Joint Risk Management Section
Canadian Institute of Actuaries
Casualty Actuarial Society
Society of Actuaries

Cybersecurity: Impact on Insurance Business and Operations

Canadian Institute of Actuaries / Institut canadien des actuaires

SOCIETY OF ACTUARIES

Preamble

The Joint Risk Management Section of the Society of Actuaries (SOA), the Casualty Actuarial Society (CAS) and the Canadian Institute of Actuaries (CIA) is pleased to release our sixth collection of essays, this time addressing the intersection of cybersecurity and insurance in “Cybersecurity: Impact on Insurance Business and Operations.”

This collection contains topical essays that express the opinions and thoughts of four leaders in cybersecurity. The thoughts and insights shared herein are the opinion of the authors and not necessarily those of the Society of Actuaries, the Casualty Actuarial Society, the Canadian Institute of Actuaries or corresponding employers of the essayists.

The editorial team awarded prizes to the following essays:

Prize Winners

First Prize

Cyber Risk is Opportunity
Michael Solomon

Second Prize

Cybersecurity and the Insurance Market
Laura Maxwell

Embedding Cyber Risk in Risk Management:
An Insurer’s Perspective
Kailan Shang

Determining the Likelihood of a Cybersecurity Failure for use in Cybersecurity Insurance Pricing
Steven Dionisi

Contents

This publication is provided for informational and educational purposes only. Neither the Society of Actuaries nor the respective authors’ employers make any endorsement, representation or guarantee with regard to any content, and disclaim any liability in connection with the use or misuse of any information provided herein. This publication should not be construed as professional or financial advice. Statements of fact and opinions expressed herein are those of the individual authors and are not necessarily those of the Society of Actuaries or the respective authors’ employers.

Introduction

Given that cyber risk is a major driver of operational risk and that businesses and individuals are looking to the insurance industry to provide coverage for the cyber risks they face, we asked authors to “share their thoughts and reflections on either how insurance companies should deal with cyber risk in an ERM context, or how insurance companies can respond to society’s call to action to expand cybersecurity insurance offerings.” We received several papers exploring a variety of ideas that spanned concepts such as Markov analysis and fuzzy logic.

In Cyber Risk is Opportunity Michael Solomon suggests that actuaries must collaborate with other insurance industry experts to develop innovative, sustainable solutions for key stakeholders. He goes on to “outline the key risks of cybersecurity, why organizations are looking to insure, why an insurance company will be required to write this business . . . and available techniques for companies to manage risk.” Solomon outlines characteristics of what a successful cyber coverage offering would look like and states that actuaries are uniquely positioned to add value given their skill set and experience. He ends by concluding that the growing need for this coverage represents opportunity for actuaries.

Laura Maxwell’s Cybersecurity and the Insurance Market explores ways to price cyber risk and some key data sources to consider. She suggests that “similar to the way insurers have led the way for loss control in traditional coverages, insurers must also lead the way in preventing and reducing the impact of cybercrime.”

Embedding Cyber Risk in Risk Management: An Insurer’s Perspective, by Kailan Shang, argues that “cyber risk needs to be embedded into the existing risk management framework to facilitate consistent capital management, risk assessment and resource allocation.” Shang then explores how one might define the risk appetite for cyber risk and shows how fuzzy logic models can be used to evaluate cyber risk exposure. Shang concludes by stating that “proactive measures such as technology investment, training, risk monitoring and cyber insurance are important to control cyber risk exposure and keep pace with new development of cyber risk.”

Determining the Likelihood of a Cybersecurity Failure for use in Cybersecurity Insurance Pricing, by Steven Dionisi, demonstrates how cybersecurity can be modeled after life insurance products and specifically explores the “quantify the probability of failure to a cybersecurity system over a period of time or a number of attacks.”

We hope that this publication generates further thought and discussion. What are your takeaways?

We welcome further commentary, editorials and rebuttals to add to our continuing thought leadership on the topic.

Enjoy!

Best wishes,

Thomas Hartl, PhD, FCAS, MAAA—Bryant University
Kevin Olberding, FSA, CERA, MAAA—Unum
David Schraub, FSA, CERA, MAAA, AQ—Society of Actuaries

On behalf of the Joint Risk Management Section Council of the Society of Actuaries, Casualty Actuarial Society, Canadian Institute of Actuaries.

Cyber Risk is Opportunity

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.[1] Costs of a breach can be in the billions (Table 1).

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 employee's 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]

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.

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.

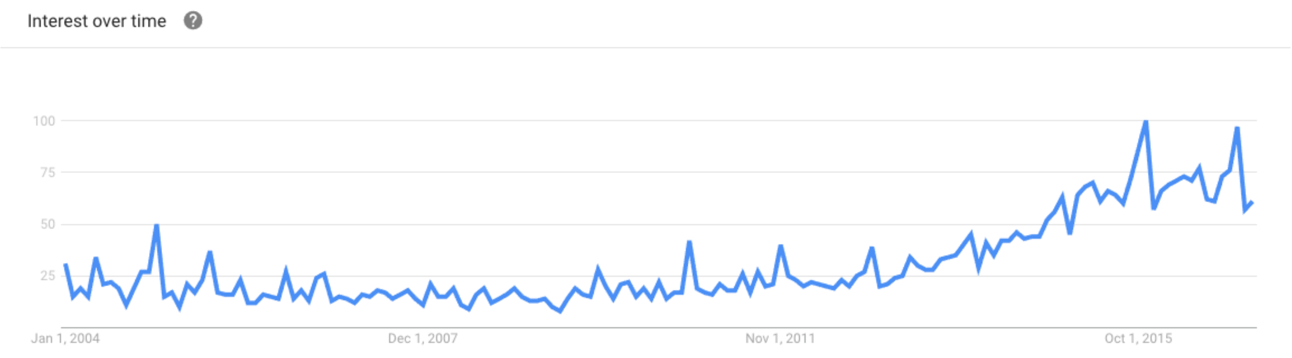
There are companies offering cybersecurity endorsements for their general liability insureds without a full understanding of expected cost or coverage, instead relying on low policy limits. Would insureds not expect guidance on appropriate limits? When a loss occurs and the limits leave the insured with 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.

