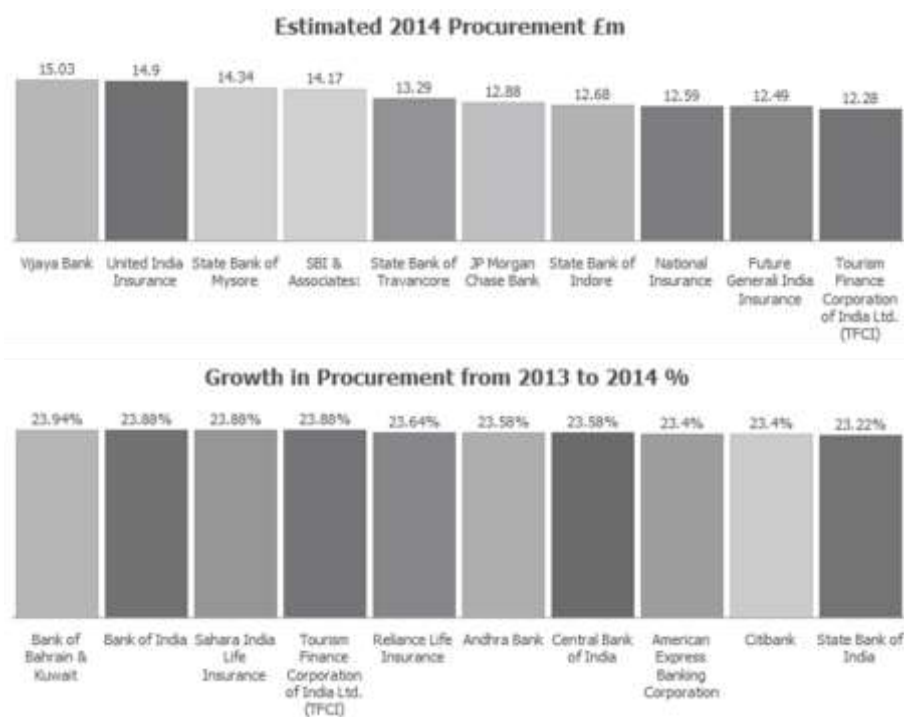
Table 53 : Definition of End- User Markets for Cybersecurity

Chemicals & Pharma Processing Commercial Facilities	Includes all aspects of chemicals and pharmaceuticals processing including both batch and continuous production. Examples are drugs, paint, solvents, cleaning products, cosmetics etc.
Communications	Includes telephone exchanges, mobile and static phone engineering, land line maintenance and installation, transmitter maintenance and installation, WIFI and blue tooth systems and development, networking systems and consultancy.
Manufacturing & Assembly	Includes all aspects of manufacture, both batch and continuous by both hand assembly and automated systems. Examples are automotive, white goods, brown goods, toys, computers, medical instruments etc.
Emergency Services	Includes, fire, ambulance, police and all civil emergency services such as flood abatement and earth quake rapid response.
Defence Industries	Includes security aspects only of the defence sector that are not covered by the defence sector definition
Construction	Includes home building, commercial buildings, civil engineering, design and architectural design, planning, project management, highways etc.
Financial Services	Includes banking, insurance, fund management, futures, private equity, trading, analysis and reporting, trading floor operations, etc.
Food and Agriculture	Includes food processing both batch and inline process, packaging and refrigeration, the crop growing supply chain, through to retail sales. The sector includes both time sensitive and non-time- sensitive products and the operational chains of supply.
Other Utilities	Includes electricity, gas and all forms of generation including coal gas, natural gas, fracking, bio-gas and other bio fuels, wind and tidal energy, photovoltaic energy, solar energy, nuclear energy,
Government Facilities	Includes government buildings and facilities in the public sector. Facilities include storage facilities, laboratory facilities, training establishments etc.
Healthcare and Public Health	Includes hospitals and mobile healthcare capabilities, not included in the emergency services. This sector also includes Doctors surgeries and other healthcare establishments in the network of supply. In addition, the sector includes pharmacies, alternative health establishments, home care networks and other specialist health units in both the public and private sectors.
Information Technology	Includes software development, design and development of networking equipment (not covered in manufacturing). Outsourced computing services and centres, cloud provision, mobile computing and data management, consultancy and systems implementation.
Education Sector	Includes schools and universities as well as specialist training centres, outward bound centres, distance- learning establishments, early learning establishments, the generation and production of learning materials, educational publishing, and consultancy.
Transportation & Logistics	This sector includes transport vehicles and networks, logistics operations and planning, warehousing and distribution centres, ERP (enterprise requirements planning) and DRP (distribution requirements planning) systems and implementation, passenger transport and goods transport by road, rail, sea and air for both the public and private sectors.

Water and Wastewater Utilities	This sector includes utilities of potable water supply, sewage treatment, potable, grey and black water distribution and management, water treatment facilities, and infield engineering.
Other	"Other" category includes all consumer related sales for the vertical markets listed above and for other vertical markets (not listed) that are not considered critical, most retail activity and a proportion of transactions that are either too small to identify or that (for commercial or other reasons) are not traceable to any of the vertical markets.

