Article from

Risk Management

December 2016
Issue 37

Cyber Risk is Opportunity

By Michael Solomon

Cybersecurity is what keeps our clients awake at night. Recent high-profile breaches have made it a boardroom concern. Whether as an endorsement to an existing policy or standalone, companies will look to their existing general liability provider for coverage and will not look kindly on those that refuse. Whether reading industry headlines or meeting with clients, cybersecurity is a key risk discussed. Actuaries must collaborate with other insurance industry experts to develop innovative, sustainable solutions for key stakeholders. This is how our internal and external clients will judge our value added.

This essay highlights the most important aspects of an actuary's role in pricing cyber insurance.

Part 1 outlines the key risks of cybersecurity, why organizations are looking to insure, why an insurance company will be required to write this business even with valid concerns, and available techniques for companies to manage risk.

Part 2 outlines the value actuaries are positioned to add.

Part 3 concludes that the growing need for this coverage represents opportunity for actuaries.

PART 1: RISK

Direct losses resulting from profit-motivated cybercrimes, such as ransoming data, are actually very low—approximately $2 billion to 3 billion per year—while direct and indirect costs of such crimes are very high. Defense costs for such crimes total approximately $19 billion per year, while indirect costs total an additional $40 billion per year. Costs of a breach can be in the billions (Table 1):

Many different costs are involved. Direct costs include the cost of ransomware, loss of data and lawsuits. Uninsured risk can lead to key people losing their jobs, and perhaps future cases will include boards being sued for negligence.

Table 1.
High-Profile Data Breaches and Their Associated Costs

Breach	Cause	Cost (Ground Up)	Cost (Insured)
Epsilon	Spear-phishing[2]	Up to $4 billion[3]	No coverage in place
Home Depot	Vendor cybersecurity failure and Microsoft Windows security failure	$ billions[4]	$100 million
Wendy's	Unknown	$ billions[5]	Unknown
Veterans Administration	Computer/ external hard Drive incidentally stolen from employees house during burglary[6]	$500 million[7]	No coverage in place
Target	Vendor cybersecurity failure	$252 million[8]	$90 million
Hannaford Bros	Malware	$252 million[9]; ID theft insurance and replacement card costs held compensable[10]	No coverage in place
Sony PlayStation	Unknown	$171 million[11]	Unknown; settlement when appeal pending after bench granted summary judgment against Sony[12]
TJ Maxx	Poorly secured wireless LAN in two stores[13]	$256 million[14]	$19 million[15]
Sony Pictures Entertainment	North Korea	$151 million + reputation	$151 million
Heartland Payment Systems	SQL injection attack[16]	$140 million[17]	$30 million[18]
Anthem	Bogus domain name/ phishing	Over $100 million[19]	$100 million[20]

IT vulnerabilities that have led to this state of affairs have shown almost no signs of improvement over time. Many organizations are "living below the security poverty line." Cybersecurity budgets for many midsize and small companies are minimal. As a result, those companies often have little or no IT expertise, are unable to follow through on IT consultant recommendations and accordingly focus only on "putting out fires" rather than managing long-term cyber risk issues.[21] Currently, there's a general lack of objective proof that particular controls—policies, processes, technologies, and otherwise—have measurable and positive risk management impacts.[22] Singapore is among the most technologically advanced countries in the world, yet its government's cybersecurity solution is eliminating employees' internet access.[23]

Limited technology solutions exist for addressing cyber risks. Most vendor options fall short of needed protection, and they don't seem to be improving. Technical controls are often too complicated and/or costly for businesses to implement. The lack of available information about which cyber risks are most likely to materialize compounds these problems. Without more security intelligence, most organizations cannot make informed decisions about where to best spend their limited cybersecurity budgets. Given this landscape, some companies may be inclined to buy cybersecurity insurance rather than spend money on technology solutions and other cybersecurity controls. They may opt to transfer risk entirely rather than invest in expensive and largely unproven cyber risk mitigation efforts. Without minimum underwriting requirements by carriers, this phenomenon could give rise to a moral hazard situation that encourages companies to take further risks rather than improve their cyber risk cultures.