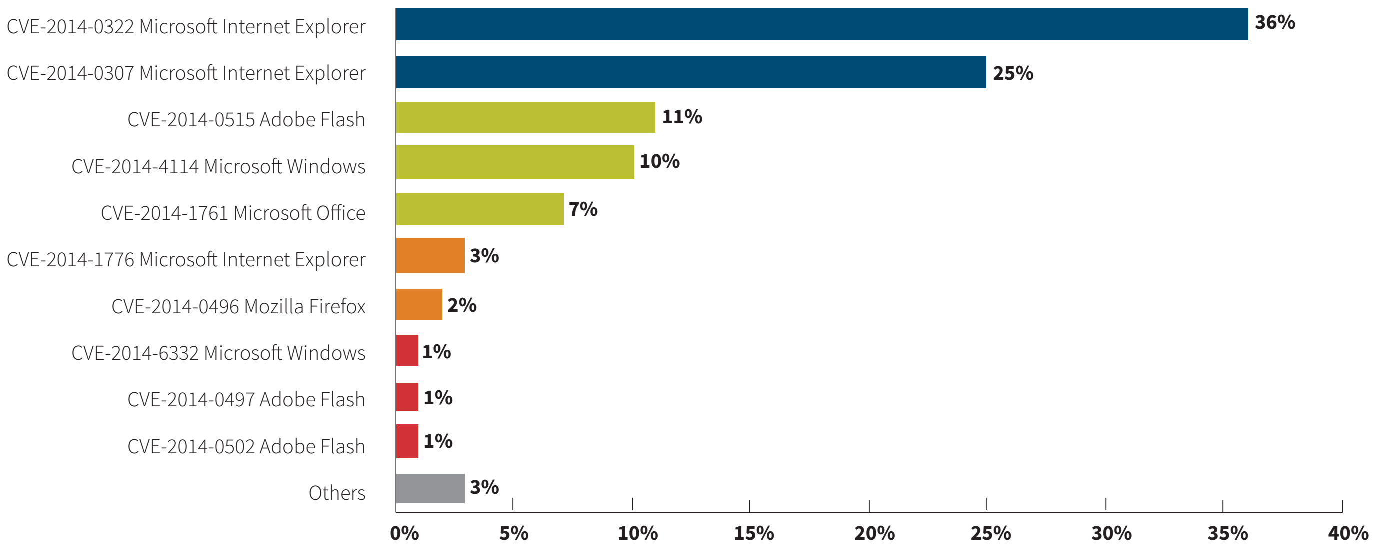
It is precisely this absence of data where actuaries can demonstrate their value. We can itemize data items that should be collected for a meaningful analysis, comb through available data for frequency and severity benchmarks, determine what data are credible and appropriately weight differing indications. 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 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

Figure 2: Top Discovered CVE-2014 Examples



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

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 prevent 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, 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!

[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] *Supra* note 8.

[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] Ibid.

[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] *Supra* note 21.

[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|7 0#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.

Cybersecurity and the Insurance Market

Laura A. Maxwell, FCAS, MAAA

The frequency and severity of cyberattacks are ever increasing. Data breaches to steal personal information occur daily, but only the largest make the news. One that that was deemed newsworthy was the data breach affecting 11 million people when hackers gained access to Premera Blue Cross's systems on May 5, 2014. The breach was not discovered until January 29, 2015.[1]

In addition to theft of personal information, cybercrime includes the theft of intellectual property. It is difficult to determine the cost of intellectual property theft, but it may have the most significant economic implications. Theft of intellectual property reduces competition and slows technological improvement.[2] Companies are slow to notice theft of intellectual property and unlikely to publicly acknowledge the theft. Hackers stole passwords from top Nortel executives, including the chief executive, and downloaded technical papers, research-and-development reports, business plans, employee emails and other documents for nearly 10 years.[3]

Ransomware, another form of cyberattack, is also increasing. With ransomware, malware locks the victim's computers and the victim must pay a ransom, generally in bitcoins, to regain control of its computers. Hollywood Presbyterian Hospital's computers were shut down by ransomware and administrators paid hackers approximately $17,000 to regain control of them.[4] In the first quarter of 2016, the FBI received reports of more than $209 million in losses from ransomware attacks.[5]

The *2015 Cost of Data Breach Study: Global Analysis Data Breaches* divides theft of personal information costs into three categories:

1. Direct Costs – the cost of the activity:
   - Notification
   - Credit monitoring
   - Legal services
   - Public relations
   - Business interruption
   - Regulatory fines and penalties

2. Indirect Costs – time and effort

3. Opportunity costs:
   - Customer turnover
   - Increased customer acquisition activities
   - Loss of reputation
   - Diminished goodwill[6]

According to an IBM-Ponemon study, the average cost paid for each lost or stolen personal information record increased from $145 in 2014 to $154 in 2015.[7] Cyber liability insurance products can help companies cover the costs of data breaches and ransomware.