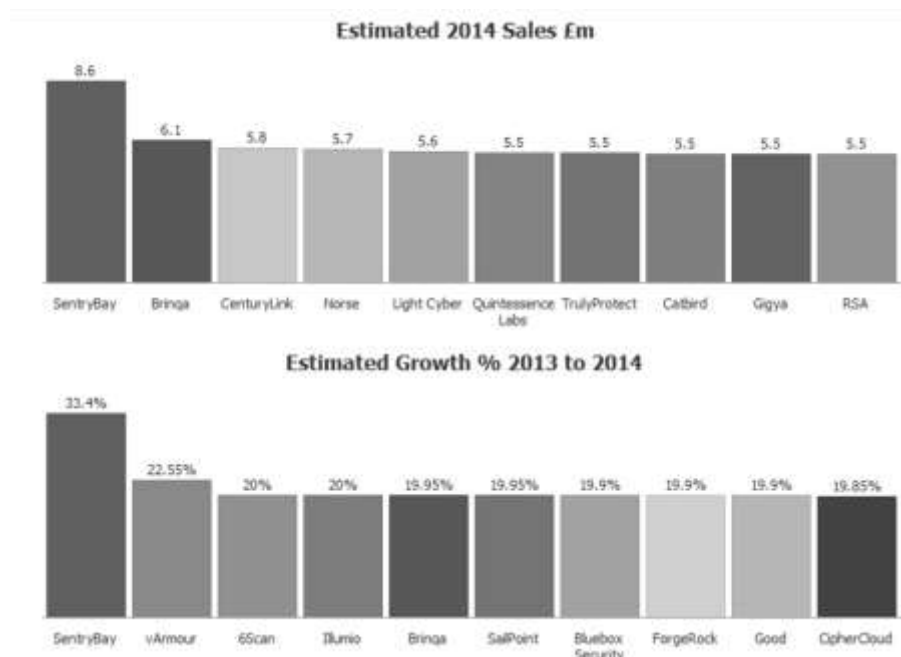
The investigation of end- users is based upon aggregated transactional data on sales and procurement. It is possible to disaggregate this data to identify suppliers and purchasers (by end- user type) of Cybersecurity products and services by country and by sub-sector. In previous research, this resulted in lists of ranked purchasers (Figure 72) and ranked suppliers (Figure 73). A further application of this approach- specifically to exports- is shown in Section 0.

Figure 72 : Example of Ranked Purchasers



:

Figure 73 : Example of Ranked Suppliers



1.1.128 Supplier Typology

Cybersecurity is also something of a hybrid sector, in that its roots extend into companies in sectors like ICT, Defence and Security. The prevailing perception is that Cybersecurity activities have primarily emerged from the ICT sector. Research, using the sector and company research processes identified above, was conducted into the company base for delivering Cybersecurity products and services, identifying the core sector for that company and the proportion of its business that relates to Cybersecurity.

An example of this is shown at Table 54, using six corporates as examples to illustrate their core business activity and then, what proportion of their activities relate to other activities- including Cybersecurity. These proportions are then converted into sales values, aggregated and then used to calculate the proportion of Cybersecurity sales generated by companies falling within the seven sectors of Cyber, ICT, Defence, Security, Academia, Insurance and "Other". For example, BAE Systems is an Aerospace/ Marine company, aligned closely with the Defence sector that also happens to provide Cybersecurity activities that are NOT related to Cyber Defence.

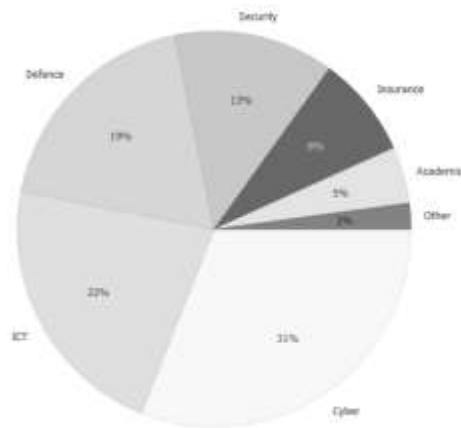
Table 54 : Example for Constructing the Typology of Cybersecurity Providers

Company	Main Stream Business	Approximation of total business activity % outside main stream business				
		ICT	Defence	Security	Cyber	Other
BAE Systems	Aerospace, Marine	2.3	4.6	7.2	6.3	1.3
Airbus	Commercial Aerospace	1.4	3.3	2.6	2.4	2.4
BT Group plc	Telecoms		1.1	1.4	3.5	0.92
QinetiQ	Defence	4.6		8.4	11.3	1.6
Thales Group	Marine, Aerospace	1.2	3.4	14.3	4.5	2.5
Rockwell Collins	Rail, Air, Infrastructure	3	2.2	11.3	3.5	1.8

The results of this research are incomplete, imperfect (the method is still be refined) but informative. It summarizes the sectors involved in delivering Cybersecurity products and services for the EU. It

shows that 31% of the sales value originates from companies that are solely involved in the Cybersecurity sector, 22% originates from companies whose core business is ICT, 19% originates from companies whose core business is Defence/ Aerospace and 13% from companies whose core business is Security. Cyber Insurance is only delivered by Insurance companies and Academia (through spin-out, research partnership or consultancy) accounts for 5%. “Other” includes the 2% that cannot be allocated elsewhere.

Figure 74 : EU Delivery of Cybersecurity by Sector



While these results rely on some subjective assessments of company core activities and estimates of the proportion of revenues relating to Cybersecurity, they do reveal that the roots of Cybersecurity reach beyond the ICT sector.

International Trade Data and Analysis

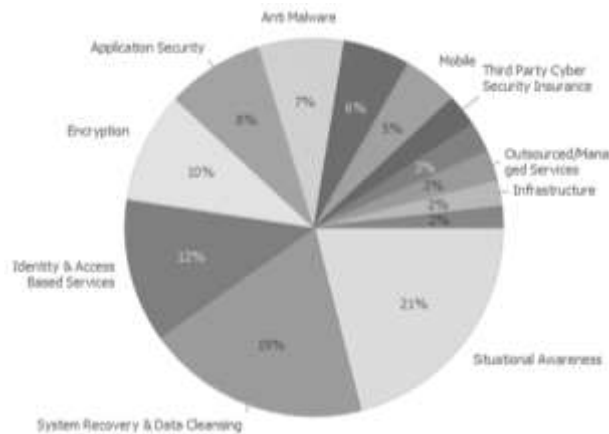
1.1.129 History of Development

International Trade provided a very strong impetus to the development of the CIMA sector research methodology. The ability to measure activity across international boundaries (both inbound and outbound) is critical to estimating national competitive performance. The demand from UK Trade and Export teams was for a methodology that could a) measure UK strengths, b) translate these strengths into a comparative analysis with other nations, c) benchmark national performance on a global basis and d) monitor trends in performance over time. The multi- source approach (as described in Section 0) allows for the creation of a common sector definition across multiple countries and, therefore, lends itself to international trade measurement and monitoring. This functionality is central to a multi- sourced approach whose roots reach back into industrial market research and competitive/ competitor analysis methods.

