Five common data security pitfalls to avoid

Learn how to improve your security posture

IBM Security

Contents

Data security should be a top priority for enterprises, and for good reason.

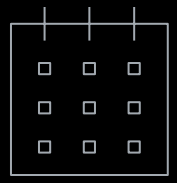
Even as the IT landscape becomes increasingly decentralized and complex, it's important to understand that many security breaches are preventable. While individual security challenges and goals may differ from company to company, often organizations make the same widespread mistakes as they begin to tackle data security. What's more, many enterprise leaders often accept these errors as normal business practice.

There are several internal and external factors that can lead to successful cyberattacks, including:

- Erosion of network perimeters
- Increased attack surfaces offered by more complex IT environments
- Growing demands that cloud services place on security practices
- Increasingly sophisticated nature of cyber crimes
- Persistent cybersecurity skills shortage
- Lack of employee awareness surrounding data security risks

$8.19 million

Average cost of a data breach in the United States in 2019[1]



245 days

Average time to identify and contain a data breach in the United States[1]

How strong is your data security practice?

Let’s look at five of the most prevalent—and avoidable—data security missteps that make organizations vulnerable to potential attacks, and how you can avoid them.

Accelerate compliance

Centralize security

Establish ownership

Assess vulnerabilities

Prioritize activities

Pitfall 1

Failure to move beyond compliance

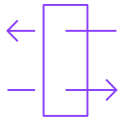
Compliance doesn't necessarily equal security. Organizations that focus their limited security resources to comply with an audit or certification can become complacent. Many large data breaches have happened in organizations that were fully compliant on paper. The following examples show how focusing solely on compliance can diminish effective security:

Incomplete coverage
Enterprises often scramble to address database misconfigurations and outdated access polices prior to an annual audit. Vulnerability and risk assessments should be ongoing activities.

Minimal effort
Many businesses adopt data security solutions just to fulfill legal or business partner requirements. This mindset of "let's implement a minimum standard and get back to business" can work against good security practices. Effective data security is a marathon not a sprint.

Fading urgency
Businesses can become complacent towards managing controls when regulations, such as the Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR), mature. While, over time, leaders can be less considerate about the privacy, security and protection of regulated data, the risks and costs associated with noncompliance remain.

1.4



per day

1.4 healthcare data breaches estimated per day in 2019 despite Health Insurance Portability and Accountability Act (HIPAA) legislation.[2]

Omission of unregulated data
Assets, such as intellectual property, can put your organization at risk if lost or shared with unauthorized personnel. Focusing solely on compliance can result in security organizations overlooking and under protecting valuable data.

Solution

Recognize and accept that compliance is a starting point, not the goal

Data security organizations must establish strategic programs that consistently protect their business' critical data, as opposed to simply responding to compliance requirements.

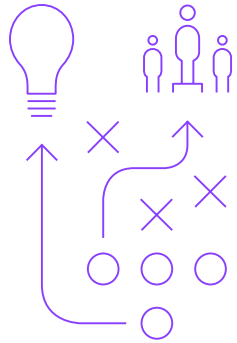
Data security and protection programs should include these core practices:

- **Discover and classify your sensitive data** across on-premises and cloud data stores.
- **Assess risk** with contextual insights and analytics.
- **Protect sensitive data** through encryption and flexible access policies.
- **Monitor data access and usage patterns** to quickly uncover suspicious activity.
- **Respond to threats** in real time.
- **Simplify compliance** and its reporting.

The final element can include legal liabilities related to regulatory compliance, possible losses a business can suffer and the potential costs of those losses beyond noncompliance fines.

Ultimately, you should think holistically about the risk and value of the data you seek to secure.

View compliance as an opportunity to innovate and raise your security standards to support your business.



Pitfall 2

Failure to recognize the need for centralized data security

Without broader compliance mandates that cover data privacy and security, organization leaders can lose sight of the need for consistent, enterprise-wide data security.

For enterprises with hybrid multicloud environments, which constantly change and grow, new types of data sources can appear weekly or daily and greatly disperse sensitive data.

Leaders of companies that are growing and expanding their IT infrastructures can fail to recognize the risk that their changing attack surface poses. They can lack adequate visibility and control as their sensitive data moves around an increasingly complex and disparate IT environment. Failure to adopt end-to-end data privacy, security and protection controls—especially within complex environments—can prove to be a very costly oversight.