The current cyber insurance market premium is $2.5 billion and is expected to grow substantially by 2020. Projections for 2020 are $5 billion (David Bradford, Advisen), $7.5 billion (PWC) and $10 billion (ABI).[8] This growth is evidenced by the number of recent rate, rule and form filings containing cyber coverages. A review of several rate filings (effective May 2016 or later) provides commercial cyber coverage for the direct data breach costs mentioned above. Some of the companies offer additional coverage for cyberattack costs, including extortion. Coverages do not appear to be available for theft of intellectual property.

Pricing varies, with some companies having a rate per $1,000 of gross sales and others a flat base rate. The premium calculations are fairly simple, with adjustments for limit, deductible, retroactive period coverage and type of risk. Two of the companies reviewed break down their hazard risks by website use:

- Low – provide only information on their website
- Medium – partially conduct business over their website and/or store credit card numbers
- High – conduct all business over their website and/or store highly sensitive information such as Social Security numbers[9, 10]

Other companies divide their risks into tier classes based on business type:

- Businesses where primary personal information is relative to employees only (manufacturing,

wholesaling)
- Businesses that keep financial or account number information on customers but not Social Security numbers (retail, churches)
- Businesses with Social Security numbers (apartments, health care, professional services)[11]
- Educational institutions
- Municipalities
- Hospitals and nursing homes[12]

All industries are affected by cyberattacks, but their frequency and severity vary. In 2015, health care, financial services, retail and education were the most frequently affected sectors, while the restaurant/hospitality industry experienced the highest levels of severity. Cybercriminals have moved from supermarkets and big box stores to restaurants, hotels and casinos.[13] Using industry type to classify risks is a good way to start pricing cyber risk, but insurers also need to consider a company's data volume, data value, number of endpoints to protect and vendors.[14]

Companies providing cyber coverage show little differentiation in pricing, which may be due to the lack of historical insurance data available to determine base rates and factors. One filing relied on publicly available data from the U.S. Government Accountability Office, Ponemon Group, Gartner and the Federal Trade Commission.[15] Insurance companies should look to external data to better price cyber risk. In addition to the sources listed above, data are available from the Identity Theft Resource Center, Department of Homeland Security, Center for Strategic and International Studies and United Nations Office on Drugs and Crime.

Although the commercial cyber liability market is growing, there is limited coverage available in the personal insurance market. Homeowners insurers are adding exclusions for liability arising out of social media and cyberbullying. Coverage is generally limited to identity theft coverage, which could be a result of cybercrime. One exception is Chubb, which recently announced cyberbullying coverage as part of its homeowner's Family Protection policy. It covers psychological counseling, lost salary and public relations.[16]

Insurance companies could also assist their policyholders with loss control. Insurers should be aware of who is responsible for data breaches and how those breaches occur in order to assist their policyholders. They also need to be educated on recent threats to proactively inform their policyholders. Insurers can evaluate the commercial policyholder's preparation for proper underwriting and pricing, and as part of loss control. As part of Chubb's individual risk-sensitive rating plan, it reviews the company's preventive measures and assesses the following:

- Firewalls and intrusion detection systems
- Passwords and authentication protocols
- Use of cryptography and encryption methodologies
- Maintenance of system logs
- Patch management program
- Planned elasticity of computing resources
- Mobile phone and mobile computing devices
- Written protocols when privileged access (administrator level) is granted
- Training program for employees and authorized users covering network security and privacy issues, including legal liabilities and threats such as social engineering (e.g., phishing), spam and dumpster diving
- Annual reports by IT security to senior management
- Incident response plan addressing data breaches, lost laptops or mobile devices
- Procedures for immediate revocation of all computer rights and retrieval of all computing equipment
- Daily backup
- Business continuity and disaster recovery plans that incorporate consideration of cyber threats

Companies that do not score well on these questions can be provided assistance to improve their defenses. A strong defense cannot eliminate all claims, but it may substantially reduce costs and time associated with a breach. The Catholic Charities of Santa Clara County was saved from ransomware by a device that scans the network for unusual behavior. The computer that was contacting a server in Ukraine was disconnected from the network before significant damage was done. Catching ransomware early can save a company money.[18]

Providing training to policyholders is another element of loss control. Human error is a significant cause of incidents. Phishing and hacking were responsible for 31 percent of cyber incidents in the BakerHostetler study. Underlying issues of phishing and hacking can often be attributed to human error. Other causes include employee mistakes (24 percent), external theft (17 percent), vendors (14 percent), internal theft (8 percent) and lost or improper disposal (6 percent).[19]

Following a cyberattack, an insurance company can provide assistance with forensic investigations. It is important for a company to quickly determine what data are at risk and to react swiftly. Consumers are well aware that breaches occur, and denying or underestimating their impact can seriously damage a company's reputation and retention.

Individuals may need home-security audits to verify their computer systems are safe. This is particularly important for individuals with investments and sensitive data on their home and mobile systems. Pure Insurance offers one-day audits and a monitoring service for home computer network intrusions. Pure started this program in response to individuals' cyber-related claims.[20]

Insurance coverage of cyber risks should continue to grow as cybercrime increases in frequency and severity. Similar to the way insurers have led the way for loss control in traditional coverages, insurers must also lead the way in preventing and reducing the impact of cybercrime.

[1] Associated Press, "Data Breach at Premera Blue Cross Could Affect 11 Million People," *SFGATE.com,* March 17, 2015, http://www.sfgate.com/business/article/Data-breach-at-Premera-Blue-Cross-could-affect-11-6139961.php.