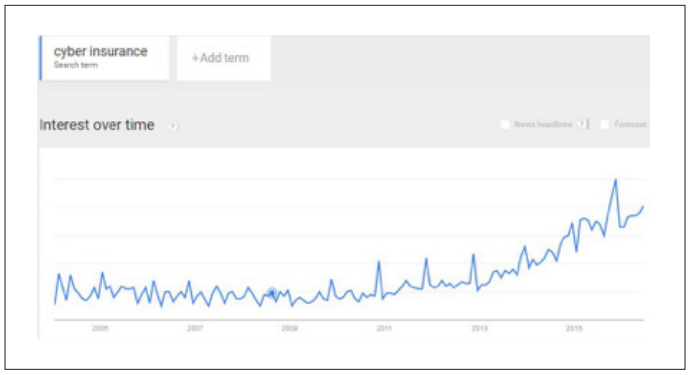
There are companies offering cybersecurity endorsements for their general liability insureds without a full understanding of expected cost or coverage, instead relying on low policy limits. Would insureds not expect guidance on appropriate limits? When a loss occurs and the limits leave the insured with a large residual loss, will they keep any business with this company? Low loss limits are no substitute for actuarial diligence. Indeed, I argue below for generous limits.

PART 2: ADDING VALUE

There are two reasons insurers are offering coverage for cyber risk. First, general liability is a large, profitable business for many insurers. Insureds will test the markets if their current carrier cannot provide necessary coverages.

Second, cyber risk is a growing line of business, with potential to generate future revenue increases. Despite a recent appellate ruling that general liability policies can cover defense costs arising from cyber breach,[24] interest in cyber insurance continues to rise, as shown in Figure 1.[25]

Figure 1
Google Trends



Source: Google Trends, "cyber insurance," *https://www.google.com/trends/explore#q=cyber%20insurance.*

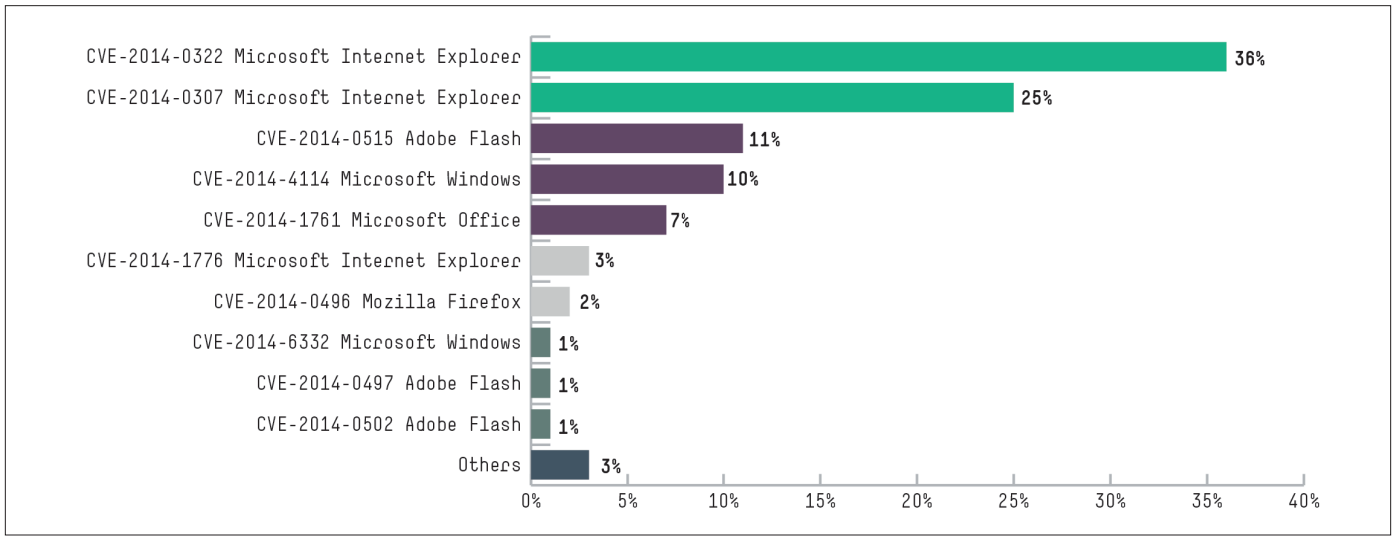
Many of the risks that arise in cyberspace are not new (e.g., intellectual property theft, lost profits, privacy and reputational damages), and other professions are looking to actuaries to take the lead. Regarding a cyber incident data repository, a broker, two underwriters and a reinsurer suggested that actuaries are uniquely qualified to process this data to develop new, and enhance existing, cybersecurity insurance products.

