Article from

Risk Management

April 2017
Issue 38

The Complications of Cyber Risk Quantification

By Juliette Fairley

Editor's Note: This article originally appeared on www.garp.com. It is reprinted here with permission.

There are measures of the economic toll of cybercrime. A recent report from insurer Allianz said the total annual cost is $445 billion, the majority concentrated in the 10 biggest economies led by theU.S. ($108 billion), China ($60 billion) and Germany ($59 billion). Allianz quoted the Ponemon Institute statistic that data breaches cost companies an average $3.8 million in 2015, compared with $3.5 million the year before.

However, for corporate managements and their boards, cyber threats and their costs are a continuously evolving, moving target and a source of uncertainty. While the need for robust security is self-evident and attracting significant investment dollars, demand is building for insurance products that can provide an important risk management backstop.

According to Allianz, the cyber insurance market is in its third major phase of development, representing an estimated $2 billion in premiums that are growing at a double-digit annual rate, but it is very much a work in progress.

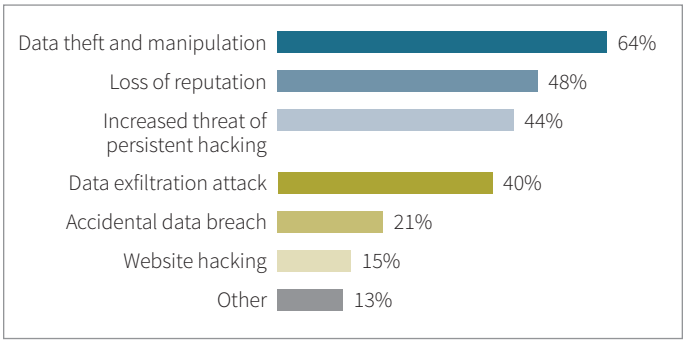
"The stand-alone cyber insurance market will continue to evolve, but development will bring challenges, with many concepts and wordings yet to be tested, potentially resulting in litigation," Allianz said in A Guide to Cyber Risk: Managing the Impact of Increasing Connectivity. "This is not unusual with new products and can improve risk knowledge."

COST ANALYSIS AND DATA SCIENCE

Enterprises are grappling with the difficulty of calculating their cyber risk exposure as a prerequisite for setting risk mitigation strategies and understanding how insurance fits in.

"The question is, is it really possible to put a dollar sign on fast-changing cyber risks with data that is difficult to find and often even harder to interpret?" Oliver Wyman consultants Leslie Chacko, Claus Herbolzheimer and Evan Sekeris wrote in the October 2016 Harvard Business Review.

Figure 1
Which Cyber Risks do Companies Fear the Most?



Source: *Allianz Risk Barometer 2015.* Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

Quantification is "challenging, but feasible," they said. It requires going beyond the conventional operational-risk approach that focuses narrowly on revenue losses, and evaluating instead "a broader set of losses associated with cyber attacks…The direct revenue losses for the companies involved in a cyber attack can be nearly negligible compared to the reputational damage incurred, which in turn can lead to future revenue losses. That is why it is essential for managers to quantify cyber risks more broadly."

The insurance industry is taking notice of Cyence, a San Mateo, California-based company that has developed, drawing on advances in data science, a platform for the economic modeling of cyber risk. Founder and CEO Arvind Parthasarathi has noted that a majority of cyber-loss incidents are the result of human actions, which, whether purposeful or accidental, are not per se technological.

Therefore, comprehensive cyber risk modeling must take technical, economic and behavioral factors into account.

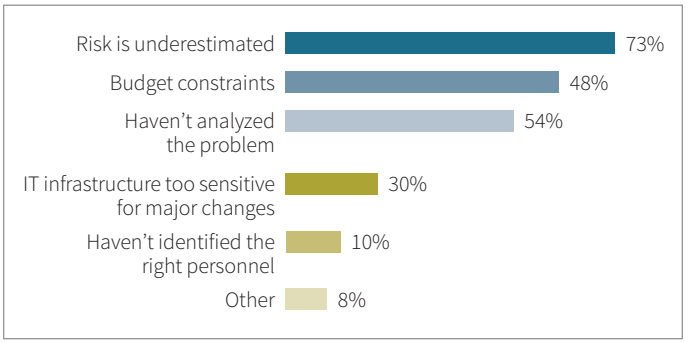
"To economically model cyber risk requires bridging the disjointed disciplines of cybersecurity and insurance/risk modeling," Parthasarathi said in October when announcing members of an advisory board of insurance and cybersecurity experts. "Barely a month out of stealth mode, our economic cyber risk modeling platform is leveraged by a who's who of the insurance industry as a competitive advantage. I look forward to working with our advisory board on continuing to be the economic risk model for cyber robust enough for insurers to deploy capital against."

Parthasarathi's who's who includes Richard Booth, former vice chairman of reinsurer Guy Carpenter; Tom Hutton, managing partner of XL Group's XL Innovate venture capital fund; and Sean Kanuck, who served as the first U.S. National Intelligence Officer for Cyber Issues, from 2011 to 2016.