[2] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, DC: Center for Strategic and International Studies, June 2014), 12, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[3] Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach," *Wall Street Journal,* February 14, 2012, http://www.wsj.com/articles/SB10001424052970203363504577187502201577054.

[4] Sean Sposito, "Locky Ransomware Lives up to its Name, Locking Files," *SFGATE.com*, February 19, 2016, http://www.sfgate.com/business/article/Locky-ransomware-lives-up-to-its-name-locking-6843516.php.

[5] Sean Sposito, "Santa Clara Charity Has a Narrow Escape from Ransomware," *San Francisco Chronicle*, April 29, 2016, http://www.sfchronicle.com/business/article/Santa-Clara-charity-has-a-narrow-escape-from-7384755.php.

[6] *2015 Cost of Data Breach Study: Global Analysis*, Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, May 2015, page 25.

[7] Caitlin Bronson, "The $2.5B Cyber Insurance Market Could be Nearly 4 Times Bigger by 2020," *IBAMAG.com*, May 5, 2016, http://www.ibamag.com/us/news/cyber/the-2-5-cyber-insurance-market-could-be-nearly-4-times-bigger-by-2020-31531.aspx.

[8] Ibid.

[9] Pennsylvania National Mutual Casualty Insurance Company, Countrywide Rules, SERFF Tracking # PNMC-130250857.

[10] Berkley National Insurance Company, Company Rules, SERFF Tracking # BNIC-130409966.

[11] American Fire and Casualty Company, Company Exceptions, SERFF Tracking # LBRC-130374617.

[12] The Cincinnati Casualty Company, Coverage Rules, SERFF Tracking # CNNA-130319569.

[13] Theodore J. Kobus, et al., *Is Your Organization Compromise Ready? 2016 Data Security Incident Response Report* (Atlanta, GA: BakerHostetler, 2016), 4, http://www.mass.gov/export/update2016/presentations/2016%20Data%20Security%20Incident%20Response%20Report.pdf.

[14] Ibid.

[15] The Cincinnati Insurance Companies Rate Filing Memorandum, SERFF Tracking # CNNA-130319569.

[16] "Chubb Adds Cyber Bullying Insurance for U.S. Homeowners," Insurance Journal, April 5, 2016, http://www.insurancejournal.com/news/national/2016/04/05/404202.htm.

[17] CUSTOMARQ IRSR Plan for Coverage "C" – Cyber Liability and Additional Coverages, SERFF Tracking # CHUB-130359516.

[18] Sposito, "Santa Clara Charity."

[19] Kobus, et al., *Is Your Organization Compromise Ready?* , 6.

[20] Priya Anand, "Do Individuals Need Cybersecurity Insurance?" *Wall Street Journal,* September 20, 2015, http://www.wsj.com/articles/do-individuals-need-cybersecurity-insurance-1442800951.

Laura A. Maxwell, FCAS, MAAA, is a consulting actuary at Pinnacle Actuarial Resources Inc. She can be reached at *LMaxwell@PinnacleActuaries.com.*

Embedding Cyber Risk in Risk Management: An Insurer's Perspective

By Kailan Shang FSA, CFA, PRM, SCJP

Cyber risk has become one of the top risks on risk managers' radar given its increasing incidence rate and impact. The 2014 emerging risk survey sponsored by the Joint Risk Management Section of the CAS, the CIA and the SOA named cybersecurity the top emerging risk chosen by 58 percent of survey responders.[1] Cyber risk includes the risk of damage to the hardware, software and security of the information system caused by people, system failures and process failures. It could cause financial losses, business disruption and reputation damage. The insurance industry has been adopting more new technologies that help information sharing with the clients and the public. Many companies are actively using social media to effectively communicate with clients and public audience. Insurers are requiring more personal information from clients such as telematics data for driving behavior analysis and health/fitness data. The embrace of the internet of things provides new opportunities but also leads to a higher exposure to more complicated cyber risk. Insurers may also offer cyber insurance that protects the insured from financial losses caused by cyber risk. These insurers are exposed to a wider range of cyber risk events. As a unique and quickly evolving type of risk, cyber risk needs to be embedded into the existing risk management framework to facilitate consistent capital management, risk assessment and resource allocation.

Appetite for Cyber Risk

According to Eling and Wirfs,[2] cyber risk is less severe than noncyber operational risk in terms of loss amount and volatility. Cyber risk is more contagious than noncyber operational risk. A single cyber risk event may affect multiple firms. Given the wider application of the internet of things, cyber risk's frequency and severity may grow significantly. For a specific insurer, insufficient investment in enhancing cyber security could also lead to much higher cyber risk exposure than the average level. Setting the risk appetite for cyber risk requires thorough assessment of the internet systems, potential losses due to data breach, internal control processes, staff knowledge of cyber risk, readiness of managing an incident and potential damage to reputation.

With a deep understanding of the potential losses, either financial or reputational, risk appetite for cyber risk can be set according to the company's willingness and ability to take cyber risk. Like other risk types, the risk appetite for cyber risk can be defined using quantitative measures such as capital at risk (CaR) and earnings at risk (EaR) or qualitative statements such as no material damage to the company's reputation and no interruption of the business caused by cyber risk are acceptable. An example of appetite for cyber risk could be:

- The company cannot lose more than 10 percent of International Financial Reporting Standards (IFRS) equity in a single cyber risk event or a series of related cyber risk events.
- The company has extremely high risk aversion to reputational risk caused by cyber security failures.
- The company has a contingency plan in place for continuing business operations in the event of an internet system failure or a cyberattack.

