insight

EXPERT THINKING FROM MILLIMAN

Cyber risk management: Breaches, threats, and vulnerabilities

24 December 2012 | ELIZABETH BART, FCAS, MAAA

Even as news coverage of cyber-attacks becomes more frequent and insurance organizations such as the Risk and Insurance Management Society (RIMS), the Casualty Actuarial Society (CAS), and the Institute of Internal Auditors (IIA) offer educational programs focused on cyber risk, many companies still appear to be unprepared. Senior managements and boards of directors have a fiduciary responsibility to oversee all facets of risk management, including cyber risk.

Many corporate executives still appear to assume that their IT departments have protected them from cyber risk. However, cyber risk should not be viewed as a technology issue that can be isolated, but as a pervasive business risk with significant negative impact on assets, revenues, and profitability. The entire organization should be cognizant. Cyber risk can also adversely affect business strategy and its execution. The current investigations surrounding now-former CIA director David Petraeus and General John Allen exemplify the fact that no entity is immune from cyber risk. Company reputation, ability to retain core talent, and executive focus can also be adversely affected by mismanagement of cyber liabilities.

Cyber risk wake-up calls

Despite the increasing dependence on digital technology and year-old disclosure guidance issued by the Securities and Exchange Commission (SEC) on cyber risk,[1] relatively few mentions of cyber risk appear in regulatory filings.[2] While financial statements of individual companies fail to fully warn stakeholders of these risks, news stories on high-profile hacks are beginning to alert investors and customers.

On August 15, the world's largest oil company, Saudi Aramco, was hit with a computer virus that destroyed data on tens of thousands of company computers (about 75% of its corporate computers) and forced the shutdown of the internal corporate network including employee email.[3] It is believed that one or more insiders with privileged access maliciously inserted the virus into Aramco's network.

Around September 14, Barnes & Noble bookstores learned that hackers were stealing credit card information and PINs from customers using keypads separate from the registers at 63 of its stores.[4] The New York Times reported on this breach on October 23—the same day it ran the Aramco story. Moreover, in the last week of September many Americans experienced firsthand a wave of nonfunctioning online banking sites; six major banks (Bank of America, JPMorgan Chase, Citigroup, U.S. Bank, Wells Fargo, and PNC) were affected.

These cases demonstrate the potential for organizational systems to be crippled by inside threats—either ones with malicious intent or through unintentional employee actions. Barnes & Noble is considering the possibility that an employee may have unsuspectingly installed the malware sent to a store via a malicious link.[5] Luggage maker Tumi (which did disclose cyber breaches in its financial statements) has acknowledged asset theft by store employees who gave refunds to coconspirators who had not made actual product purchases.[6]

The denial of service attacks that overwhelmed the half dozen American banks may not have permanently affected customers' accounts but did these actions damage the banks' reputations or otherwise affect the banking industry? Would an attack on an individual bank's website cause it to lose customers to competitors?

Implementing cyber risk management

Cyber attacks can occur at any company and without warning. Delving into the details of the attacks, it is evident that the risk factors are more than just technical malfunctions or actions precipitated by outside parties. Cyber risk defenses need to address more than just technology

and system firewalls. Executive management and boards of directors need to think through the full range of cyber exposures and examine all contributing sources of cyber risk in designing what must be an integral component of an organization's enterprise risk management process.

James Lam, the first formal Chief Risk Officer in the United States, advises in his foundational book, *Enterprise Risk Management*, that "over the longer term, the only alternative to risk management is crisis management—and crisis management is much more expensive, time consuming, and embarrassing."[7] Companies waiting to see what happens to others and then adjusting their strategies accordingly may be too little, too late. Corporate cyber risk loss data is still sparse; some companies have not disclosed known breaches, some breaches do not require disclosure (for example, stolen data that is encrypted), and other breaches remain unidentified.

As companies wake up to the threat of cyber risk, their good intentions may be hampered by not knowing where to start. Milliman's Risk Advisory Services can assist companies in identifying their exposure, completing risk assessments, and implementing action plans to manage and mitigate risk. Milliman risk consultants bring both expertise in cyber risk management and an ability to integrate its treatment within an overall enterprise risk management program. "We help companies get started and maintain their momentum by first developing a road map of activities to manage, mitigate, and communicate on cyber risks," explains Joanna David of Milliman's Risk Advisory Services group. "We will work with multidisciplinary executive management from IT, Finance, HR, Legal, and the major business functions to examine the company's cyber risk across the entire enterprise. This addresses not only post-event mitigation strategies but proactive mitigation through internal process and control improvements as well."

