Equifax Case Study

Minjoo Kim
Georgia Institute of Technology
Atlanta, GA, USA
Email: mkim908@gatech.edu

Do you think Equifax executed an incident response effort that aligns with the incident response process discussed in lesson 4?

Equifax policies and plans on paper; however, it is unlikely that Equifax strongly enforced these policies. David Webb, the former CIO, testified that the company allowed the breach mainly because they could not execute the policies. The U.S. House Report noted from its patch management audit that the company had several vulnerability issues, but the company did not implement any of the recommended updates prior to the data breach in 2017. The company did not create a comprehensive policy and plan nor procedures that handled security incidents.

On March of 2017, Equifax Security ran a component scan for any system vulnerabilities within Apache Struts, but was unable to find any fault despite its apparent vulnerabilities. It is possible that the failure to implement the right scanner for the job allowed the breach to happen.

Equifax did not establish a strong line of communication, which also led to failure in implementing detective and preventative security controls. Graeme Payne, the former Senior VP and CIO for Global Corporate Platforms, stated that "[Equifax] had notifications, but we didn't notify… everyone that needed to be notified…" The company's former CEO Richard Smith also testified that "failure to communicate the need to apply a patch" as one of the underlying reasons for the breach.

The detection and analysis process was also severely delayed. Although the cyberattack occurred in May 2017, it wasn't until July that the company noticed this unusual activity. These delays also gave the attackers enough time to cause extensive damage to the system, which limited the ability for the company to isolate compromised systems during the critical early stages of the cyberattack. Although Equifax was eventually able to restore its systems, the delayed eradication of the threats had a huge impact on Equifax's operations.

Given that resources are almost always constrained, what improvement to the IT or security environment would you chose to implement first and why?

Equifax should benefit from implementing the right patch management system as the company primarily suffered due to its failure to apply the correct patch for the Apache Structs vulnerability, even with internal audit's recommendation to implement the new patch. Although advanced detection tools or incorporating complex security architectures could help decrease the cybersecurity risk, updating the patch management system could be the most cost-effective method to address the root cause of various large-scale data breaches.

In the U.S. House of Representatives oversight report, there is a good discussion on the reporting relationship of the Chief Information Security Officer. At the time of the incident the CISO reported to the Chief Legal Council. In the report, it is stated repeatedly that a better structure would be to have the CISO report to the Chief Information Officer. The Equifax CISO now reports to the CEO. Which reporting structure do you feel would be best from a cyber incident response perspective?

For technical risk mitigation, it may be more helpful for the CISO to report directly to the CEO, as this reporting structure could allow the CEO to mobilize the resources faster to isolate the risk and respond to the incident promptly. Reporting to the CEO often escalates the security risk and calls for executive attention. Although reporting directly to the CIO could improve technical implementations and integrations with the current IT models, it can potentially cause delays in the incident response for multiple reasons. For example, CIOs are often evaluated in their project delivery; addressing these incidents could potentially affect business operations and prevent the team from delivering more, which could deter the CIO's incentive to address the issue at hand promptly.

References

U.S. House of Representatives, Committee on Oversight and Government Reform. (2018, December). *The Equifax data breach* (Majority Staff Report, 115th Congress).