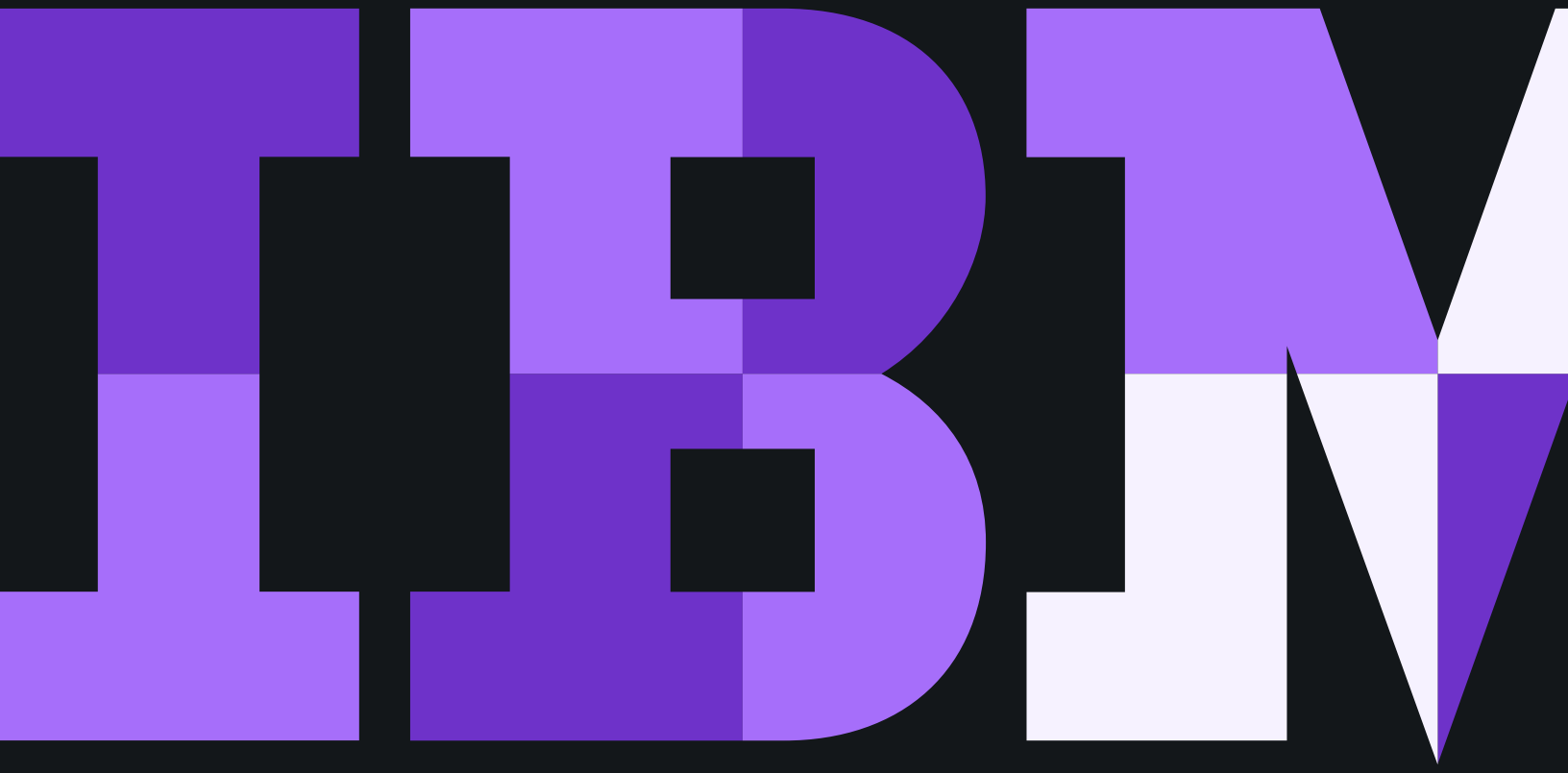
IBM Security

January 2020

Strategies for managing cybersecurity risk

Assess and advance your security and compliance posture



IBM

Contents

The current cybersecurity landscape

Data breaches, ransomware attacks, privacy failures and other cybersecurity challenges are on everyone's radar screen, yet most businesses still struggle with effectively preparing for them. Many organizations lack a clear and aligned security strategy, have limited insight into their cybersecurity maturity and insufficiently practice their plans for responding to a cybersecurity incident — if they have an incident response plan at all. You could say that most organizations' approach to risk management is, in fact, pretty risky.

Organizations often face disruptive forces that increase IT risk: mergers, acquisitions and divestitures; developing technologies such as cloud, IoT and quantum; and regulatory compliance changes. At the same time, organizations must innovate and move forward while addressing security and compliance. Challenges that can hold companies back include:

- Complex regulatory requirements
- Lack of alignment on security strategy as well as cybersecurity and compliance maturity
- Frequent organizational changes
- Security skills shortages
- Uncertainty regarding security "best practices"

279 days

The global average time to identify and contain a breach

25,575 records

The global average size of a data breach

Lost business

The biggest contributor to data breach costs[1]

Meet risks with action

Keeping up with cybersecurity threats and regulatory compliance isn't easy. Many companies engage the support of trusted advisors to better understand their cybersecurity and compliance posture, learn best practices and pursue their business goals in the face of cyber uncertainty. With a trusted advisor, you can better anticipate disruption, adapt to a changing security landscape and look to new innovations to gain a competitive advantage without losing sight of security.

Leading organizations seek accurate benchmarks of where they are and develop plans to better manage risk, compliance and governance. These assessments can include risk quantification; third-party security risk identification; penetration testing to find weaknesses in one's own systems; as well as cyber breach simulations to test personnel and technology, identify requirements and build muscle memory to prepare for cyberattacks.