Initially, the multi- sourced approach was used for “difficult-to-measure” sector definition first and international trade measurement second, thereby filling the gap left by standard industrial classification i.e. for sectors like Space Technology and Agri-technology. But over time, the ability to compare international performance and target export resources has meant that this methodology has been applied to sectors that are less difficult to measure (i.e. are partially or fully covered by industry codes) but where comparative analysis of performance is difficult.

The development story can best be told using a series of graphics that represents key points in the ever- increasing measurement of international trade. This history runs from the more traditional measures of exports to more sophisticated global ranking and market share analysis. Ultimately, due to the transactional nature of many of the sources used in calculating data point values it has also been possible to identify specific customer types and even individual customers.

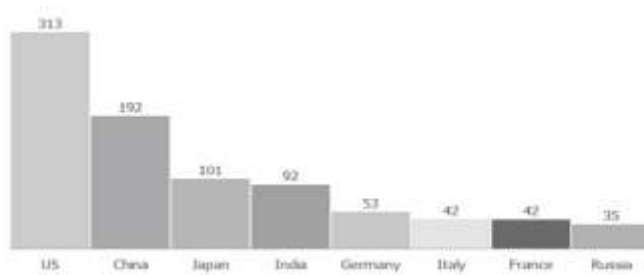
Figure 75 : Measuring Exports by sector and sub-sector



Initially, research focused on being able to replicate the measures provided by national statistics for most industries i.e. the volume of exports by sector and by sub-sector (Figure 74).

Typically, this would involve calculating export by destination country (Figure 75).

Figure 76 : Measuring Exports by Destination Country



The major break-through occurred in 2010/ 11 when the methodology progressed from measuring single country trade flows to multiple country trade flows. This switch from a one-to-many model to a many-to-many model opened opportunities to measure market share (Figure 76)

Figure 77 : The Transition from Trade to Inter- Trading

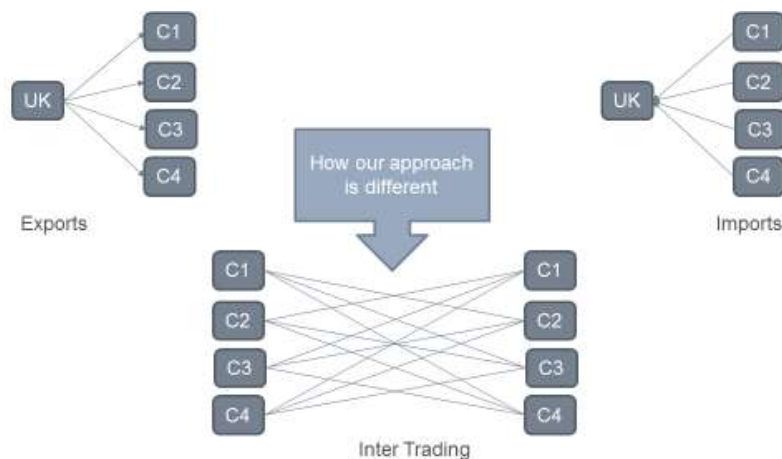


Figure 78 : Inter- Trading and National Trade Flows

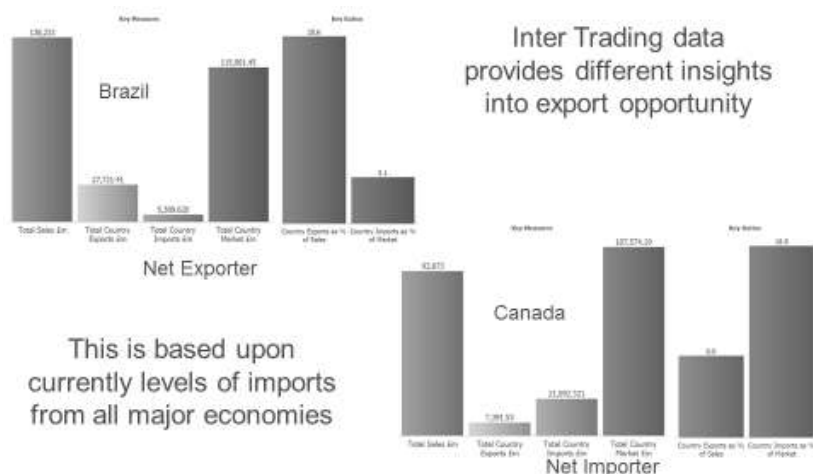


Figure 79 : Measuring Market Share

By comparing trade flows for multiple countries, it became possible to identify those economies that were heavily dependent on imports (targets) and those that were net-exporters (competitors).

This enabled a different approach to designing and implementing export strategy (Figure 77).

It also became possible to measure existing export performance in terms of share of a country's imports.

Share of global exports could now be calibrated to share of country market, identifying where current trade flows were strong (Figure 78).