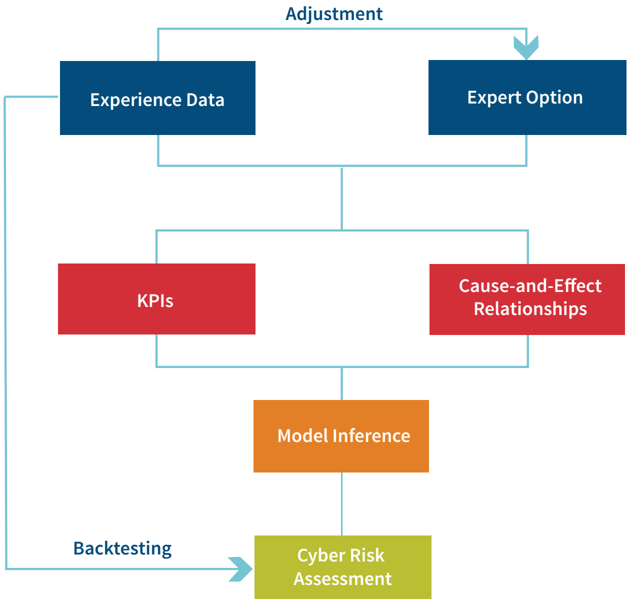
Here the 10 percent should be supported by quantitative analysis of cyber risk exposure. Setting the risk appetite for cyber risk in a quantitative way requires experience data, expert opinions and sophisticated modeling to incorporate the changing environment. The percentage can also be roughly estimated as the percentage for noncyber operational risk multiplied by the relative extremity of cyber risk compared to noncyber operational risk.

Hybrid Model

The uncertainty of cyber risk, the increasing use of the internet of things to share information and data privacy concerns often lead to insufficient experience data for measuring the exposure to cyber risk. Even with sufficient data, some impact of cyber risk, such as the damage to reputation, is difficult to quantify. A hybrid model is a model that uses both limited experience data and experts' input to evaluate cyber risk exposure. Given the significant amount of input from a variety of experts, the model also needs to be able to consistently incorporate subjective input and draw conclusions.

Hybrid models such as fuzzy logic models can be used to evaluate cyber risk exposure. Fuzzy logic models are built on fuzzy set theory and fuzzy logic. The models allow an object to belong to more than one exclusive set with different level of confidence. They are useful for analyzing risks with insufficient knowledge or imprecise data. Shang and Hossen (2013) studied the application of fuzzy logic models to risk assessment.[3] Available experience data can be used to help calibrate the quantitative part of the model, which describes the characteristics of key risk indicators (KRIs). Expert opinions on KRIs and their relationships to cyber risk exposures can be incorporated into fuzzy logic models as well. Consistent inference rules used in fuzzy logic models help reduce the adverse impact of human biases normally seen in qualitative risk assessment. Figure 1 shows the structure of a fuzzy logic model.

Figure 1: Fuzzy Logic Model Structure



Given that the knowledge and experience of cyber risk evolve quickly, fuzzy logic models make the assessment of cyber risk both flexible and consistent. Experts need to compile a list of key indicators of cyber risk considering the company's IT infrastructure, business and data. Table 1 illustrates some sample key risk indicators for several subcategories of cyber risk. Most of the indicators are not quantifiable and need to be rated to represent the degree of confidence that the current level is high, medium or low.

Table 1: Sample Key Risk Indicators for Cyber Security

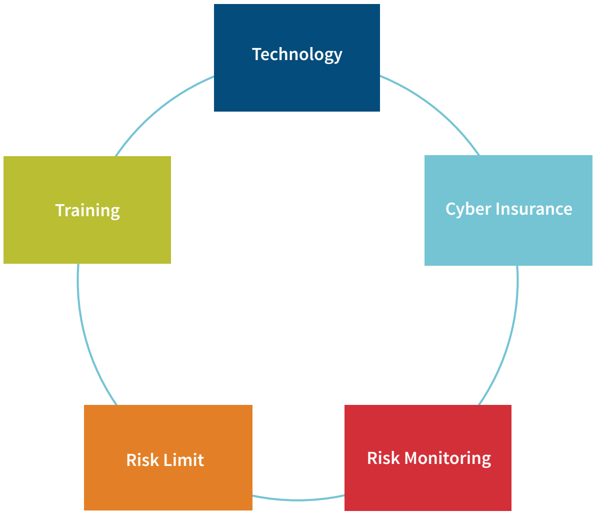
Category	Key Risk Indicator
Resource	Number of cyber security specialists
	Sufficiency of cyber security training
	Level of cyber security awareness
	Sufficiency of financial resources for cyber security framework
	Response time for cyber security management
Control	Sufficiency of cyber risk assessment (people, process and technology)
	Sufficiency of vulnerability checking of hardware, software, network, remote working, mobile devices, etc.
	Sufficiency of cyber risk assessment of IT service provider
	Degree of cyber risk control centralization
	Timeliness of security updates and checking
Risk Governance	Scope of cyber security policy
	Clarification of roles and responsibilities
	Sufficiency of internal audit and external review
	Senior management support
	Scenario analysis
Detection	Number of detected security events
	Average time before a security event being detected
	Sufficiency of detection tools
	Automation of real-time detection
	Comprehensiveness of cyber risk detection
Data	Number of wrong data access rights
	Number of unauthorized data access
	Previous losses due to data breach
	Data recovery capability
	Data security technology update speed
Incidence Management	Average response time of material incidence
	Communication plan
	System, network, data and business recovery
	Incidence investigation and root cause identification capability
	Historical incidence database (company and industry)

Expert opinions on the relationship between these indicators and the risk assessment result for each category listed in Table 1 and the aggregate cyber risk level are needed. For example, if the number of detected security events is not high and the average time before a security event being detected is long, the risk of cyber event detection is high. With the indicators and cause-and-effect relationships, fuzzy logic models can be used to calculate the level of cyber risk, indicating both frequency and severity. New experience data can be used to backtest prior cyber risk assessment results. Experts may also change their opinions after digesting new knowledge and new experience.