Operating security solutions in silos can cause additional problems. For example, organizations with a security operations center (SOC) and security information and event management (SIEM) solution can neglect to feed those systems with insights gleaned from their data security solution. Likewise, a lack of interoperability between security people, processes and tools can hinder the success of any security program.

Encryption, business continuity management, integrating security into the software development process (DevSecOps) and threat intelligence sharing can help lower data breach costs.[1]

Solution

Know where your sensitive data resides, including on-premises and cloud-hosted repositories

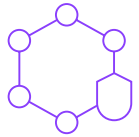
Securing sensitive data should occur in conjunction with your broader security efforts. In addition to understanding where your sensitive data is stored, you need to know when and how it's being accessed, as well—even as this information rapidly changes. Additionally, you should work to integrate data security and protection insights and policies with your overall security program to enable tightly aligned communication between technologies. A data security solution that operates across disparate environments and platforms can help in this process.

So, when is the right time to integrate data security with other security controls as part of a more holistic security practice? Here are a few signs that suggest your organization may be ready to take this next step:

Risk of losing valuable data
The value of your organization's personal, sensitive and proprietary data is so significant that its loss would cause significant damage to the viability of your business.

Regulatory implications
Your organization collects and stores data with legal requirements, such as credit card numbers, other payment information or personal data.

Securing sensitive data should occur in conjunction with your broader security efforts.



Lack of security oversight
Your organization has grown to a point where it's difficult to track and secure all the network endpoints, including cloud instances. For example, do you have a clear idea of where, when and how data is being stored, shared and accessed across your on-premises and cloud data stores?

Inadequate assessment
Your organization has adopted a fragmented approach where no clear understanding exists of exactly what's being spent across all your security activities. For example, do you have processes in place to measure accurately your return on investment (ROI) in terms of the resources being allocated to reduce data security risk?

If any of these situations apply to your organization, you should consider acquiring the security skills and solutions needed to integrate data security into your broader existing security practice.

Pitfall 3

Failure to define who owns responsibility for the data

Even when aware of the need for data security, many companies have no one specifically responsible for protecting sensitive data. This situation often becomes apparent during a data security or audit incident when the organization is under pressure to find out who is actually responsible.

Top executives may turn to the chief information officer (CIO), who might say, “Our job is to keep key systems running. Go talk to someone in my IT staff.” Those IT employees may be responsible for several databases in which sensitive data resides and yet lack a security budget.

Typically, members of the chief information security officer (CISO) organization aren’t directly responsible for the data that’s flowing through the overall business. They may give advice to the different line-of-business (LOB) managers within an enterprise, but, in many companies, nobody is explicitly responsible for the data itself. For an organization, data is one of its most valuable assets. Yet, without ownership responsibility, properly securing sensitive data becomes a challenge.

74%

of organizations surveyed say that cybersecurity skills shortage has impacted their organization.[3]

“In 2018, 67.9% of surveyed firms reported having a chief data officer (CDO). However, the role remains ill-defined.”[4]

NewVantage Report
Big Data and AI Executive Survey 2019, Executive Summary of Findings

Read the study →

Solution

Hire a CDO or DPO dedicated to the well-being and security of sensitive and critical data assets

In complex IT environments, it's critical to account for data in the following locations:

Shared across business units

Located in hybrid multicloud infrastructures

Stored on mobile devices

A chief data officer (CDO) or data protection officer (DPO) can handle these duties. In fact, companies based in Europe or doing business with European Union data subjects face GDPR mandates that require them to have a DPO. This prerequisite recognizes that sensitive data—in this case personal information—has value that extends beyond the LOB that uses that data. Additionally, the requirement emphasizes that enterprises have a role specifically designed to be responsible for data assets.Consider the following objectives and responsibilities for choosing a CDO or DPO:

Technical knowledge and business sense
Assess risk and make a practical business case that nontechnical business leaders can understand regarding appropriate security investments.

Strategic implementation
Direct a plan at a technical level that applies detection, response and data security controls to provide protections.

Compliance leadership
Understand compliance requirements and know how to map those requirements to data security controls so that your business is compliant.

Monitoring and assessment
Monitor the threat landscape and measure the effectiveness of your data security program.

Flexibility and scaling
Know when and how to adjust the data security strategy, such as expanding data access and usage policies across new environments by integrating more advanced tools.