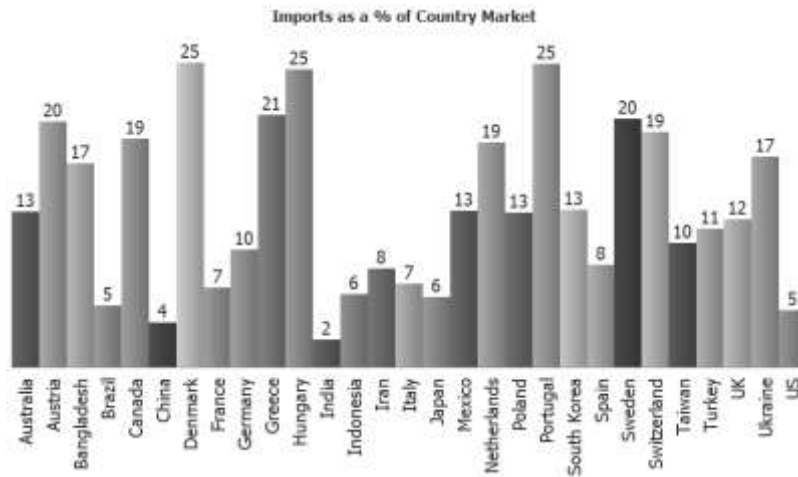


Figure 80 : Measuring Market Share of Country Market

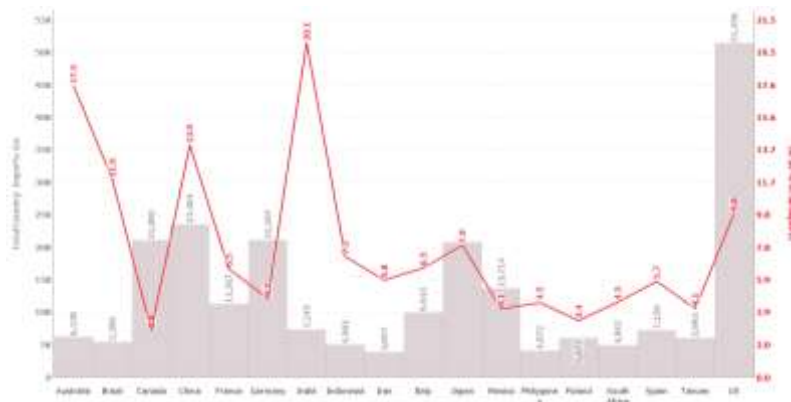


Figure 81 : Comparing Market Share as a measure of Competitive Performance

This meant that efforts could be focused on where trade and market growth were strongest, which may not be where the volume of exports was highest. For the first time, qualitative decisions about export strategy were made using quantitative data (Figure 79).

The transition to Inter- Trading also made it possible to track national competitors (over time) in key country markets (Figure 79).

This acted as a barometer of UK performance and provided the basis for evaluating the success of export initiatives over time.

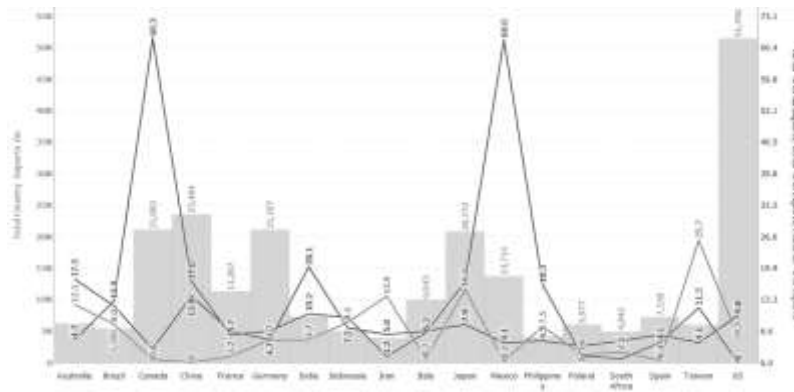
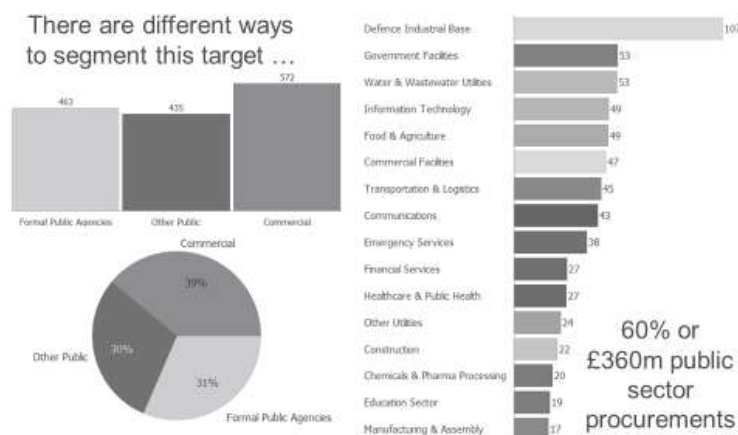
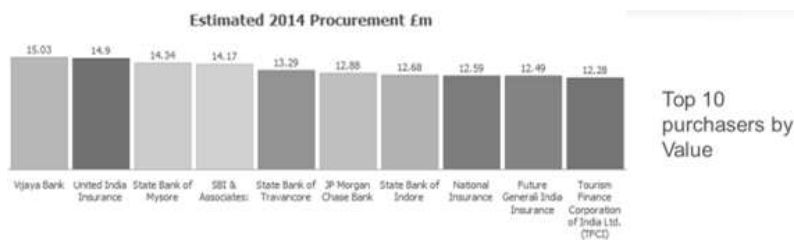


Figure 82 : Identifying End User Groups for Targeting Exports



The latest (but not final) stage of development involved using all available intelligence about national markets and performance to leverage resources to affect specific end-user groups, either in the public or private sector. This required coding of the sector data per known purchasing history (Figure 81).

Figure 83 : Identifying In-Country Customer for Targeting Exports



And once an- end user group is identified then the next step is to identify, attempt to influence or meet with In- Country purchasers in a country that already has established and strong trade links (Figure 82).

What Figures 74 - 82 illustrate is one of the core advantages of the multi- sourced approach i.e. its ability to go beyond the data that official statistics provide on a national level, to create a truly global picture of the flow of goods and services that can be used to benchmark and then improve upon national competitive performance.