It is precisely this absence of data where actuaries can demonstrate their value. We can itemize data items that should be collected for a meaningful analysis, comb through available data for frequency and severity benchmarks, determine what data are credible and appropriately weight differing indications. Furthermore, technologists are at a loss as to what protections work best. For example, how beneficial is encryption? What level should be adopted? Actuaries are uniquely skilled in finding answers to such questions in the data. By synthesizing available data, actuaries can guide insurers' efforts to work with insureds to reduce losses and increase profitability.

Cybersecurity policies generally consist of multiple subcoverages (e.g., Beazley's Breach Response has eight[26]). Actuaries can determine the relative exposure from each of these subcoverages and tailor the policy specifications to the insured's concern.

One major issue in cyber insurance is what level of cybersecurity carriers should demand from the insured. If these levels are made too onerous, the marketability of the product will suffer. However, standards that are too lax will encourage insureds to skimp on expensive cyber protection solutions. Some have expressed the opinion that demanding the latest software patch updates from all employees is unreasonably onerous. In my opinion, it is not (Figure 2). The insured is in a position to ensure all employees are on a given patch at a given point in time through centralized updates. Insureds are also in a position

Figure 2
Top Discovered CVE-2014 Examples



Source: HPE Security Research Cyber Risk Report 2015. Hewlett Packard Enterprise Development LP.

to require administrator rights for all downloads, encryption for external drives, natural language processing and so on. Many companies demand their employees take sexual harassment awareness training annually, to avoid lawsuits and the loss of key personnel. Insurers are justified in mandating annual cybersecurity training.

There are many causes of loss, and a data breach may be caused by several. While not all of these causes can be controlled by insureds, Verizon's 2013 Data Breach Investigations Report found that 90 percent of cyberattacks over the previous year were preventable with simple or intermediate systems in place. There's clearly room for improvement in most organizations when it comes to cyber risk management.[27] Insurance should not cover those breaches in the insured's control; it exists to cover those things outside the insured's control. Carriers should motivate insureds to do what they can, through both compulsory precautions, and policy terms, as discussed herein.

Frequency and severity of events are the "holy grail" of cybersecurity risk management. While companies can analyze the frequency of cyber incidents based on some available data, estimating severity is more difficult. Different industries are held to different standards. For example, the medical industry has higher cyber claims frequency because of the rigorous information security and privacy standards of the Health Insurance Portability and Accountability Act (HIPAA). Insurers assess insureds on geography and sector. Judgment is used to identify which companies are most likely to be attacked.

Frequency is short tailed and companies generally find out quickly if they have been breached. This has two implications: First, it makes it easier to price, and therefore a more insurable risk. Second, it is rare more than one policy will be triggered with one event, and those rare events, generally related to cloud providers, can be specifically excluded from contracts. Some have suggested a federal backstop, like the Terrorism Risk Insurance Act, would be required to cover such events.

