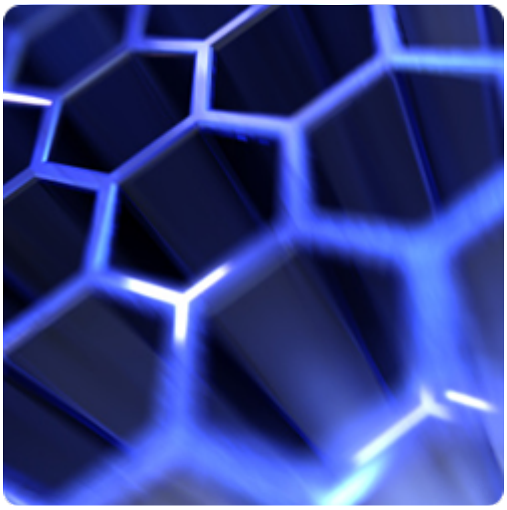
@ISACA

Five Key Lessons Learned From Publicly Disclosed Data Breaches and Security Incidents



Author: John P. Pironti, CDPSE, CGEIT, CISA, CISM, CRISC, CISSP, ISSAP, ISSMP

Date Published: 27 November 2019

Key lessons can be learned from publicly disclosed data breaches and security incidents. These lessons can help organizations more effectively focus their investments and efforts to prevent themselves from becoming victims in similar instances. Recently, both the pace and impact of data breaches and security incidents have increased, and many organizations are deficient in their information risk management and security programs.

The following 5 key lessons can be learned from publicly disclosed data breaches and security incidents:

- **Security policies and standards must meet your organization's capabilities**—Organizations are often held accountable to policies and standards in legal proceedings. In the Equifax Data Breach Settlement, the US Senate Banking committee highlighted that Equifax did not comply with their own published information security policies and standards on multiple occasions. For example, Equifax's IT team was required to install critical patches within 48 hours. A 9 March 2017 email from an Equifax's internal security team noted that the Apache Struts vulnerability required patching. Equifax did not complete patching for the Apache Struts vulnerability until August 2017, approximately 173 days later.
  In some cases, organizations develop and publish information security policies and standards with expectations and requirements that they believe they need to include to satisfy customers, regulators and other stakeholders even though they do not have the means or intention of being able to comply with them. This practice can be more damaging to an organization in legal proceedings and/or public perception than if they were to include expectations and requirements with which they could realistically and consistently comply. Establishing standards that can be successfully implemented and maintained gives organizations the opportunity to explain their strategy and plans to enhance their capabilities within commercially reasonable timeframes to align with leading practices, expectations and requirements.

- **Visibility of assets key to protection**—You cannot protect what you do not know. In the case of the of the Equifax data breach, it was noted that the lack of patching of affected systems was, in part, due to reduced visibility. The vulnerability management scanning solutions that would have identified this issue were disabled due to an expired digital certificate.
  Oftentimes, organizations focus their visibility activities exclusively on production environments or Internet-facing assets. Capable and motivated adversaries are aware of this and often target assets outside of this focus as to avoid detection. It is important for organizations to develop and maintain a comprehensive asset inventory and to monitor all their systems and technologies that process, store or interact with sensitive data assets. This inventory should also include configuration management information about these capabilities so organizations can quickly identify vulnerable systems and technologies once a new credible threat or vulnerability is identified and validated.

- **Zero-day attacks are often not the biggest threat to an organization**—Many organizations have a heightened level of concern for their ability to detect and repel zero-day attacks, even though they are more likely to be affected by attacks that exploit vulnerabilities they are already equipped to remedy. Adversaries will try to take advantage of zero-day attacks, but these attacks are often limited to advanced and

capable attackers. In many cases, materially impacting attacks, such as the city of Baltimore (Maryland, USA) ransomware attack, take advantage of attack code and vulnerabilities that have been available for use and exploitation for significant periods of time.
Organizations should focus their protective activities on well-known and understood threats and vulnerabilities that can negatively affect them immediately. Once they are secure, they can then spend time and effort on combating new and less mature attacks, unless one is imminent.

- **Vendor-based insider attacks can cause significant breaches and incidents**—It is often the case that a knowledgeable and capable insider can cause significant material damage to an organization in ways that are not easily defended or remediated. In the Capital One data breach, it was not a Capital One employee who carried out the attack, but an individual who worked for a key and trusted vendor of Capital One, Amazon Web Services (AWS). This individual had intimate knowledge of Capital One's Amazon-based operating environment and was able to evade defenses and controls to carry out one of the largest data breaches publicly disclosed to date. This situation highlights the need for organizations to extend their strategies for insider threat monitoring and prevention to third parties that interact with sensitive data assets, key business technologies and processes. "Trust, but verify" should be instilled in the governance processes for these vendors. Contracts should define expectations of monitoring capabilities and security controls to mitigate insider risk, and organizations should establish a regular set of communications and security reviews with third parties. This can help ensure that insider-threat-based security controls are constantly maintained, monitored and matured appropriately.

- **Expectations of due care are rising as security capabilities are considered easier to implement and follow**—Organizations that have been subject to legal action as a result of data breaches and security incidents are often held to a standard known as due care. A recognized legal definition of due care that aligns with information risk and security programs is, "[Due care] refers to the level of judgment, care, prudence, determination and activity that a person or organization would reasonably be expected to do under particular circumstances."
The characteristics of due care change as expectations of affected parties evolve and the ability for organizations to more easily implement leading security practices and technologies becomes readily available. Both legal systems and the court of public opinion typically do not accept that foundational and hygiene-focused security measures and controls are hard to implement and maintain. These are considered a cost of doing business that should be incurred to provide proper protections.
Organizations should focus on areas of information security hygiene with an immediate focus on visibility of assets, patching, configuration management and system hardening at a minimum. An April 2018 study by *InformationWeek: Dark Reading* found that 60% of organizations that experienced a data breach cited a

> known, unpatched vulnerability as the root cause, so patching a known vulnerability becomes an expectation of due care.

Publicly disclosed data breaches and security incidents highlight the threats and vulnerabilities that organizations consistently face every day. This information should be used as valuable intelligence to help organizations adjust their information risk and security strategy approach. Organizations that learn and implement strategies based on these examples strengthen their capabilities to combat and prevent future data breaches and incidents. At a minimum, organizations can use this information to understand due care expectations and incorporate these data into their information risk profiles and strategies.

John P. Pironti, CISA, CRISC, CISM, CGEIT, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

Previous Article Next Article

QUICK LINKS

Resources

COBIT

ISACA Journal

Press Releases

Resources FAQs

Insights and Expertise ›

Audit Programs and Tools

Publications

White Papers

Engage Online Community

News & Trends >

@ ISACA

Industry News

ISACA Now Blog

ISACA Podcasts

ISACA TV

ISACA Videos

Frameworks Standards and Models >

IT Audit

IT Risk

Glossary

Call for Case Studies

Contact Us | Terms | Privacy | Cookie Notice | Fraud Reporting | Bug Reporting | COVID-19