5 Epic Fails in Data Security

Common Data Security Pitfalls and How to Avoid Them

Introduction

Data security is on everyone's mind these days, and for good reason. Although the number of data breaches in the first half of 2017 was about the same as the first halves of 2015 and 2016, the number of records stolen between January 1 and June 30, 2017 has exceeded all of 2016.[i] And that's not counting one of largest security breaches of all time, announced in September.

Many factors are contributing to the increase in successful attacks – the erosion of network perimeters and increased attack surfaces offered by more complex IT environments, a growing use of cloud services and the new demands that places on security practices, and the increasingly sophisticated nature of cyber criminals – and the landscape continues to evolve.

One part of this story that has remained consistent over the years, however, is that most security breaches are preventable. Although every organization's security challenges and goals are different, there are widespread mistakes that many organizations make as they begin to tackle data security. What's worse, these mistakes are often accepted as the "norm," hiding in plain sight under the guise of common practice.

This paper looks at five of the most prevalent – and avoidable – data security missteps organizations are making today, and how these "epic fails" open them up to potentially disastrous attacks.

Is your data security practice all that it should be? Read on to see if your organization's data security practices are sound enough to face the pressure of today's threat landscape.

1 – Failure to move beyond compliance

The failure: It is often said that compliance does not equal security, and most security professionals would agree with that statement. Yet time and again, organizations focus many of their always-limited security resources on proving compliance, and then, upon receiving their certification, become complacent. One sign of this is that many of the largest data breaches in recent years have happened in organizations that are fully compliant on paper. Several examples show how an emphasis on compliance alone actually works against effective security:

- Compliance certification often represents a "snapshot in time". For example, when it comes to patch management, too often there is a scramble to bring all endpoints up to date just prior to an audit. Once the auditor is happy, everyone breathes easy until next year's audit. This intense focus on patch management should not be an annual event, but rather an ongoing activity.
- Many businesses adopt security solutions because of a legal requirement to do so, or because a business partner requires it. This engenders a mind-set of "let's implement a minimum standard that gets us past this pesky requirement so we can get on with our business." That mindset actually works against good security practices.
- Another aspect of compliance that encourages the "minimum standard" or "checkbox" mentality is that compliance with most standards is graded on a "pass-fail" system, which encourages organizations to invest only what's necessary to "pass". Passing has nothing to do with the quality or effectiveness of the implementation. Good security requires moving beyond the checkbox mentality.
- Businesses often focus their attention on controls related to new regulations, but as time passes and the urgency fades, they become lax in managing those controls. There was a lot of attention paid to regulatory requirements around Sarbanes Oxley when it was new, and PCI and HIPPA/HITECH a few years later. Today the focus is on GDPR. When there is no new regulation, people become less thoughtful about data privacy, data security and data protection, yet the threats do not go away.
- Finally, it is important to remember that compliance only deals with data that is regulated. Most organizations have data assets (such as intellectual property) that don't fall under the compliance umbrella, but could still put the organization at risk if they were lost or shared with the wrong people. Focusing solely on compliance leaves this data out of the picture.

The Solution: Organizations need to recognize and accept that compliance is not the goal. It is just a starting point.

A data security and protection practice, including all the controls an organization adopts to put this practice in place and continuously enforce it, should serve business needs, not just compliance requirements. A security standard provides excellent guidance, but specific implementations must be based on factors unique to each organization, including:

- Risk assessments that relate directly to the business value of the data in question, including legal liabilities related to regulatory compliance, but also all the possible losses a business can suffer and the potential costs of those losses beyond noncompliance fines.
- Vulnerability assessments that take into account exposures across the entire infrastructure.
- The organization's ability to effectively implement and manage controls in a consistent way.

Ultimately, organizations need to think holistically about the risk and value of the data they seek to secure. Rather than stopping at compliance, they should view it as an opportunity to innovate and raise their security standards in a way that fully supports the business.

2 – Failure to recognize the need for centralized data security

The failure: Compliance can help raise awareness for the need for data security, but without broader compliance mandates that cover data privacy and security, organizations forget to move past compliance and actually focus on consistent, enterprise-wide data security. A typical organization today has a heterogeneous IT environment that is constantly changing and growing. New types of data sources pop up weekly, if not daily, and sensitive data is dispersed across all of these sources.

Many companies, especially those that are growing and expanding their IT infrastructures, fail to recognize the risk their changing attack surface poses. They focus their efforts on perimeter defenses and solutions that provide security information and event management (SIEM), but they lack adequate visibility and control over their sensitive data as it moves around the increasingly complex IT environment. A data security strategy that rigorously protects 50 percent of an organization's sensitive data sources is still exposing half of its data – this is a serious vulnerability. Failure to adopt end-to-end data privacy, security and protection controls, especially in the era of big data and complex environments that include mainframes and cloud instances, can prove to be a very costly oversight.

These negative effects are compounded when organizations operate their security solutions in silos, rather than allowing data security to serve as the foundation for a holistic security approach. For example, while most organizations are aware of the need for a Security Operations Center (SOC) and SIEM (Security Intelligence and Event Management) solution, many fail to realize the importance of feeding the SOC and SIEM solutions with the insights gleaned from their data security solution. Operating in this way results in each solution being less effective alone than they could be working together.