Insurers should not cover frequency risk. This burden should be placed on the insured. Insurance companies add value to companies by assuming volatile risk so management can concentrate capital in other areas. The company itself is best-placed to manage predictable losses through cash-flow management, perhaps through a single-parent captive. High per-occurrence deductibles keep frequency risk with the insured and transfer only the volatile severity risk to the carrier. Following this logic, high aggregate deductibles would not be required. I suggest a per-occurrence limit across the policy.

High per-occurrence deductibles prevents insurance from being seen as a replacement for proper cybersecurity. As mentioned above, some argue cyber insurance is currently cheaper than cybersecurity, and therefore moral and morale risk is the biggest impediment to insurance companies wishing to expand in this area. To be sustainable in the long term, insurers must make their policies unattractive to companies that choose insurance as a replacement for investing in cyber risk management.

The carrier will normally be more able to assume the risk of high-severity losses than the insured. Carriers can spread the risk among many policies, so they are more able to absorb low frequency events. To maximize value, carriers should therefore offer high policy limits. Low policy limits are used to keep

premiums down when the insured is willing to risk high-severity losses, implicitly choosing to use their resources and capital to protect against other risks. Inadequate limits can lead to bankruptcy in the most severe cases. My experience is that insureds are not willing to accept the risk of high-severity losses from cybersecurity where the risks are not fully known. Carriers are in a much better place to accept this risk through the normal insurance risk-pooling mechanisms.

Another reason for policy limits is to keep the insured's skin in the game. As outlined above, severity risk is significantly higher than frequency risk, so per-occurrence deductibles will be much more effective. Insureds are more able to retain the risk from high deductibles than low limits.

PART 3: CYBER RISK IS OPPORTUNITY

I conclude that insurance companies can expand cybersecurity insurance offerings as follows:

Policies must contain austere per-occurrence deductibles and rigorous demands on insureds' cybersecurity protection. This will keep premiums affordable while encouraging insureds to mitigate their risks.

- Limits should be generous on both per-occurrence and aggregate bases, since carriers are more able to assume the risk of high-severity losses than insureds, and there is limited opportunity for insureds to minimize these low-frequency events.
- Coverages should be flexible to address insureds' particular concerns.

While cyber risk is associated with some stunning losses, a lack of data and lack of consensus in the technology world as to how to treat it, this is precisely why actuaries' specific skill set and experience can add value. As I write, the largest insurance companies are expanding their cyber liability teams,[28] recognizing this coverage's tremendous potential. Those who can solve the puzzles of cyber coverage and address their clients' problems will be rewarded. Opportunity knocks! ■

ENDNOTES

1 *Cybersecurity Insurance Workshop Readout Report,* National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, DC, November 2012.

2 Jaikumar Vijayan, "Epsilon a Victim of Spear-phishing Attack, Says Report," *Computerworld,* April 7, 2011, http://www.computerworld.com/article/2507075/security0/epsilon-a-victim-of-spear-phishing-attack--says- report.html. Retrieved June 8, 2016.

3 Lori Widmer, "The 10 Most Expensive Data Breaches," *Life Health Pro*, June 18, 2015, http://www.lifehealthpro.com/2015/06/18/the-10-most-expensive-data-breaches?t=practice- management&slreturn=1465402403&page=5. Retrieved June 8, 2016.

4 Greg Masters, "Home Depot Breach Costs Expected to Reach Billions," *SC Media*, October 2, 2015, http://www.scmagazine.com/home-depot-breach-costs-expected-to-reach-billions/article/442849/. Retrieved June 8, 2016.

5 "Credit Unions Feeling Pinch in Wendy's Breach," *Krebs on Security*, March 2, 2016, http://krebsonsecurity.com/2016/03/credit-unions-feeling-pinch-in-wendys-breach/. Retrieved June 8, 2016.

6 "Veterans Affairs Data Theft," *Electronic Privacy Information Center,* n.d., https://epic.org/privacy/vatheft/. Retrieved June 8, 2016.

7 *Supra* note 4.