Cyber Risk Management

The risk appetite for cyber risk sets the high-level strategy regarding cyber security. However, like other operational risks, proactive management is important to make sure that the cyber risk tolerance level will not be exceeded. Most approaches used for managing operational risks can be adjusted and used for cyber risk management.

Figure 2: Components of Active Cyber Risk Management



Investment in new technologies is important. New technologies can help identify the sources of cyber risk, prevent cyberattacks and maintain robustness of the internet system. New forms of cyber risk emerge every day, and the technologies used to combat cyber risk also evolve quickly. Even though new technologies may be too expensive to use now, it is important to understand their functions and applications so that they can be adopted when it is economical and necessary to do so.

Cyber risk training can help employees understand the sources and formats of cyberattacks, detect the existence of these attacks, follow precautious procedures and be able to take timely actions to mitigate their impact.

Risk limit setting for cyber risk is quite different from other risk types. For example, limits for insurance risk can use quantitative measures such as net amount at risk and mortality/morbidity/lapse experience. With the risk appetite setting the risk tolerance for cyber risk, the company’s internet system, data attractiveness to cyber criminals and employee awareness need to be assessed to understand the current level of cybersecurity. KRIs for cyber risk need to be designed based on the company’s specific business, data and system. Possible KRIs may include the number of system breakdowns per month, number of users with access to key sensitive data, the level of risk awareness measured by the training that has been taken by employees and the average length of time before a cyberattack is detected. Limits can be set by making reference to pioneers in cyber risk management while at the same time making adjustments according to the company’s situation.

Cyber risk monitoring is difficult because of the risk’s wide scope and fast evolution. Focus needs to be put on key data and key system protection, as the monitoring is unlikely to be complete and perfect. Because cyber risk events can happen quickly, the monitoring frequency needs to be higher than most other risk types such as insurance risk. The monitoring should include not only checking the current risk exposure against the risk limit, but also automatic and real-time monitoring of the internet system, communication system (email, phone, etc.) and social media data to identify any issues that could lead to a cyber risk event. Monitored issues may include a break of system security policies and procedures, malware, inappropriate user privileges, irregular system activities, communication to outside systems such as a third-party system or a home computer, key data access and transfer and so on.

A contingency plan is critical to managing losses, either financial or reputational, caused by cyber risk events. An action plan can help the company quickly respond to a cyber risk event such as a data breach and a system failure. It can help minimize business disruption and avoid being a headline on cyber security, or at least demonstrate the company's determination and capability to manage cyber risk.

Cyber insurance can be used to transfer severe impact of cyber risk events to a counterparty. Even with heavy investment in technology, training and active risk monitoring, unexpected cyber risk events can still happen. Cyber insurance adds an extra layer of protection to cover unexpected losses. Proactive cyber risk management is needed because cyber insurance does not cover all losses, and good cyber risk management can reduce the exposure to cyber risk and therefore get lower cyber insurance premiums. If a counterparty insures a huge amount of cyber risk, its ability to pay the promised benefits needs to be assessed because cyber risk events can affect many companies and personal users at the same time.

Conclusion

Cyber risk has become a top risk for the insurance industry with the embrace of the digital world and the internet of things. Cyber risk shares many features with other operational risks but is considered a fast-evolving and more influential risk in the future. Like other risks, risk appetite for cyber risk is useful for setting the high-level risk tolerance. However, it needs sophisticated modeling that can leverage both limited experience data and subject matter expertise in a consistent way. Proactive measures such as technology investment, training, risk monitoring and cyber insurance are important to control cyber risk exposure and keep pace with the development of new cyber risks.

[1] Max J. Rudolph, *Emerging Risks Survey* – 2014, Joint Risk Management Section, Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, December 2015, 7.

[2] Martin Eling and Jan Hendrik Wirfs, *Modelling and Management of Cyber Risk*, International Actuarial Association, 2015, 5–7, http://www.actuaries.org/oslo2015/papers/IAALS-Wirfs&Eling.pdf.

[3] Kailan Shang and Zakir Hossen, *Applying Fuzzy Logic to Risk Assessment and Decision-Making*, Joint Risk Management Section, Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, November 2013, 32–50.

Kailan Shang, FSA, CFA, PRM, SCJP, is cofounder of Swin Solutions Inc. He can be reached at *kailan.shang@swinsolutions.com.*

Determining the Likelihood of a Cybersecurity Failure for use in Cybersecurity Insurance Pricing

Steven Dionisi, CISSP, CISA, PMP, FFSI, CSSGB

The pricing of cybersecurity insurance is similar to pricing property and casualty (P&C) or liability insurance. For example, the pricing of home insurance is based on the house having fire detectors, re-enforced concrete in earthquake areas, location in flood or tornado zones, and so on. Similarly, cybersecurity insurance is based on the network having intrusion detection and prevention tools, patching of software, secure data centers and more.