The solution: Companies must recognize the need to protect data and take actions that focus on securing it in conjunction with their broader security efforts. This first requires knowledge of where sensitive data is, and which data sources need protection – even as this information changes daily. Second, organizations must work to integrate data security and protection insights and policies with their overall security program to enable tightly aligned communication between technologies – and adopting a platform agnostic data security solution is one way to begin down this path.

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 an organization may be ready to take this step:

- The value of personal data, sensitive data, and an organization's own proprietary data is significant enough that its loss would be a serious blow to the viability of a business.
- The organization collects and stores data that has regulatory implications. This might be credit card numbers, other payment information, or personal data.
- An organization has grown to the point where its existing method of tracking and securing all its network end points, including cloud instances, is becoming very difficult, or the organization no longer has a clear idea of what is in its network.
- An organization is pursuing a fragmented approach to data security in which there is no clear understanding of exactly what is being spent across all its security activities, and there is no way to accurately measure the return on its investment in terms of risk reduction.

If an organization experiences any of these situations, and no one in the organization is actually responsible for the data itself or the security initiatives required to protect it, then it is time to consider acquiring dedicated data security skills and a data security solution that integrates with the existing security practice.

3 – Failure to define who owns responsibility for the data itself

The Failure: Even if awareness of the need for data security exists, in many companies, no one specifically owns responsibility for the sensitive data that's being collected, shared, and depended upon to perform business operations. This becomes obvious if you try to find out who is actually responsible.

You can tell when top executives scratch their heads and direct you to the CIO, and the CIO says "No, our job is to keep key systems running, go talk to someone in my IT staff." That person, who may in fact be responsible for several databases in which sensitive data resides, doesn't actually have a security budget. Then, there are folks on the CISO's team that are responsible for various aspects of security… but they aren't directly responsible for the sensitive data that's flowing through the organization. They may give advice to the different lines of businesses within an organization, but in most companies, nobody is explicitly responsible for the data itself. This is ironic given that data is one of the business's most valuable assets – yet without ownership responsibility, properly securing sensitive data becomes a challenge.

The Solution: In today's complex IT environments that include data sharing across business units, data in hybrid cloud infrastructures that involve third party service level agreements, data on mobile devices, and sophisticated cyberattacks that have become big business, someone in the organization needs to own responsibility for data itself. To effectively account for this, organizations should have a Chief Data Officer (CDO) or Data Protection Officer (DPO) who is dedicated to the well-being and security of sensitive and critical data assets. Companies based in Europe or doing business with EU data subjects now face GDPR regulations that require them to have a DPO. This requirement sets a positive example, because it shows clear recognition of the fact that sensitive data, in this case personal information, has value that extends beyond the line of business that holds it, and there must be a role specifically designed to be responsible for data assets.

When outlining the objectives and responsibilities for this role, organizations should consider the following:

- The CDO or DPO must have both technical knowledge and business sense. This person will be able to assess risk and make a practical business case that non-technical business leaders understand regarding appropriate security investments for the business.
- The CDO or DPO will be able to direct a data security strategy at a technical level that implements detection, response, and data security controls to provide protections

- They will understand compliance requirements and know how to map those requirements to data security controls so that the business is compliant.
- They will monitor the threat landscape and measure the effectiveness of the data security program.
- They should know when adjustments are needed in the data security strategy, such as when it's time to implement a SOC and integrate more advanced data security tools.
- They will be instrumental in setting expectations with cloud service providers regarding who is responsible for what parts of the shared data security program that is part of any cloud service.
- Finally, the CDO or DPO will play a key role in helping devise a response plan in the event of a data breach.

Ultimately, the CDO or DPO will take the lead in fostering data security collaboration across teams and throughout the enterprise. To effectively secure corporate data, everyone needs to work together. Work groups and teams need to be open to collaboration under the guidance of the CDO or DPO, who will be dedicated to all the programs and protections an organization needs to secure its sensitive data.

4 – Failure to address known vulnerabilities

The Failure: Industry research shows that 99 percent of all exploits use known vulnerabilities, while malware and ransomware attacks typically use vulnerabilities that are at least six months old.[ii] Recent high profile breaches have resulted from known vulnerabilities that went unpatched even after patches were released. Cyber criminals actively seek unpatched vulnerabilities, because these are easy points of entry. Failure to quickly patch known vulnerabilities puts an organization's data at risk. Many organizations, however, are challenged to quickly implement patches because of the level of coordination needed between IT, security, and operational groups. Furthermore, patches often require testing to be sure they do not 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, and even if a vulnerability is found, users of that service often do not have control over the service provider's remediation process.