1.1.130 Assumptions

One inherent assumption in many analyses of international trade is that exports are good and imports are the opposite- the “balance of trade” measure that is frequently used to judge economic performance. In a world of global trade and global supply chains this is clearly not a true measure of performance. Imports may be finished goods that compete with domestically produced goods, but they may also be the componentry that enable completed goods to be exported and enable entire industries to be effective. To downgrade or underestimate imports or to ignore the international movement of unfinished goods and services is to ignore many of the ways in which industries within major economies operate.

The CIMA process focuses on the most complete available picture of trade flows and, therefore, includes unfinished goods and services. To clarify, this means that:

- an import may be an unfinished good that later becomes incorporated into a further or final product that is subsequently sold domestically or is exported
- an import may be a finished good that is “rebadged” or branded and subsequently sold domestically or is exported
- an import may be a finished “branded” good that is purchased domestically.
- an export may be an unfinished good that later becomes incorporated into a further or final product overseas that is subsequently sold domestically or is re- exported
- an export may be a finished good that is “rebadged” or branded and subsequently sold domestically or is re- exported
- an export may be a finished “branded” good that is purchased overseas.

This means that the estimation of imports/ exports using the CIMA approach is likely to a) produce different, and often higher, numbers when compared to national statistics and b) the relationship between imports and exports becomes more inter- relational.

A second assumption within the CIMA research model relates to the geographic origin of an export. For example, great care is taken to locate sector activities according to where they are conducted rather than where they are reported. This means that a multi-site company located in the UK may report its performance nationally, but the research process attempts to assign activities to the region, city or sub region where they are performed i.e. the manufacturing plant in the North West, the distribution centre in the East Midlands and the sales team in London. For an international company, this becomes more complex, especially for how exports are reported. In the approach taken for the C40 (and more generally) and using the UK as an example:

- an international sale from a company in the UK to a customer in another country is registered as a UK export i.e. it has crossed international boundaries
- a sale by a UK company that is delivered by a business unit in India to an Indian customer is recorded as a domestic sale

- a sale by a UK company that is delivered by a business unit in India to a customer in another country is recorded as an Indian export, despite the ultimate ownership or “nationality” of the company.

A final assumption in the compilation of export data is that it is relatively easy to see the initial (and mostly final) destination, but it is not always so easy to track the onward transmission of (primarily) goods. An example is exports into Hong Kong, where it is clear the volume of UK exports exceeds the country’s demand, but it is not always clear where the final South East Asian destination might be. In this case, no effort is made to re-allocate exports to “probable” locations.

1.1.131 Research Model

Imports and exports are inherently more complex to measure than domestic sales and, typically, company data is more protected. This is especially true of new or emerging sectors where national statistics do not exist and where company surveys may be the only possible alternative. Compiling export data for Environmental and Low Carbon has stumbled in the UK (for example) when companies have been unwilling to share export data.

Figure 84 : Challenges presented by Exports



Comment:

It is rare for companies to share detailed information about their import/ export performance.

Public information is usually presented or modified to protect a commercial position. There is, therefore, no single source of information that can be trusted to reveal detailed import/ export data.

The alternative approach is to use multiple sources to estimate exports and not to be over-reliant on company data. Exports and imports leave multiple data trails, whether via industry reporting, insurance, logistics, legal, procurement or other customer sources. Imports and Exports are also calculated using both in- country and out- of- country data to ensure:

- At least one end of the transaction is recorded
- A possible cross- check on both ends of the transaction
- Descriptions about the goods and services sold and purchased are normalized across international borders and can be accurately recorded.

The transition from measuring single trade flow (one-to-many) to measuring multiple trade flows or inter- trading (many-to-many trading as outlined above), while massively increasing the complexity of mapping imports and exports, has increased the number of triangulation points and has contributed significantly to the process of compiling more robust data.

The increased complexity of mapping imports/ exports means that the standard research process is modified and encompasses two steps, leading to an estimated value. The first step estimates what is expected (using industry level data) and the second step calculates what it is possible to confirm (using company and country level data). The difference between the two provides the "confidence level" i.e. the level of imports or exports that can be traced as a percentage of what the figure might be if full visibility of data was possible and if all data sources agreed.

Initially, company turnover is checked via direct sources and indirect sources. This serves as a back check for import or export claims made by the companies. Available benchmark data also acts as an indicator of what level of imports or exports to expect from companies of a certain turnover in certain markets. Any deviation from this can trigger additional research.

Import and export data is available from a number of sources, some directly announced by the companies and some via external sources that include institutional, industry bodies, government, academic as well as other sources not necessarily associated with company imports and exports such as logistics, packaging, personnel, publicity, shipping, consulting, legal and accounting, which all provide services to the sector and collect data directly from companies and from various parts of the sector's supply chain. This information provides the "notional" value for imports or exports. This provides a target figure against which to test our ability to trace actual export performance by country.

The notional value is based upon all easily available data for companies and the industry sector. The degree of variance between sources of data gives an indication of how accurate this initial estimation may be. For example, if the variance is only 20% then the estimation should be better than 80%. However, variances are often wider than this and require further analysis. The location of data for this second step of the analysis is usually identified by the process of estimating the notional value itself. At this point a new series of data processes and sources are used to improve the estimate and increase the confidence level, using data triangulation. The data triangulation process identifies in more detail which countries the imports or exports were attributed to and, therefore, what additional country data sources need to be attached to and analysed. The new sources are then compared for their variance and then compared with the original sources for the notional estimate. At this stage, the variance should have decreased and confidence levels increased.

This two- step process gives an overall view of the sectors import or export value. There is, however, usually a small proportion of the most likely export value that cannot be apportioned to any country. In some cases, this proportion of the notional export figure is often either misclassified or is an indirect export which just cannot be seen. If it is impossible to clarify this activity, it is excluded from the final estimate. What remains at the end of the two- step process (although, in reality, it is an iterative process within and between steps) is an estimated value for imports and exports, evidenced from named sources, that can be attributed to specific countries, with a confidence level based upon the variances in the source data.