Division of labor
Set expectations with cloud service providers regarding service-level agreements (SLAs) and the responsibilities associated with data security risk and remediation.

Data breach response plan
Finally, be ready to play a key role to devise a strategic breach mitigation and response plan.

Ultimately, the CDO or DPO should lead in fostering data security collaboration across teams and throughout your enterprise, as everyone needs to work together to effectively secure corporate data. This collaboration can help the CDO or DPO oversee the programs and protections your organization needs to help secure its sensitive data.

Pitfall 4

Failure to address known vulnerabilities

High-profile breaches in enterprises have often resulted from known vulnerabilities that went unpatched even after the release of patches. Failure to quickly patch known vulnerabilities puts your organization's data at risk because cybercriminals actively seek these easy points of entry.

However, many businesses find it challenging to quickly implement patches because of the level of coordination needed between IT, security and operational groups. Furthermore, patches often require testing to see if they don't break a process or introduce a new vulnerability.

In cloud environments, sometimes it's difficult to know if a contracted service or application component should be patched. Even if a vulnerability is found in a service, its users often lack control over the service provider's remediation process.

51%

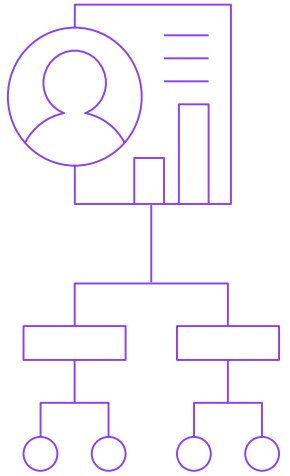
of breaches recorded in 2019 were caused by malicious attacks. Malicious attacks are the most common and expensive leading cause of breaches.[1]

Solution

Establish an effective vulnerability management program with the appropriate technology to support its growth

Vulnerability management typically involves some of the following levels of activity:

- Maintain an accurate inventory and baseline state for your data assets.
- Conduct frequent vulnerability scans and assessments across your entire infrastructure, including cloud assets.
- Prioritize vulnerability remediation that considers the likelihood of the vulnerability being exploited and the impact that event would have on your business.
- Include vulnerability management and responsiveness as part of the SLA with third-party service providers.
- Obfuscate sensitive or personal data whenever possible. Encryption, tokenization and redaction are three options for achieving this end.
- Employ proper encryption key management, ensuring that encryption keys are stored securely and cycled properly to keep your encrypted data safe.



Even within a mature vulnerability management program, no system can be made perfect. Assuming intrusions can happen even in the best protected environments, your data requires another level of protection. The right set of data encryption techniques and capabilities can help protect your data against new and emerging threats.

Pitfall 5

Failure to prioritize and leverage data activity monitoring

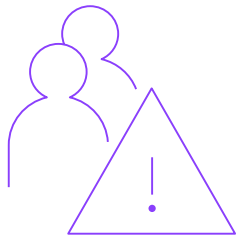
Monitoring data access and use is an essential part of any data security strategy. An organization leader needs to know who, how and when people are accessing data. This monitoring should encompass whether these people should have access, if that access level is correct and if it represents an elevated risk for the enterprise.

Privileged user identifications are common culprits in insider threats.[5] A data protection plan should include real-time monitoring to detect privileged user accounts being used for suspicious or unauthorized activities. To prevent possible malicious activity, a solution must perform the following tasks:

- Block and quarantine suspicious activity based on policy violations.
- Suspend or shut down sessions based on anomalous behavior.
- Use predefined regulation-specific workflows across data environments.
- Send actionable alerts to IT security and operations systems.

The global average cost of an insider threat is

$11.45 million.[6]



Accounting for data security and compliance-related information and knowing when and how to respond to potential threats can be difficult. With authorized users accessing multiple data sources, including databases, file systems, mainframe environments and cloud environments, monitoring and saving data from all these interactions can seem overwhelming. The challenge lies in effectively monitoring, capturing, filtering, processing and responding to a huge volume of data activity. Without a proper plan in place, your organization can have more activity information than it can reasonably process and, in turn, diminish the value of data activity monitoring.

Solution

Develop a comprehensive data detection and protection strategy

To that end, when starting on a data security journey, you need to size and scope your monitoring efforts to properly address the requirements and risks. This activity often involves adopting a phased approach that enables development and scaling best practices across your enterprise. Moreover, it's critical to have conversations with key business and IT stakeholders early in the process to understand short-term and long-term business objectives.

