MILLIMAN WHITE PAPER

# Assessing and quantifying cyber risk:

## Could today's emerging cyber regulation have helped prevent the Equifax breach?

**Mark Stephens**, Managing Director, Risk Advisory Services
**Lisa Henderson**, Chief Strategist, Casualty Products and InsurTech Consulting

Milliman

In February 2017, New York's Governor Andrew Cuomo announced cybersecurity regulations to protect the state's financial services industry and consumers from the threat of cyberattacks.

At the time, the regulation covered banks, insurance companies, and other financial services companies. Then in September 2017, the consumer credit reporting agency Equifax announced it had been hacked in a cyber breach, potentially affecting over 143 million consumers. Immediately thereafter, Gov. Cuomo proposed expanding these regulations so that credit reporting agencies would also need to meet these requirements.

As cyberattacks occur with increasing severity and frequency, cyber risk has quickly emerged as a critical risk exposure that has moved to the top of many organizations' 10K risk lists or enterprise risk management (ERM) risk registers. Furthermore, current and future regulation will require a reliable, evidence-based approach to risk assessment as one of the minimum requirements for compliance. This article outlines actionable steps for companies looking to assess and quantify their cyber exposure.

## The evolution of cyber risk

Years ago, large organizations noticed an increasing number of network incidents such as small data breaches, minor Distributed Denial of Service (DDoS) attacks, employee errors, and contractor access issues, along with customer concerns about data security. As some of these incidents escalated into more serious operational interruptions and created reputational damage issues, these organizations began to increase staff and budget to better manage these concerns. At the same time, boards of directors, regulators, large clients, and other key stakeholders were asking more questions about the control and management of these risks.

What most stakeholders began to realize was that to understand the extent of this risk exposure, there had to be some assessment of exposure vulnerability and potential organizational impact. What they found was that the determination of operational and financial materiality was both challenging and critical to managing the risk.

Often, companies need to determine if they have sufficient capital to cushion the negative financial impact of the risk. Equifax had to confront this question after its security breach was announced. The credit reporting agency took a major hit, and its CEO was replaced.

## Importance for large organizations and insurance companies

Not only is the determination of financial materiality important to organizations themselves, but also to insurance and reinsurance companies asked to underwrite different versions of cyber risk transfer strategies. A critical component of underwriting is the adequate understanding of the risk exposure itself and the financial consequences of an occurrence or an event.

This raises many questions in several key areas, including:

- Current control effectiveness
- Future or target control effectiveness
- Loss response preparation
- Customer impacts
- Insurance retention versus transfer
- Insurance limits determination
- Residual balance sheet or liquidity impact
- Reputational impact

Many organizations are struggling to devote the staff and resources necessary to adequately manage these cyber risk assessment objectives.

## Challenges to managing the risk assessment process

As boards of directors asked questions about cyber risk exposure levels, they are forced to confront their risk appetites or tolerance for some residual level of risk that might not be well controlled. In many cases, boards had no framework or measurements to support decision making for this discussion.

Milliman was recently invited to collaborate with a Fortune 50 client that wanted to build a risk management model to better understand its cyber risk exposure and to improve

the communication of such to its stakeholders. This project proved to be a valuable learning experience for both the client and Milliman. It brought together executives from corporate, business segments, and many functional departments. The first challenge was to assess and understand the company's dynamic and complex risk exposure. Milliman and the client made an early assessment decision to try to understand the risk on a residual basis with current controls. From there, Milliman strategized about the positive effect of future or targeted controls on the residual risk exposure and the resulting cost/benefit analysis. The client's risk assessment working group wanted the model to function like a risk management platform by examining the benefits of multiple potential strategies through a dynamic iterative process environment.

## Improving methods of risk assessment

In previous efforts, the company had used surveys, interviews, and consultants to cut and paste together a scoring index that ranked cyber risk against other significant risks. But this was considered more of a compliance or audit approach that was interesting, but not especially helpful in managing risk. The board of directors also thought it was an insufficient solution to support risk management capital decisions. The new approach was to combine internal and external expert opinions with company incident data, internal claims data, an information security framework score, an external loss event database, a large cyber event loss database, and a vulnerability score. These data inputs were used to parameterize a loss distribution using different threat vectors in unique scenarios.

There were numerous meetings with various stakeholders to validate assumptions and to gain consensus from the group. Some external benchmarks were used as a basis for customization and refinement.

## Frequency and severity

In understanding frequency and severity assumptions, there are many considerations that needed to be collaborated and validated. For example, unique loss scenarios were developed with multiple threat vectors so that frequency and severity inputs were viewed as being realistic and as evidence-based as possible.

## Translation to cash flows or capital

The model outputs needed to be directly connected to key financial measures including cash flows, equity, and capital needs. This financial statement connectivity allowed us to develop multiple use cases for the model and was the basis for formulating future mitigation strategies.

## Use cases and value proposition

There are multiple use cases for the cyber risk model that can add tangible business value to an organization. Since the global economy is so deeply dependent on data and networks, and with the impending explosion of the Internet of Things, organizations need to devote adequate resources to cyber risk assessment and capture the full value of the resulting model output. Considerations include:

1. Enhancing stakeholder communication with a framework for understanding the exposure
2. Determining financial materiality for regulatory filings
3. Developing a strong cost/benefit analysis for improved risk controls
4. Analyzing risk transfer insurance options considering both limits and retentions
5. Using cyber risk outputs in key ERM loss scenarios for stress testing
6. Helping to understand cyber exposures in merger/acquisition due diligence and third party risk assessment

Many regulatory and industry organizations have developed regulations, standards, principles, and risk frameworks around cyber risk. Some of these are the New York Department of Financial Services, the U.S. Chamber of Commerce, the National Association of Insurance Commissioners, and the American Institute of Certified Public Accountants. There will be more regulation to come, as evidenced by New York State's immediate response to the Equifax breach.

This begs the question: If these requirements had been in place prior to the Equifax breach, what would have happened? Regulation could have mandated that security officers have better tools to work with and mechanisms for highlighting the risk. It's possible that the breach could have been avoided entirely—or could have had a lesser impact or been better managed.

As more regulatory and government organizations follow New York's lead and enact similar regulations, and more businesses begin to fortify risk management strategies for cyber, the impact on both consumers and businesses could be profound.

**CONTACT**

Mark Stephens
mark.stephens@milliman.com

Lisa Henderson
lisa.henderson@milliman.com