CMMI® Institute
AN ISACA ENTERPRISE

Cyber Lessons for Enterprises from the Equifax Breach and Record Fine

By E. Doug Grindstaff II, CMMI® Institute Sr. VP of Cybersecurity Solutions

Government regulators and representatives of Equifax announced a settlement on penalties and consumer restitution related to the 2017 data breach that exposed sensitive information belonging to 148 million people. The potentially $700 million agreement, the largest of its kind, revealed on July 22, 2019, still needs to be approved by a court.

In addition to the actions by state and federal U.S. agencies, last May Moody's credit rating agency downgraded Equifax, making it the first company to have its credit outlook negatively affected for cybersecurity reasons.

All of this serves as a reminder of just how fast the fortunes of any company—large or small—can fall due to cybersecurity concerns. In the wake of the attack, annual profits for Equifax were cut in half and the CEO, CIO and CSO were removed. Equifax also has been providing credit monitoring for victims since the breach, and those services will continue as part of the settlement. The monetary costs to Equifax are measurably high, but the reputational impact of this breach should not be confused with the settlement amount—the reputational impact is far greater. There is no insurance coverage or balance sheet that can overcome the impact to the brand of a loss in trust.

Equifax also compounded its problems by not being upfront about the breach. Data was stolen from Equifax over a 76-day period through a flaw that was known, but accidentally not fixed. Then, once it discovered the breach in July 2017, Equifax waited another six weeks to inform customers and government regulators.

Enterprises can't be in denial about cyber breaches. For all enterprises, it is a matter of when, not if, a breach will occur. You will be hit. And when that inevitable day comes, the enterprise needs to be ready, to be in a cyber-resilient position.

Moving forward, Equifax clearly needs to refocus its efforts on cybersecurity, and the Moody's downgrade of Equifax shows how much work needs to be done. Public trust needs to be restored—and monetary penalties only go so far in that regard. Equifax's new leadership team and board of directors must show they are taking the right actions.

To achieve cyber resilience, enterprises should assess which risks are their greatest cyber risks—the ones most likely to irrevocably damage or destroy that particular business—and then focus resources on a roadmap to mitigate those risks and overcome them when trouble arises. No enterprise can protect against every risk, so it makes sense to prioritize efforts and build cyber maturity in the areas most appropriate to that unique business.

For Equifax, it wasn’t a matter of the risks they didn’t know—the organization knew about the flaw that allowed access to consumer information (the lifeblood of their business). Ultimately, the enterprise failed to prioritize a risk it was aware of in its most vital area of operations.

The key to not just restoring public confidence but also internal and Board confidence is a transparent understanding of organizational risks and the capability of the organization to mitigate. Strategically focusing resources on the most critical areas and making evidence-based decisions with regards to investments is critical to building a more resilient organization. Resiliency is owned by everyone, and building cyber maturity requires constantly reassessing and prioritizing the most relevant risks.

The CMMI Cybermaturity Platform help enterprises on their journey toward cyber resilience. It provides a risk-based approach to measuring and managing security risks in the context of the business mission and strategy. This CMMI cybersecurity capability maturity model solution:

- Offers a unique cybersecurity risk assessment framework to simplify security gap analysis.
- Prioritizes a customized roadmap of improvements based on the organization’s unique cybersecurity risks.
- Provides an evidence-based approach for assessing, optimizing and reporting on cyber capabilities.
- Helps to implement leading frameworks, stay ahead of the cybersecurity vulnerabilities and threats most relevant to your business, and build board confidence in your cyber programs.

Equifax could benefit by taking a similar cyber resilient approach to rebuilding its cybersecurity function and business reputation. Meanwhile, every enterprise can learn from these missteps and should be preparing for the day when the organization will inevitably face a breach. The damage and its aftermath will depend on how cyber resilient the enterprise has become.