INTERCONNECTIONS AND SUPPLY CHAINS

"Failure to keep pace with technological advancements will leave an organization at a terrible disadvantage," said Julie Pemberton, president of RIMS, the Risk Management Society, which in October released results of its annual Cyber Survey. "Embracing technology has enabled organizations to strengthen their performance, but, at the same time, has created many new exposures that risk management must address."

Figure 2
What is Preventing Companies Being Better Prepared Against Cyber Risks?



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

Among those emerging exposures, highlighted in the Allianz report, are the Internet of Things—web-connected devices that heretofore have been largely insecure and could number more than a trillion by 2020—as well as heavier reliance on cloud computing and third-party risks stemming from vendors and supply-chain relationships. All have the element of interconnectivity that complicates risk assessment and management.

"Businesses are driven by real-time data," Allianz said. "Any interruption of the process chain—even for a minute—could cause a severe business interruption, impacting the balance sheet."

"With increasing interconnectivity, globalization, and the commercialization of cybercrime, there has been an explosion in both frequency and severity of cyber attacks," said Chris Fischer Hirs, CEO of Allianz Global Corporate & Specialty (AGCS).

The RIMS 2016 survey, conducted in August and September with 272 respondents, found that 80% of organizations had stand-alone cyber insurance policies, up from 51% in 2015. One-fourth were spending more than $500,000 on premiums. Those purchasing cyber insurance as a result of contractual obligations increased to 25% from 8%.

Each company that has a role in the supply chain is trying to protect its status in that supply chain, according to Emily Cummins, a RIMS board member and managing director of tax and risk management for the National Rifle Association. "It's the likelihood of contractual requirements in the chain that is increasing, because no company is self-reliant," she says.

E&O PROTECTION

Technology vendors would do well to carry errors and omissions (E&O) in addition to cyber risk coverage, says Emy Donavan, head of cyber business for AGCS in North America.

"When an organization relies on a vendor for their network, and that network goes down, the vendor is probably not covering their client's consequential business-income loss under a cyber policy," Donavan tells GARP Risk Intelligence. "With a tech E&O policy, there can be coverage for a vendor's liability resulting from a client's losses."

With the increasing popularity of cloud services for data storage, 69% in the RIMS survey said they have obtained coverage for it.

"It's one of the most sensitive areas in the insurance application process, because the fact that different insurance policyholder might be sharing some of the same cloud providers is an aggregation of risk for the insurance company," Cummins points out.

INCREASING REGULATION

Companies also must cope with a "shifting regulatory landscape," as Allianz put it, notably data protection and breach-disclosure requirements that can increase both compliance and remediation expenses.

"In Europe, we can expect tougher rules on a country-by-country basis," Nigel Pearson, global head of fidelity, AGCS, said in the Allianz report. "Politically, it is difficult to be seen to be soft on data breaches. We will see more notifications and significant fines for data breaches in future."

In the RIMS survey, 48% said cyber breach reporting should be mandated by government, and 27% disagreed.

In the U.S., where insurance is regulated on the state level and a number of states have enacted breach reporting requirements, a federal mandate is seen as unlikely. Allianz's Donavan sees a "standard of care" evolving along the lines of the National Institute of Standards and Technology cybersecurity framework, to which directors and officers of companies can be held accountable.

DOCUMENTATION AND EDUCATION

"A risk manager or risk professional can help control the steady rise in insurance premiums by providing very good documentation during the insurance application process," Cummins says.

"Detail about risk controls in an application's cyber security risk assessment section can help lower the cost of premiums."

Such details may include documentation of employee security training, encryption and authentication, intrusion prevention and detection, vendor risk assessment, security by design, and compliance with the PCI (Payment Card Industry) standard.

Because "most reportable data breaches are triggered by unintentional employee error," Cummins says, "emphasizing year-round employee security training sends a strong message that an organization is a good insurance risk because they're doing the best they can to prevent a reportable event."

She underscores year-round employee education and training "because they need constant reinforcement of lessons" – phishing attacks being a continuing concern.

"In some of the companies with which I've been involved, one of the biggest problems is employees inadvertently opening an infected email or document because cyber hackers have gotten so good at disguising who and what they are," says Christine Todd Whitman, the former New Jersey governor who is chairperson of the American Security Project, a nonpartisan educational organization focused on national security. "These communications often look like they're coming from the personnel or CEO's office."

"If the government were to introduce a cyber hygiene public awareness campaign, it would help consumers understand a server's function, how a hacker gets in, and what a phishing attack looks like," Donavan says.

As a response to policymakers' viewing insurance as a component of national cyber resilience, Donavan is working with the U.S. Department of Homeland Security and the American Insurance Association on a glossary of insurance terms relating to cyber insurance coverage.

"In the U.S. and Europe, governments have been encouraging companies to build their resilience to a cyber attack, promoting cybersecurity standards and greater levels of cooperation, including sharing data," the Allianz report noted.

Pearson added, "Interest in protecting critical infrastructure is likely to see governments becoming increasingly involved in cybersecurity, with much greater levels of scrutiny and liability." ■

GARP editor-in-chief Jeffrey Kutler contributed to this article.