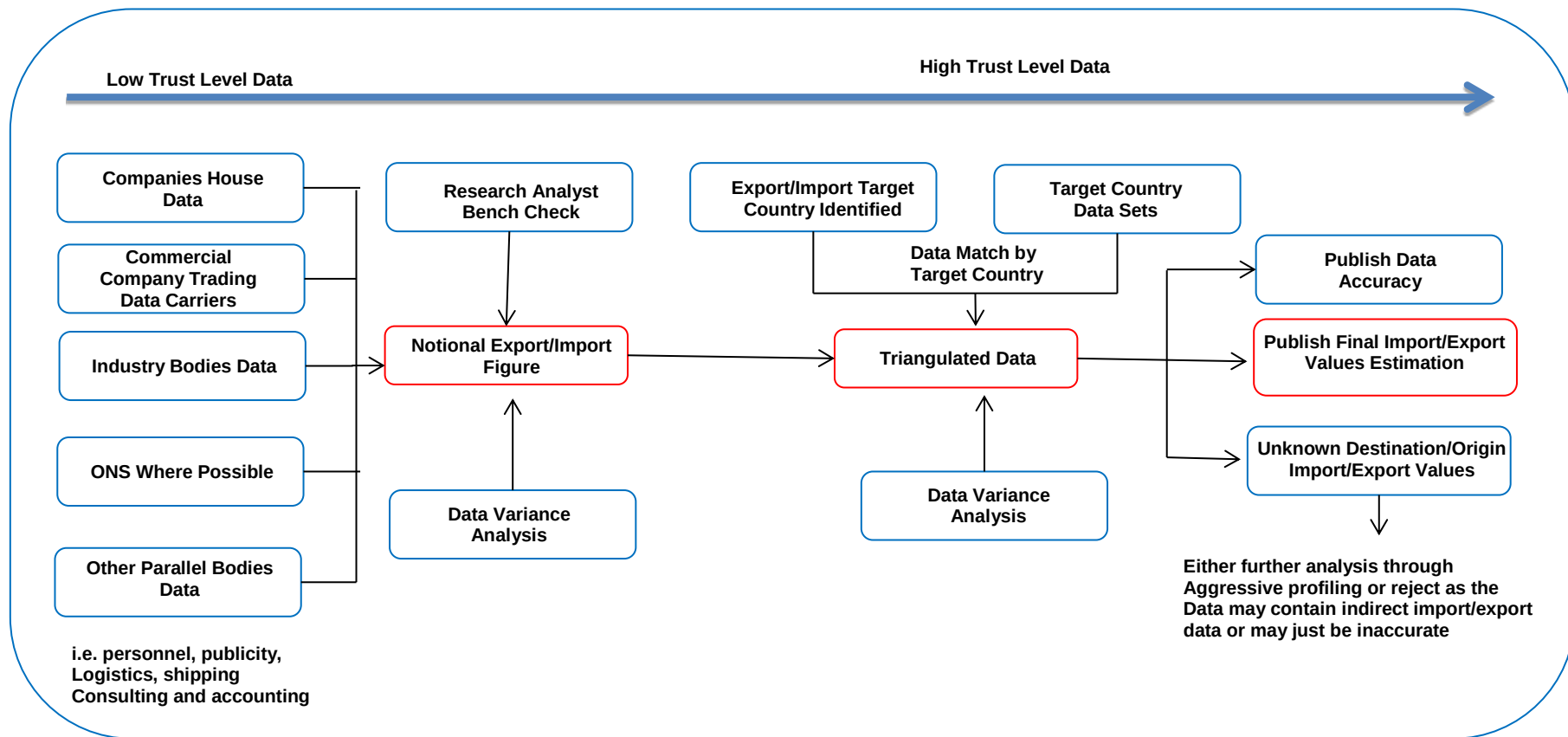


Figure 85 : The Assessment of Import and Export Trading for Sectors

The quality assurance of the accuracy of import/ export data has historically been achieved through a series of blind tests that involve large exporters sharing data with a trusted third party (like a Government Department) and the Research Analysts having to provide estimates of company exports using its own processes. This is a form of competitor

intelligence, the type that is practiced daily by the more competitively focused companies. The results of these blind tests are typically within the confidence levels quoted for the research i.e. the estimated value is within +/- 15% of the actual company number.

Other ways of testing the data include case studies. In Case Study 2, the client was a Government Department and the challenge was to reconcile two divergent versions of national exports. Ultimately, the case proved that single sourced data can often be misleading.

Case Study 3: Using Multiple Sources to Estimate/ Reconcile Export Values

The Question

Why is there a significant difference between what CIMA reports about Israeli exports and what Israel reports about itself?

The Approach:

Using the standard multi- source approach highlighted above

The Findings:

R&D Operations For International Companies in Israel:

- PayPal
- IBM
- EMC
- GE
- VMWare
- Cisco
- Deutsche Telekom
- Lockheed Martin
- CA Technologies
- McAfee

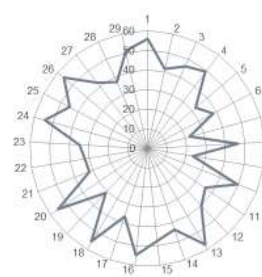


This creates a complex cluster of companies when it comes to measuring value-added

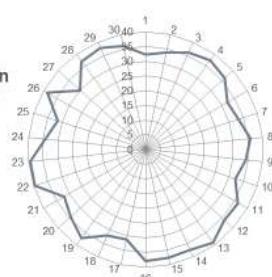
The Evidence:

In- Country data sources vary significantly in their reporting and in addition they also vary on a year by year basis. This means that fewer data sources reach our data standard.