Insurance, in these cases, is based on an event not happening. The risk is divided over many houses to cover the one house that is hit by a tornado or flood. Insurance companies, and their actuaries, do not plan for every house to be hit by a tornado or flood. This model may not work for cybersecurity. As John Chambers, CISCO's CEO, stated, "There are two types of companies in the world, those that have been hacked and those that don't know they have been hacked."[1]

Being hacked will be added to the list of death and taxes as outcomes that cannot be avoided. With that in mind, cybersecurity could be modeled after life insurance products. The question changes from whether or not a company is hacked to how likely a company is going to be hacked in a certain time frame. To calculate this probability, the factors of a likely cybersecurity incident need to be considered in a similar way that behavior, such as smoker/nonsmoker, and other factors are considered in calculating likely mortality over a period of time.

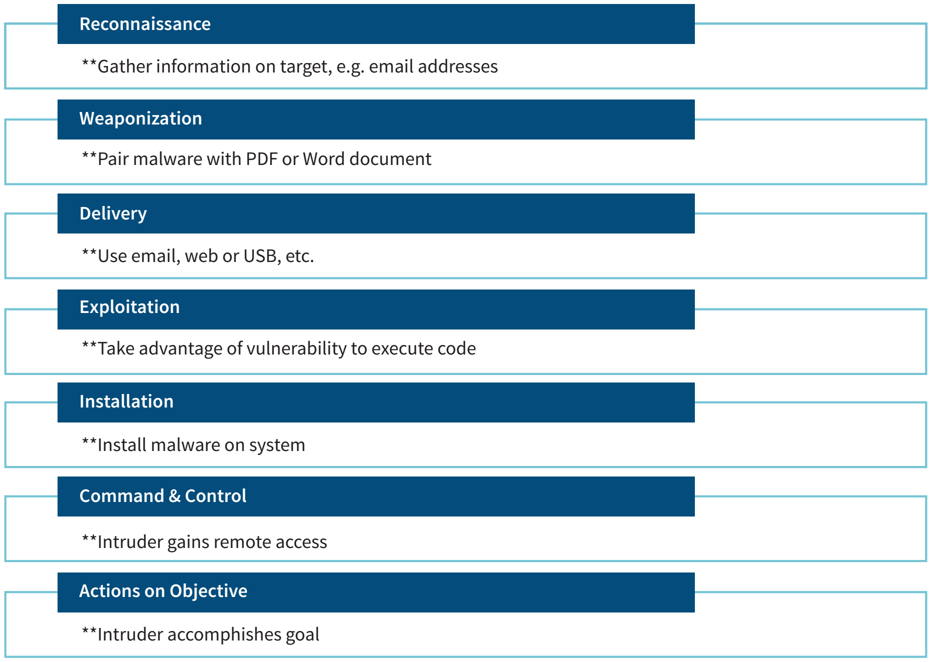
The factors that lead to a cybersecurity incident are outlined by Lockheed Martin and are called the Intrusion Kill Chain or Cyber Kill Chain (CKC).[2] The CKC defines seven stages of a cyberattack, where each stage requires a successful breach of the previous stage. The seven stages are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective. Because of the dependency of a stage in the CKC on failure of the previous stage, a cybersecurity incident can be modeled stochastically with a Markov analysis. This paper discusses the application of a Markov analysis to the CKC as a method to quantify the probability of failure to a cybersecurity system over a period of time or a number of attacks.

Cyber Kill Chain

Lockheed Martin's CKC outlines the set of steps, or stages, an attacker takes to breach and exploit a computer network (Figure 1). Each stage in the process builds on or takes advantage of the success of the previous stage. Any break in the chain will stop the attacker. The CKC is based on methodology developed by the Department of Defense to outline the structure of an attack.

The first step in the chain is reconnaissance. Attackers research, identify and select targets. During this stage, they gather email addresses and scan ports of the target company. With this information, they can prepare for the next step: weaponization. The attackers pair the malware with other tools, such as a Word document or Adobe Flash content. Once the weapon is created, delivery takes place. For example, delivery can be done by leaving USB drives with malware in the parking lot of a targeted company in the hope that employees will access the USB with their work computers. If the malware is delivered on the company's computer network, the attackers' code is activated and goes after an application or operating system. This is called the exploitation step in the CKC. Once the exploitation occurs, the intruders try to gain access by installing a trojan or a backdoor in the system. After the installation step, the command and control (C2) stage starts. The compromised system calls back to the attackers' computer, thereby establishing command and control. After the first six steps, the intruders can go after the company's data. Lockheed calls this "actions on objective."

Figure 1: Lockheed Martin's Cyber Kill Chain



Reconnaissance

**Gather information on target, e.g. email addresses

Weaponization

**Pair malware with PDF or Word document

Delivery

**Use email, web or USB, etc.

Exploitation

**Take advantage of vulnerability to execute code

Installation

**Install malware on system

Command & Control

**Intruder gains remote access

Actions on Objective

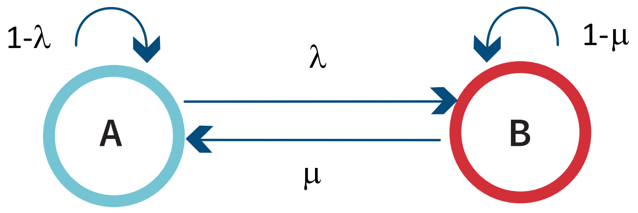
**Intruder accomphishes goal

There are information security tools or processes to detect and/or prevent an intruder at each stage. The probability of success of the attacker or inversely the probability of failure by the security tools can be estimated. While two of the stages, reconnaissance and weaponization, occur outside the targeted computer network, a likelihood of success/failure can be estimated. For example, intrusion detection systems can watch for port scans during the reconnaissance stage or use web analytics to determine if a possible attacker is gathering information. Process controls, like removing Adobe Flash or removing local administrative rights, can also factor into the probability calculations for weaponization.