Mark Stephens, director of Milliman's Risk Advisory Services and the executive director of the Milliman Risk Institute, emphasizes that cyber risks are not isolated, stand-alone risks but are intertwined with corporate financial, operational, strategic, and reputational risk. "The biggest difficulty with cyber risk is gaining a comprehensive understanding of the true exposures and how a cyber incident would resonate throughout the organization."

As part of its enterprise risk management (ERM) assessment process, the Risk Advisory Services team commonly works with companies in facilitating workshops to identify, prioritize, and quantify major threats and vulnerabilities. While the industry database on historical cyber losses is minimal, a structured examination of known, publicized cyber attacks, and a careful examination of the company's exposure through the eyes of key managers, can serve to identify the potential cyber risks. Frequent assessment, prioritization, and quantification of cyber risk is an essential component of a cyber risk management program.

"The evaluation often brings to light differing views of the organization's cyber risks among managers," notes Joanna. "The management group weighs in on the priority levels—via a group consensus, anonymous voting, or one-on-one interviews based on company culture and the organization's goals." The anonymous responses allow the participants to openly share their concerns and raise the group's awareness of their colleagues' associated activities and business processes that are related to cyber risk.

An organization's unique cyber and risk management characteristics are discussed during the workshop. Participants are guided through an identification of individual losses and planning possible cyber risk scenarios. How likely are the losses from a particular cyber risk over the course of a year? Five years? Ten years? What will the dollar impact be across the business? What are the most likely, optimistic, and pessimistic event descriptions, risk drivers, and risk scenarios? What are and what should be the potential mitigation strategies for the top risks?

After looking at company cyber risks, the company's mitigation plans are examined. How prepared is management for these scenarios? What is the optimal scope and maturity level for cyber risk management? Which resources and technology are currently available or need improvement? How can we assess the cost and benefit analysis of mitigation strategies?

How should the cyber risk management program be implemented? How can cyber risk management be integrated into the business units including internal budgeting processes and strategic decision making? Who should be involved in the day-to-day operations of ERM? Which cultural and change management issues need to be addressed? And finally—how do we measure success? Which metrics and assessment criteria should we use to both qualitatively and quantitatively address key risks?

By the end of the half- or full-day workshop Milliman has worked with the client to assess all aspects of managing cyber risk—from identification to assessment of internal processes through to mitigation and budgeting. Not only can Milliman develop a custom implementation plan for cyber risk management, but it also helps to ensure that the required risk management processes and controls are embedded throughout the organization and in its culture. Milliman can also assist in developing company communication and policy documents for the cyber risk management program.

Milliman ERM services

Mark Stephens, CCSA, manages the Milliman Enterprise Risk Management Services practice group. The practice delivers a portfolio of risk consulting services, such as enterprise risk design, test, and build projects, operational risk assessments, ERM education and training, and ERM technology evaluation. The ERM practice uses diagnostic consulting strategies to understand an organization's enterprise risk goals and challenges and then customizes solutions to deliver required business results.

In addition, Mark is the executive director of the Milliman Risk Institute, which supports ERM research and development. The Milliman Risk Institute Advisory Board meets on a semiannual basis, conducts corporate surveys, and publishes the results along with expert commentary. Mark can be reached at 312.499.5765.

Joanna David, MBA, CPCU, ARM, is a senior enterprise risk management consultant. Her primary responsibilities include delivering customized results-focused enterprise risk solutions and integrating these results into performance management, stakeholder management, and operational excellence for clients. She is the also the assistant director of the Milliman Risk Institute and can be reached at 312.499.5649.

[1] U.S. Securities and Exchange Commission (October 13, 2011). CF Disclosure Guidance: Topic No. 2: Cybersecurity. Retrieved December 12, 2012, from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] Menn, J. (February 2, 2012). Major companies keeping cyber attacks secret from SEC, investors: Report. Insurance Journal. Retrieved December 12, 2012, from http://www.insurancejournal.com/news/national/2012/02/02/233863.htm.

[3] Perlroth, N. (October 23, 2012). In cyberattack on Saudi firm, U.S. sees Iran firing back. New York Times. Retrieved December 12, 2012, from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[4] Schmidt, M. & Perlroth, N. (October 23, 2012). Credit card data breach at Barnes & Noble stores, New York Times. Retrieved December 12, 2012, from http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html.

[5] Schmidt & Perlroth, New York Times, ibid.

[6] Menn, Insurance Journal, ibid.

[7] Lam, James (2003). Enterprise Risk Management From Incentive to Controls, p. 3, John Wiley & Sons, Inc.

Elizabeth Bart is a consulting actuary in Milliman's Chicago office. Contact her at elizabeth.bart@milliman.com.