International data sources are more consistent and in addition they tend to maintain their relatively tight data variance on a year by year basis

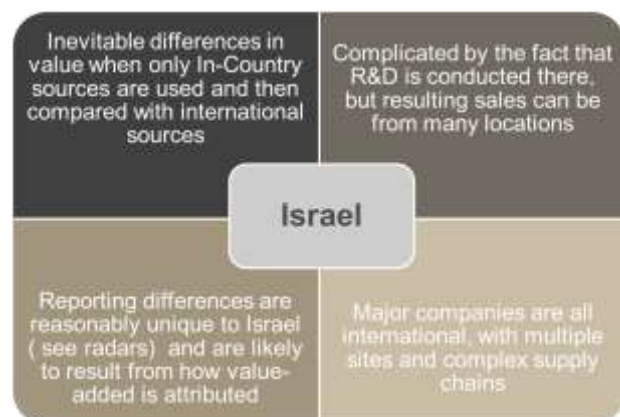


Note the differences in calibration



Internal Country sources can often claim all of the good news, but this is often mediated by international data sources

The Conclusions:



1.1.132 Export Data Example

To illustrate the process for calculating exports we have included a “deep dive” example for Chinese exports into France and Germany. The example includes data from two sub-sectors- Identity and Access Based Services and Mobile Services- and the data subset is shown at Table 55 values for both France and Germany. *Note: Values are in Sterling, as this was how they are stored in the Source Management System.*

Table 55 : Data Subset for Export Example (m GBP)

Level 2	Level 3	Level 4	Level 5	France	Germany
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	Large Corporate Networks	0.015	0.038
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	Small Business Networks	0.007	0.010
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	Cloud Services Networks	0.005	0.012
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	Public Sector Networks	0.005	0.009
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	Smart Comms Networks	0.010	0.019
Identity & Access Based Services	Messaging Security	Development of Software for Messaging Security	General Applications	0.003	0.006
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	Large Corporate Networks	0.053	0.332
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	Small Business Networks	0.024	0.089
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	Cloud Services Networks	0.010	0.076
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	Public Sector Networks	0.019	0.093
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	Smart Comms Networks	0.025	0.109
Identity & Access Based Services	Messaging Security	Supply of Software for Messaging Security	General Applications	0.007	0.033
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	Large Corporate Networks	0.031	0.280
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	Small Business Networks	0.013	0.176
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	Cloud Services Networks	0.015	0.152
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	Public Sector Networks	0.015	0.164
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	Smart Comms Networks	0.025	0.276
Mobile	Mobile Security/Device Management	Development of Software for Remote Access Management	General Applications	0.007	0.115
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	Large Corporate Networks	0.011	0.259
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	Small Business Networks	0.002	0.164
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	Cloud Services Networks	0.002	0.142
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	Public Sector Networks	0.004	0.163
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	Smart Comms Networks	0.005	0.192
Mobile	Mobile Security/Device Management	Supply of Software for Remote Access Management	General Applications	0.001	0.040
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	Large Corporate Networks	0.027	0.115
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	Small Business Networks	0.011	0.027
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	Cloud Services Networks	0.012	0.040
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	Public Sector Networks	0.013	0.041
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	Smart Comms Networks	0.011	0.074
Mobile	Mobile Security/Device Management	Consulting Services for Remote Access Management	General Applications	0.009	0.030

The full sample dataset is shown at Section 1.1.105.

The export values were calculated using the process described in Section 1.1.113 and using the sources listed in Appendix I. Companies were then validated using some or all of the steps identified in Section 1.1.113. The sample is designed to show how individual exporters were traced as part of the aggregation and quantification process. The sample does not attempt to show all Chinese exporters in each of the market areas shown in Table 55, rather (to reduce complexity) it shows the most representative exporters (up to four in number). So, the totals in the Appendix will not equal the totals in the above table. This is because Chinese exports are often very fragmented (high volume and low value) and are sometimes provided as an input into a wider service i.e. mid to low end of the supply/ value chain.

The Appendix tables show a range of metrics, which demonstrate some of the ways in which Chinese exporters were searched for, identified and categorized:

- Value- actual or estimated contract value per Chinese exporter
- Mode of contract- in searching through procurement sources it is possible to identify whether an export sale is “ad hoc”, a full contract, part of a wider contract or “unknown”
- Delivered by- the name of the exporter from China (this is different from a Chinese exporter). A total of 34 are included as part of this example
- Partners- Occasionally an export sale is delivered through, and identified within, a partnership i.e. with Apple, IBM etc.
- Source of Procurement- country where the export arrives i.e. France or Germany
- Contract- the procurement data and other sources will often identify a contract as “direct” or delivered via a consortium
- Data Confidence- as described in Section 1.1.122, levels of data confidence are calculations based upon the spread of values in the sources consulted. The range is 71%-98%
- Number of sources used- we typically use at least seven sources of validate each calculated value. In this example, the range is between 7- 22.

In total, 34 China- based exporters are listed for the sample activities, each of which appears several times in the example data. These are listed below:

30WISH	HILLSTONE	PAYEGIS
360 ENTERPRISE SECURITY	INTERFRITYTECH	RISING
ANTIY	JIT	SAFEDOG
BANGCLE	JN TASS	SANGFOR
BLUEDON	KINGSOFT SECURITY	SBR-INFO
CNNS	KNOWNSEC	SUNINFO
DBAPPSECURITY	LENEDSEC	SURFILTER
DBSEC	MEIYA PICO	TOPSEC
EVERSEC	NETENTSEC	VENUSTECH
FEITIAN	NEUSOFT	VRV
GOOANN	NSFOCUS	WESTONE
H3C		

This “deep dive” example into exports illustrates the “connection” between the aggregated and high-level export values and the underlying and disaggregated transactional nature of the data. It shows how the different processes as outlined earlier - export analysis, company search, source management- are combined within the larger research model.

Final Report Executive Summaries

This Cybersecurity Industry Market Analysis (CIMA) report documents the market research of the European Cybersecurity industry and its comparison with other relevant markets. PwC and LSEC – Leaders In Security performed the study for the European Commission in 2017 – 2018.