Cyber ranges are increasingly becoming a part of leading organizations' risk management strategies. They allow organizations to bring together their security teams and key executives to experience a simulated security breach in a contained environment. A cyber range experience can help organizations to assess gaps in their incident response plan and critically evaluate how their security and compliance teams should integrate incident response across their entire organization.

Finastra tests their cyberattack readiness with IBM

London-based Finastra, one of the largest financial technology companies in the world, engaged IBM Security for a cyber range event to test their ability to battle a cross-continental data breach.

Watch video

The pillars of security risk management: assess, reduce and manage

To minimize security risk, know your weaknesses and how to address them:

Assess your current cybersecurity and compliance posture

Determine how to best reduce risk

Manage risk exposure in the future

This kind of security introspection can richly benefit from an experienced, external perspective — a trusted advisor who can help you ask the right questions, use a tested approach for success and get results. **You need to uncover hidden security vulnerabilities that could expose your business to data breaches, regulatory non-compliance or other risks that have the potential to hurt your reputation and your bottom line.**

Using proven methodologies based on countless engagements and industry best practices, security advisors can help you to both identify risks and identify solutions to reduce those risks.

Security is a continuous challenge. An advisor can provide ongoing security monitoring, management and training to help you maintain a strong security and compliance posture, foster a security culture, help address new threats and adjust your security and compliance program over time.

A successful security strategy starts at the top. Trusted advisors can provide recommendations to help you prioritize resources, align decision-making and build executive support for the security and compliance initiatives that matter most. This can include cloud, IoT, mobile and other initiatives such that security is an integral part of your digital strategy and transformation initiatives.