The Solution: To meet these challenges, organizations must have an effective vulnerability management program – and the technology to support it. Vulnerability management typically involves several levels of activity, including:

- Maintaining an accurate asset inventory and baseline state for those assets.
- Conducting frequent vulnerability scans and assessments across the entire infrastructure, including cloud assets. This can be automated.
- Having a method of prioritizing vulnerability remediation that considers the likelihood of the vulnerability being exploited and the impact that would have on the business.
- When third party service providers are involved, including vulnerability management and responsiveness as part of the service level agreement. Don't be shy about pressing for quick remediation of a known vulnerability.
- Obfuscating sensitive or personal data whenever possible. Encryption, tokenization and redaction are three options for achieving this end.

Even with an excellent vulnerability management program, no system can be made perfectly bullet proof. Assuming intrusions are going to happen even in the best protected environments, data requires another level of protection. As stated above, the right set of data encryption techniques and capabilities can help secure data against new and emerging threats. It can also act as a strategic tool set for all types of business environments — whether they have adaptable, new technology platforms, or older, more rigid legacy technologies

5 – Failure to prioritize and leverage data activity monitoring

The Failure: In addition to moving past compliance, establishing organizational awareness of the need for comprehensive data security, establishing data ownership and addressing vulnerabilities, monitoring data access and use is an essential part of any data security strategy. Organizations need to know who, how, and when people are accessing data, if they should be, if that access is normal or not, and if it represents elevated risk. For instance, privileged user IDs are the most common culprits in insider threats. A data protection plan should include real-time monitoring of privileged users – in the case that there's a malicious privileged user, or if there's a privileged user whose credentials have been compromised. To prevent possible malicious activity, a solution needs to identify outliers, block activity, conduct dynamic masking that ensures sensitive data is not shared, and quarantine user accounts associated with high-risk access activities.

Keeping tabs on all of this information at once and knowing how to act on it, however, can prove difficult. Thus, the challenge for many organizations comes from monitoring and capturing too much activity data, and having no reasonable plan to efficiently filter, process, and respond to the huge volume of data that's captured. With all the authorized users accessing all manner of data sources (databases, file systems, mainframe environments, cloud environments, etc.), monitoring and saving data on every interaction across every data source across the enterprise becomes a heavy lift. Without a proper plan in place, it's possible for a security organization to have more activity information than it can reasonably process, resulting in a needle-in-the-haystack scenario that defeats the purpose of monitoring in the first place: protecting the business's most critical assets.

The Solution: Detection and protection is the heart of any data security strategy, so it is important to develop a strategy that aligns with the organization's risk and security management program, which in turn ties directly to business requirements. When starting on a data security journey, organizations need to size and scope monitoring efforts to address those requirements and risks. This often involves adopting a phased approach that enables development and scaling best practices across the enterprise.

Organizations should begin by prioritizing 1 or 2 data sources that have the most sensitive data, and start in a focused way. They need to make sure data security policies are clear and tight for these limited sources before extending their practices to the rest of the infrastructure. Furthermore, they should look for a data or file activity monitoring solution that is automated, with rich analytics that can hone in on key risks and unusual behaviors, while also allowing them to add on automated data protection activities that will work best for the business. Many organizations just starting out opt for automated security alerting when a data or file activity monitoring solution detects abnormal behavior. Usually, only more sophisticated and mature data security deployments leverage capabilities like dynamic data masking or blocking.

As organizations engage in the process of developing data activity monitoring and protection plans, they should be asking themselves the following questions:

- What are my top 2 most sensitive data sources? These will be the starting points.
- Which 5-10 data sources should I plan to target next, based on their volume of sensitive data? The initial phase of monitoring and control will scale to cover these.
- Are there high risk users or privileged accounts that need to be turned off or that require closer scrutiny?
- Does the monitoring solution support real time activity monitoring and automated data protection capabilities?

- Are there certain endpoints or cloud assets associated with higher risk data freely moving to and from on-premises, hybrid, and cloud environments? Real-time monitoring needs to track data in files, databases, Hadoop distributions, NoSQL platforms and more.
- Does the monitoring solution generate customized reports and escalate them to the right people at the right time?
- Does the solution provide rich risk analytics and help filter monitoring results to hone in on the riskiest areas?

The more specific an organization can be about monitoring priorities and protection requirements, the more effective it will be in applying its available detection and response resources.

Conclusion

In complex IT environments, businesses cannot afford to continue with siloed approaches to data security. Organizations must adapt their data protection strategies to span across their entire data infrastructure and support all data types.

There is nothing easy about securing sensitive data to combat today's threat landscape. But there are steps organizations can take to assure they are devoting the right resources to protect their valuable data assets.

Key elements underlying the 5 epic fails described in this paper include building a data security strategy that truly supports an organization's risk appetite and security requirements, and then implementing that strategy with a proper set of resources and tools. Few organizations, however, can afford all the security measures they would like to have, so when resources and budgets are limited, it is of paramount importance to prioritize and leverage the resources they do have.

To learn more about data security and an end-to-end data security and protection offering that can flexibly meet your needs, go to the IBM Security Guardium web site.

[i] Tina Orem, "'Stunning' Increase in Data Breaches in 2017," CreditUnionTimes, July 26, 2017

[ii] Brian Evans, "Assessing Risks and Remediating Threats With a Layered Approach to Vulnerability Management," SecurityIntelligence, August 9, 2017