MILLIMAN CASE STUDY

The cyber risk spend

How do you quantify the cost of cyber risk – and your return on investment?

Chris Harner, FRM
Lisa Henderson

Milliman

It is estimated that cyber breaches cost the U.S. economy anywhere from $57 billion to $109 billion in 2016,[1] more than the GDP of Puerto Rico.

But those numbers mask a cost for individual companies that varies dramatically based on industry sector, risk management protocols, and the type of breach.

In 2015, Milliman was approached by a major Fortune 50 company. The chief information security officer (CISO) was requesting hundreds of millions of dollars from his board for further cyber risk protections. But the size of the ask–and the frequency with which these funding requests were coming–caused the board to balk. They wanted numbers to support the spend. Before any additional funding would be approved, the CISO needed to quantify the cost of a potential cyberattack and justify his budget.

As cyber evolves as a threat, companies are facing an increasingly complex enterprise risk management (ERM) process: the need to not only assess the risk associated with an attack, but also quantify the potential cost of this risk in order to make sure the exposure is both fully protected and efficiently and accurately budgeted. Knowing *where* to allocate money is just as important as knowing *how much* money to allocate.

Putting dollar amounts behind controls such as cyber security, cyber insurance, and hiring practices helps build a business case for C-suite executives looking to quantify and justify what a company's cyber spend should be.

Milliman's work with the Fortune 50 company began with a methodology to evaluate the company's cyber risk exposure profile and the potential organizational impact of a breach. This includes liabilities that are both a direct and indirect result of an attack. Working with key stakeholders throughout the company, we identified the various threat vectors, potential assets that could be compromised, and security positioning. Important questions included:

- What type of information is vulnerable and how much exists?
- What security protocols are in place?
- What could be the cost of remediation and potential litigation as well as reputational impact?
- What are the potential costs not covered by cyber insurance?

By identifying over 200 different parameters via internal key risk indicators (KRIs), third-party data, and Milliman proprietary data, we built an actuarially sound model for our client that allows for scenario development in order to determine the potential costs associated with various types of plausible events. What would the financial impact be if the company fell prey to a spear-phishing scam? How does that differ from the costs associated with a malicious insider or a DDoS event such as a server slowdown or crash? Running tens of thousands of iterations using a simulation technique allowed us to create a continuous distribution of loss outcomes and quantify the potential range of cyber risk costs, including expected loss, tail loss, and the volatility around these losses.

Milliman's expertise and cyber model allowed our client to understand some of the more challenging questions associated with the cost of cyber exposure. How well would the company's current insurance cover the expected loss associate with a cyberattack? Are there gaps that need to be considered, and what do they look like? What if a more extreme event materialized–what are the possible drivers and how well is a company prepared for a worst-case scenario?

Perhaps most importantly, this distribution of loss outcomes also allowed Milliman to offer a cost-benefit analysis to our client. With this model, we were able to answer questions for the CISO such as:

- If the company were to spend $1 million to improve certain controls or hire additional resources, and if that improved the control environment and decreased the frequency or severity of an attack, how much money is the company saving?
- What dollar amount put toward mitigation or security protocol measures moves the needle –where do you see a return on investment?

[1] The Cost of Cyber Attacks to U.S. Economy. "Insurance Journal," February 20, 2018. Retrieved on September 26, 2018, from https://www.insurancejournal.com/news/national/2018/02/20/481121.htm.

One of the key issues for executives of any company is determining how the exposure changes as cyber risk evolves, and how in what ways investing could potentially change that outcome. By providing a cost-benefit analysis and linking the model results to our client's financial statements, Milliman was able to help quantify the impact of cyber risk from a business perspective and create an ongoing discussion about actionable results. Milliman's work with our Fortune 50 client provided not only more confidence to justify security spending and capital allocation, it also provided a structural approach to understanding and quantifying the company's residual cyber risk.

For more on Milliman's work quantifying cyber risk, visit www.milliman.com/cyber/.

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Chris Harner
chris.harner@milliman.com

Lisa Henderson
lisa.henderson@milliman.com