Trusted advisors provide recommendations to help you prioritize resources, align decision-making and build executive support

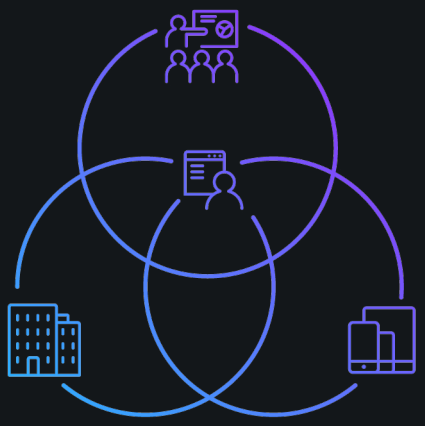
Navigate the unexpected

Risk is everywhere. It's outside your business, lurking in the form of hidden ransomware and brute-force attacks designed to divert your attention while data is being stolen. It's inside your business, crouched behind a trusted identity or introduced through simple human error. And it's standing in the shadows of opportunity, from automated factories to AI-powered customer care centers.

You need a trusted advisor to shine a light on risk and bring it out into the open. **You need a reliable view of risk in your organization that enables improved management of governance, risk and compliance.** No one expects to be the victim of a cyberattack until they are the victim of a cyberattack. A security advisor can help identify, quantify and prioritize risks, and then manage them.

Reliable risk management isn't the responsibility of a single person or team. It requires a systemic, aligned approach that reaches across business units, leaders and processes, intersecting every individual, machine and element of the organization.

Reliable risk management requires a systemic, aligned approach that reaches across business units, leaders and processes, intersecting every individual, machine and element of the organization



Trust IBM Security

With IBM Security, you never have to face risk alone. Our services help to ensure the right security and compliance capabilities are in place to manage risk effectively, spanning processes, people and technology. As the security landscape changes due to new threat vectors, new compliance regulations or even the unexpected, IBM's security expertise will be there to help you keep risk in check.

IBM Security expertise can help you create an effective security strategy, as well as critically evaluate your security and compliance posture across your entire organization, accurately measure your capabilities (e.g., how quickly you are able to respond to a data breach) and identify the weak links in your chain of control. IBM Security has the right people, methodologies and experience to help you assess, reduce and manage risk, including:

IBM Security Strategy Risk and Compliance Services (SSRC): We help you assess your current security governance against your corporate objectives, guide you in creating a risk management strategy and program, and then support your journey to improved security maturity. Working with IBM can help you better manage your risks, compliance and governance through:

- C-suite and board security advisory services
- Risk quantification
- Mergers and acquisition security risk assessment
- Cloud security and compliance
- Data privacy strategies
- Regulatory compliance and governance
- Third-party security risk assessment and management
- Automated IT risk management
- Critical infrastructure security
- SAP security strategy assessment and risk reduction
- Employee security awareness management

SSRC can help you assess, reduce and manage security risk. Whether your business needs expert guidance on regulatory compliance, a data privacy readiness review or to quantify risk for leadership, look to IBM Security Strategy Risk and Compliance services.

IBM Security Command Centers: Helping you prepare for your worst day while improving your overall security culture and readiness is what IBM's Command Centers do best. Cyber range engagements immerse your cross-functional teams in simulated security situations to help them develop and hone the skills and confidence they'll need to handle high-stakes cyberattack scenarios in the real world. At our Executive Briefing Centers, you can leverage IBM's security brain trust: experienced incident responders, penetration testers, security strategists and leaders who can help you dramatically improve your security posture and minimize your risk exposure.

Related topics

Compliance: You need to track how your organization is handling data, whether it's at rest or in motion, and be able to prove compliance at any point. Get ahead of regulatory shifts with compliance that is easier to manage and implement. Use solutions that help your organization address compliance so that you can deploy resources to other priorities. Simplify compliance with talent and technology from IBM Security.

Leadership and Culture: Technological innovations, market disruptions, changes in skill requirements and other factors can cause volatility impacting your security and compliance standing. While there is no magic shield to protect your organization, you can take effective measures to improve your security and compliance position with access to the latest research and insights on security trends and innovative solutions.

Sources

1. Ponemon Institute and IBM Security, “2019 Cost of a Data Breach Report,” 2019.

IBM Security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2020

GDPYL8KD