The report results from a quantitative research for gathering, categorising and analysing the Cybersecurity Industry Market data of 2016, by applying a big data approach to extracting economic and market values from over 900, mainly transactional data sources. Its methodology considers all relevant Cybersecurity sales, including products and services that are distributed and resold by system integrators, and represents genuine economic activities. The study considers companies that solely provide Cybersecurity products and services; companies that (amongst other activities) provide Cybersecurity products and services; and companies that provide products and services that form part of the Cybersecurity supply/value chain.

The report builds a Cybersecurity products and services catalogue and analyses what products and services require attention taking into account the Network Information Security directive, the existing gaps in the market and the upcoming trends and threats.

It documents the strengths of the European Cybersecurity market in supply and demand, including the sector's segmentation, vertical market insights and comprises an analysis of the demand patterns per category and the geographical market fragmentation. Furthermore, the intra and extra European market flows and the main barriers that providers find when selling their products and services inside and outside the European market are documented.

The report concludes with a wrap-up of the main findings of the study and an overview of the strengths, weaknesses, opportunities and threats of the European Cybersecurity market.

Dieser Bericht über die Marktanalyse der Cyber-Sicherheitsbranche (CIMA) dokumentiert die Marktforschung der europäischen Cyber-Sicherheitsbranche und ihren Vergleich mit anderen entsprechenden Märkten. PwC und LSEC – Leaders In Security führten die Studie 2017–2018 für die Europäische Kommission durch.

Der Bericht beruht auf quantitativer Marktforschung zur Erfassung, Kategorisierung und Analyse der Marktdaten 2016 der Cyber-Sicherheitsbranche im Form eines Big-Data-Ansatzes, mit dem Wirtschafts- und Marktzahlen aus mehr als 900 Quellen, vor allem Transaktionsdatenquellen, gewonnen wurden. Diese Methodik berücksichtigt alle entsprechenden Cybersicherheitsverkäufe, darunter Produkte und Dienstleistungen, die von Systemintegratoren vertrieben und weiterverkauft werden, und die tatsächliche wirtschaftliche Aktivitäten abbilden. Die Studie berücksichtigt Unternehmen, die ausschließlich Cyber-Sicherheitsprodukte und -dienstleistungen anbieten, Unternehmen die (neben anderen Aktivitäten) Cyber-Sicherheitsprodukte und -dienstleistungen anbieten sowie Unternehmen, die Produkte und Dienstleistungen anbieten, die Teil der Liefer- oder Wertschöpfungskette für Cyber-Sicherheit sind.

Der Bericht enthält einen Katalog von Cyber-Sicherheitsprodukten und -dienstleistungen und analysiert unter Berücksichtigung der Richtlinie über die Sicherheit von Netzen und Informationssystemen, der vorhandenen Lücken auf dem Markt und der sich abzeichnenden Trends und Bedrohungen, welche Produkte und Dienstleistungen Aufmerksamkeit benötigen.

Er dokumentiert die Stärken des europäischen Cyber-Sicherheitsmarkts bei Angebot und Nachfrage sowie die Segmentierung der Branche und vertikale Markteinblicke. Außerdem enthält er eine Analyse der Nachfragemuster nach Kategorie und die geografische Marktfragmentierung. Darüber hinaus werden die Marktbewegungen innerhalb und außerhalb des Europäischen Marktes sowie die wichtigsten Hindernisse dokumentiert, vor denen Anbieter stehen, wenn sie ihre Produkte und Dienstleistungen innerhalb und außerhalb von Europa vertreiben.

Der Bericht schließt mit einer Zusammenfassung der Hauptergebnisse der Studie und einem Überblick der Stärken, Schwächen, Chancen und Bedrohungen des europäischen Cyber-Sicherheitsmarktes.

Le présent rapport d'analyse du marché de l'industrie de la cybersécurité (CIMA - *Cybersecurity Industry Market Analysis*) reprend les études de marché de l'industrie européenne de la cybersécurité et les compare avec d'autres marchés pertinents. PwC et LSEC – Leaders in Security ont réalisé cette étude pour la Commission européenne en 2017 – 2018.

Le rapport résulte en une recherche quantitative pour le rassemblement, le classement et l'analyse des données du marché de l'industrie de la cybersécurité en 2016, en appliquant une approche big data pour extraire les valeurs économiques et les valeurs du marché de plus de 900 sources de données, principalement transactionnelles. La méthodologie de l'étude prend en compte toutes les ventes pertinentes de produits de cybersécurité, y compris les produits et services qui sont distribués et revendus par les intégrateurs de systèmes, et représente de véritables activités économiques. L'étude prend en compte les sociétés qui fournissent uniquement des produits et services de cybersécurité, les sociétés qui fournissent des produits et services de cybersécurité (et qui effectuent d'autres activités) et les sociétés qui fournissent des produits et services faisant partie de la chaîne d'approvisionnement/de valeur du secteur de la cybersécurité.

Le rapport établit un catalogue de produits et services de cybersécurité et analyse les produits et services qui nécessitent une attention particulière en tenant compte de la directive sur la sécurité des réseaux et des systèmes d'information, des lacunes existantes sur le marché et des tendances et menaces à venir.

Il reprend les forces du marché européen de la cybersécurité en termes d'offre et de demande (notamment la segmentation du secteur et les perspectives verticales du marché) et comprend une analyse des tendances des demandes par catégorie et de la fragmentation géographique du marché. En outre, le rapport reprend également les flux de marché dans et en dehors de l'Europe et les principaux obstacles rencontrés par les fournisseurs lors de la vente de leurs produits et services au sein du marché européen et en dehors.

Le rapport conclut par un résumé des principales conclusions de l'étude et un aperçu des forces, faiblesses, opportunités et menaces du marché européen de la cybersécurité.

European Commission

Cybersecurity Industry Market Analysis – CIMA

Luxembourg, Publications Office of the European Union

2018– 358 pages

ISBN 978-92-76-08859-2

doi:10.2759/018751



doi:10.2759/018751

ISBN 978-92-76-08859-2