CLIENT ALERT

Lessons From the House Report on the Equifax Breach

Dec.20.2018

On December 10, 2018, the Republican majority of the House Oversight and Government Reform Committee released a report detailing the Committee's 14-month long investigation and conclusions relating to Equifax's September 2017 data breach, which compromised the personal information of 148 million Americans. The Democratic minority also released a shorter, separate report that provides some insight into the priorities of the incoming majority regarding data protection legislation.

The Majority Report detailed how the Equifax incident, which the Committee described as "entirely preventable," resulted from a combination of institutional and technological errors within the company.

As chronicled by the Report, the attackers penetrated Equifax's network through its outside-facing Automated Consumer Interview System (ACIS) by exploiting a back-end piece of open-source software called Apache Struts. The Report attributed this vulnerability in part to "a culture of cybersecurity complacency" at the company.

Two Points of Failure

The House Report faulted Equifax for not addressing two specific points of failure that would have allowed it to "mitigate, or even prevent, this data breach." First, the company's IT management structure lacked clear lines of authority, leading to a gap between IT policy development and execution. Second, Equifax's aggressive growth strategy and rapid growth "resulted in a complex IT environment" dependent on custom-built legacy systems that it was unprepared or unable to secure.

1. The Report Faulted Equifax's Chain of Command:

The report first faulted Equifax's lack of clear authority within its IT department. The lines of responsibility between the company's CIO, CSO, and the CIO's subordinates were often blurry and unclear. Equifax's internal structure was unusual in that the CSO did not report to the CIO, but rather to the company's chief legal officer. The House report describes this CIO/CSO split as creating an "accountability gap" because it separated IT operational and security responsibilities—the CSO and Security personnel designed the security practices, but it was up to IT personnel to implement them directly, over whom the CSO had no direct authority.

For example, the Report noted that the company's patch management policy effectively operated "on the honor system." Responsibility for keeping systems current was not transparently assigned to specific employees; instead, Equifax acknowledged that it had been relying on employees to self-designate as system owners with operational responsibilities for the maintenance of specific systems.

Equifax did not ensure clear ownership of the creation of security policy, its implementation, and clarity in the connection between the two.

2. The Report Found that Equifax's Growth Outpaced its Cybersecurity Protections

Equifax's second major failure was its unwillingness to sufficiently prioritize its security program alongside its aggressive acquisition strategy. Equifax devoted minimal resources, relative to its size and the volume of data it controlled, to privacy and data security. The Report detailed the company's unwillingness to devote serious resources to its IT and Security infrastructure problems while pursuing an aggressive acquisition and expansion strategy. As a result of both its historical operations and recent acquisitions, the company's IT infrastructure contained a large and increasing number of unique legacy IT systems, against the backdrop of its organizational chaos, while the policy and operational disconnect continued. The company's environment was so fragmented it did not have a complete inventory of IT systems—and it had declined to fund several requests from internal stakeholders for resources to create one.

Even the resources that Equifax did have were under or ineffectively utilized—for example, the intrusion-detection system that detected the compromise had been nonfunctional for 19 months due to an expired certificate. As soon as its certificate was renewed, the problem was detected, but the damage was already done—and millions of individuals' records were exposed.

Equifax's security situation was so complex and disorganized that it prevented the company from identifying which systems needed to be patched in the first place. Although the company used two different commercial scan tools with an updated signature to check for the vulnerability used by the attackers once it was publicly disclosed, both failed.

The mobility of the attackers within Equifax's system was greatly enhanced by the company's failure to follow basic security procedures. The Report faulted Equifax for failing to deploy file integrity monitoring, limit access to sensitive files within its secured system, segment within its secured legacy networks, or even keep an accurate inventory of the tools operating in its environment. Once the attackers were able to get in to the initial application used to compromise Equifax's network, they were quickly able to make more of their access and compromise the organization on a global level. The system initially compromised in the breach had access to more than 40 of the company's internal databases, despite only needing three to function properly.

Recommendations from the Majority:

The Majority made a number of recommendations for those wishing to learn from Equifax's failures. The Report suggested that greater transparency by companies like Equifax would help to empower consumers to better know what data is collected and how it is used. The Report also suggested that the Federal Trade Commission's oversight authority and the current identity monitoring and protection services commonly offered as remediation in data breach scenarios should both be assessed for adequacy. The Majority further suggested that private industry in general and federal contractors specifically should be subject to greater disclosure requirements about cybersecurity risks. Practically, the Majority recommended a reduction in the use of Social Security Numbers as personal identifiers, and instead encouraged the government and private sector to explore the possibilities offered by "new technology," while encouraging companies storing sensitive consumer data to "transition away from legacy IT and implement modern… solutions."

Ultimately, the Majority report shows how deep lawmakers are willing to dig into a company's dirty laundry when faced with the degree of public outrage generated by an incident of this scale. Taking heed of the recommendations in the Report (and the failures it detailed) is a good step towards ensuring that large organizations are taking important measures to prevent similar attacks.

Signals from the Minority:

Democratic Committee staff also released a report detailing the Minority's recommendations for new legislation in response to the breach, which are likely indicative of where the Democrats' priorities will be as they take the House Majority next year.

According to the minority, there are "four key legislative reforms" that will help prevent future attacks:

1. To "hold federal financial regulatory agencies accountable for their consumer protection oversight responsibilities," primarily the CFPB and banking regulators.
2. To "require federal contractors to comply with established cybersecurity standards and guidance from the National Institute of Standards and Technology (NIST)," specifically, the standards in Special Publication 800-171 that already apply to DoD contractors.
3. To "establish high standards for how data breach victims should be notified" via the creation of a "comprehensive federal notification law."
4. Finally, "strengthen the ability of the Federal Trade Commission (FTC) to levy civil penalties for private sector violations of consumer data security requirements" by allowing the FTC to immediately penalize companies whose data security practices violate Section 5 of the FTC Act, rather than being limited to consent decrees in the aftermath of a major security failure.

The Equifax breach and these reports leave companies with a number of lessons to ponder in attempting to avoid a similar fate.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Kristin J. Madigan, CIPP/US
Partner – San Francisco
Phone: +1 415.365.7233
Email: kmadigan@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Evan D. Wolff
Partner – Washington, D.C.

Phone: +1 202.624.2615
Email: ewolff@crowell.com

Lee Matheson, CIPP/US/E/A, CIPM, PCIP
Associate – Washington, D.C.
Phone: +1 202.654.6728
Email: lmatheson@crowell.com