8 Michael Kassner, "Data Breaches may Cost Less Than the Security to Prevent Them," *Tech Republic,* April 9, 2015, http://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/. Retrieved June 8, 2016.

9 Widmer, "10 Most Expensive."

10 Decision and Order on Plaintiffs' Revised and Supplemented Motion for Class Certification, U.S. District Court, District of Maine (Portland), Civil Docket No.: 2:08-MD-1954-DBH, http://www.med.uscourts.gov/Opinions/Hornby/MDL/MDL1954_2013_03_20_ORDER11.pdf. Retrieved June 8, 2016.

11 *Supra* note 3.

12 Young Ha, "Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York ," *Insurance Journal*, May 1, 2015, http://www.insurancejournal.com/news/east/2015/05/01/366600.htm. Retrieved June 8, 2016.

13 Jaikumar Vijayan, "One Year Later: Five Takeaways from the TJX Breach," *Computerworld*, January 7, 2008, http://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later--five-takeaways-from-the-tjx-breach.html. Retrieved June 8, 2016.

14 Ross Kerber, "Cost of Data Breach at TJX Soars to 256m," *Boston Globe*, August 15, 2007, http://archive.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/. Retrieved June 8, 2016.

15 "Insurance Company Reimburses TJX Almost $19 Million for Data Breach," *Fierce Retail*, February 22, 2008, http://www.fierceretail.com/story/insurance-company-reimburses-tjx-almost-19-million-for-data-breach. Retrieved June 8, 2016.

16 Jeremy Kirk, "Miami Man Indicted for Massive Credit Hack," *CSO Online*, August 18, 2008, http://www.csoonline.com/article/2124294/malware-cybercrime/miami-man-indicted-for-massive-credit- hack.html. Retrieved June 8, 2016.

17 *Supra* note 8.

18 Jaikumar Vijayan, "Heartland Breach Expenses Pegged at $140M—so Far," *Computerworld*, May 10, 2010, *http://www.computerworld.com/article/2518328/cybercrime-hacking/heartland-breach-expenses-pegged-at-- 140m----so-far.html.* Retrieved June 8, 2016.

19 Kassner, "Data Breaches.".

20 Mary A. Chaput, "Calculating the Colossal Cost of a Data Breach," *CFO*, March 24, 2015, http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/. Retrieved June 8, 2016.

21 *Cyber Risk Culture Roundtable Readout Report*, National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, DC, May 2013.

22 *Supra* note 21.

23 "No Internet for Singapore Public Servants," *BBC News*, June 8, 2016, http://www.bbc.com/news/world-asia-36476422. Retrieved June 8, 2016.

24 John P. Mello Jr., "Insurance Industry Buzzes Over Data Breach Ruling," *Tech News World*, April 21, 2016, http://www.technewsworld.com/story/83403.html. Retrieved June 14, 2016.

25 Google Trends, "cyber insurance," https://www.google.com/trends/explore#q=cyber%20insurance. Retrieved June 9, 2016.

26 https://www.beazley.com/london_market/specialty_lines/professional_liability/technology_media_and_business_services/beazley_breach_response/understanding_the_coverage.html. Retrieved June 14, 2016. Original data source: Breaches handled by Beazley Breach Response Services in 2014.

27 *Cyber Risk Culture Roundtable Readout Report*, National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, DC, May 2013.

28 Joyce Famakinwa, "Allianz Expands Cyber Insurance Team," *Business Insurance*, June 7, 2016, http://www.businessinsurance.com/article/20160607/NEWS06/160609839?tags=58|285|93|137|98|83|76|71|70#utm_medium=email&utm_source=-bi-breakingnews&utm_campaign=bi-breakingnews-20160607. Retrieved June 9, 2016 (subscription required).

Michael Solomon, FCAS, CERA, MAAA, is a consulting actuary at The Actuarial Advantage, Inc. He can be reached at *MichaelSolomon613@gmail.com.*