Markov Analysis

Markov analysis is used for many types of reliability calculations where a sequence of dependent events can cause system failures. This analysis is typically used to calculate meantime between failure for aviation components, computer networks and other systems. One type of Markov analysis is called a Markov chain. It is a stochastic method of determining likely the state of a process based on the probability of events where each event is only dependent on the event immediately preceding it. For example, in the CKC, the exploitation stage occurs only if the delivery stage was successful. The interdependence of states can be represented using a state transition diagram (Figure 2). The states are noted by A and B. Probability of moving from state A to state B is λ and the probability of moving back to state A from state B is μ. The probability of remaining in a particular state is represented by 1 minus the probability of moving out of the current state. For state A, the probability of remaining in state A is 1-1-λ.

Figure 2: Simple Markov Chain State Transition Diagram



From the transition diagram, a transition matrix can be constructed (Figure 3). The probability of staying in state A is 1-λ(e.g., moving from state A to state A). As noted previously, moving from state A to state B is λ.

Figure 3: Simple Transition Matrix

$$\begin{bmatrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{bmatrix}$$

The likelihood of being in a certain state after a number of cycles can be represented by the following equation:

$$x_t = x_0 P^t$$

where

x represents the system state vector

P is the transition matrix and t is number of cycles where the probability vector will be calculated

x_0 is the initial state vector

In a simple example, state A is where a machine is working and state B is where the machine has failed. The machine has a 0.2 chance of failure in a single day and a 0.3 chance of being repaired in a day (μ). The (λ) initial state is represented by $x_0 = [1\ 0]$ where the machine is working. The transition matrix is

$$P = \begin{bmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \end{bmatrix}$$

So the likelihood of the machine being in a failed stated after three days is

$$x_3 = [1\ 0] * \begin{bmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \end{bmatrix}^3,$$

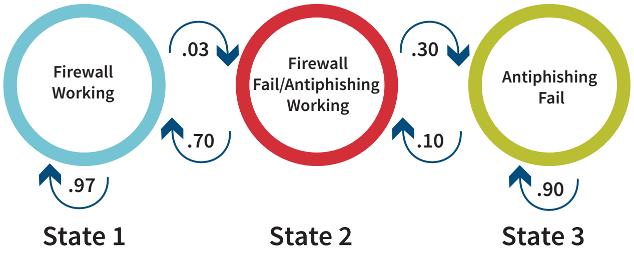
which resolves to x_3 = [0.650 0.350]. In other words, there is a 35 percent chance the machine will fail after three days.

Applying the Markov Chain to the Cyber Kill Chain

The Markov chain can be applied to the CKC to quantify the probability of failure to a cybersecurity system. For this paper, a simple example with static probabilities for the individual components will be used. Information security defenses are built around preventive, detective and corrective controls. The probability of remaining in CKC stage will be tied to the preventive controls. The detective and corrective controls will be combined to determine the probability of returning to a previous stage. For example, a corrective control would be the patching of a vulnerable operating system. To also simplify this example, only two stages will be examined.

The CKC Markov chain will be defined from state 1 to state 3 using the following stages: delivery and exploitation. In state 1, delivery prevention is working (i.e., the firewall is blocking spam emails at a 97 percent rate). In state 2, the delivery prevention has failed and exploitation prevention is working (i.e., users are trained not to open .exe attachments at a 70 percent rate and report the email). In state 3, exploitation prevention has failed. For this example, there will be a small probability that the exploitation is detected by other tools (10 percent) and the chain returns to state 2.

Figure 4: Cyber Kill Chain Transition Diagram



Based on the probabilities, the transition matrix becomes

$$P = \begin{bmatrix} .97 & .03 & 0.0 \\ .70 & 0.0 & .30 \\ 0.0 & .10 & .90 \end{bmatrix}$$

And the initial state vector is x_0= [1 0 0]. After 100 cycles, the resulting vector is x_{100} = [0.853 .036 .109]. In other words, there is approximately an 11 percent chance of the malware being executed. (State 3 probability is .109.)

Conclusions

The CKC model allows the various tools and processes used in cybersecurity to be grouped in a logical sequence. With this logical sequence established, stochastic reliability analysis can be used to determine the probability of failure.

In this example, a very simplistic model with static probabilities was used. More robust and complex probabilities, such as Weibull, would be used when the reliabilities of the individual security tools are better understood. Additionally, companies have increased their sharing of threat information. Better sharing between companies will greatly improve the understanding of the reliability rates of these cyber protection tools.

As demonstrated, applying reliability methodology to cybersecurity systems can help quantify the likelihood of a cyber protection failure. Once the likelihood of failure is estimated, actuarial analysis used for insurance products such as term life could be applied to cyber systems.

The views expressed herein are those of the author and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System.

[1] "John Chambers' 10 Most Memorable Quotes as Cisco CEO," *Networkworld*, July 24, 2015, http://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html.

[2] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," white paper, Lockheed Martin Corporation, n.d., http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

Steven Dionisi, CISSP, CISA, PMP, FFSI, CSSGB, is a commissioned IT examiner at the Federal Reserve Bank in Boston. He can be reached at *steven.dionisi@bos.frb.org.*

SOCIETY OF
ACTUARIES