These conversations should also capture the technology that will be required to support their key initiatives. For instance, if the business is planning to set up offices in a new geography using a mix of on-premises and cloud-hosted data repositories, your data security strategy should assess how that plan will impact the organization's data security and compliance posture. If, for example, the company-owned data will now be subject to new data security and compliance requirements, such as the GDPR, California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD) and so on.

You should also prioritize and focus on one or two sources that likely have the most sensitive data. Make sure your data security policies are clear and detailed for these sources before extending these practices to the rest of your infrastructure.

The average total cost of a data breach was

95% higher

in organizations without security automation deployed in 2019.[1]

$5.16 million **without automation**.[1]

$2.65 million **with fully-deployed automation**.[1]

You should look for an automated data or file activity monitoring solution with rich analytics that can focus on key risks and unusual behaviors by privileged users. Although it's essential to receive automated alerts when a data or file activity monitoring solution detects abnormal behavior, you must also be able to take fast action when anomalies or deviations from your data access policies are discovered. Protection actions should include dynamic data masking or blocking.

As you develop your data activity monitoring and protection plans, it's often helpful to consider the following questions:

- What are my top two most sensitive data sources?
- Which five to ten data sources should I prioritize next, based on their volume of sensitive data?
- Are certain endpoints or cloud assets associated with higher-risk data?
- Is sensitive data freely moving to and from on-premises, hybrid and cloud environments?
- Which users should be granted access to the data source and under what conditions?
- What high-risk users or privileged accounts need to be turned off or require closer scrutiny?
- Does my data security solution support real-time activity monitoring and automated data protection capabilities?
- Is real-time monitoring in place to track data in files residing in data stores, such as Structured Query Lanuage (SQL) databases, Hadoop distributions, Not only SQL (NoSQL) platforms and so on.
- Does my monitoring solution account for data stores spanning hybrid multicloud environments and allow me to generate customized reports that go to the right people at the right time?
- Do I have the risk analytics and filtered monitoring capabilities needed to effectively prioritize risk, vulnerabilities and remediation efforts?

The more specific you can be about monitoring priorities and protection requirements, the more effective the solution will be for you to apply its available detection and response resources.

What's next?

How can you avoid these common data security pitfalls, especially as more companies are pursuing hybrid multicloud environments? It begins with recognizing the issue and preparing your organization to take a proactive and holistic approach to securing data, regardless of where it resides.

If your business has a complex and hybrid IT environment, you can't afford a siloed approach to data security. You need to add data protection strategies that span across your entire data infrastructure and support all your data types.

Immediate next steps you can take to protect your organization's valuable data include:

- Building a data security strategy that supports your organization's short-term and long-term business and technology objectives
- Implementing that strategy with the proper people, processes and tools
- Planning your resources to ensure your data security and compliance program can effectively scale as your organization embraces modern technologies

IBM® Security Guardium® data protection platform is designed to help organizations take a smarter and more adaptive approach to protecting critical data wherever it resides. See why it can be a good fit for your organization.

Learn more at ibm.com/guardium.

>4 weeks

Most organizations recognize value from Guardium in less than one month.[7]

Why IBM Security?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications. It offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures.

IBM operates one of the world's broadest security research, development and delivery organizations, monitoring more than

60 billion

security events per day in more than 130 countries.

IBM holds more than 3,700 security patents

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2020

1 “Cost of a Data Rreach report 2019.” *IBM Security*. databreachcalculator.mybluemix.net/executive-summary

2 “Healthcare Data Breach Statistics.” *HIPAA Journal*. www.hipaajournal.com/healthcare-data-breach-statistics

3 Jon Oltsik. “The Life and Times of Cybersecurity Professionals 2018.” *Enterprise Strategy Group and Information Systems Security Association International*, April 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, “Big Data and AI Executive Survey 2019 Executive Summary of Findings.” *NewVantage Partners*, 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. “Why Privileged Account Management Is Key to Preventing Insider Threats.” *Security Intelligence*, June 20, 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 “Cost of Insider Threats: Global Report 2020.” *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 “Ponemon Report: Client Insights on Data Protection with Guardium.” *Ponemon Institute*, August 2019. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

SEL03144-USEN-02