Developing cyber insurance products and services: Three recent case studies

Elizabeth Bart, FCAS, MAAA

Milliman

Even though we're in a time of big data, we still don't have all the insurance-specific data we need for pricing cyber risk.

There are innumerable statistics on the cost of cyber losses– but how relevant are these generalized dollar amounts to an individual insurer or entity? Cyber costs are often stated with mind-boggling figures: the average cost of a U.S. cyber crime was $15 million[1] and global costs totaled $400 billion in 2014[2]—and could reach $2 trillion by 2019[3].

These astronomical numbers and the publicity of large retailers' hacks have drawn attention to cyber liability, especially by insurers, information technology vendors, and lawyers. Even as cyber becomes an issue for the C-suite and boards of directors in all companies, the cost information available—which tends to focus on the massive claims filed by the largest companies—does not lend much insight for small- and mid-sized businesses or for those with less exposure to cyber.

Without traditional actuarial and insurance data, how are small- to mid-sized insurers, captives, and self-insurers pricing cyber insurance?

While large cyber cost numbers make for splashy headlines, in the insurance arena, cyber costs require specificity. Actuaries working on traditional lines of insurance have the luxury of years of claims data– not only do they have access to loss information on indemnity and defense costs, but also to timing information on claim development, reporting, and payment patterns. Additionally, the loss information is robust enough to be analyzed for more homogeneous exposures (e.g., workers' compensation pricing can be done specifically for a distributor only in the Pacific Northwest or medical malpractice pricing can be done by physician specialty by county in Ohio).

Not only are consistent characteristics of the insured important (number of employees, type of employee responsibilities, location, revenue, etc.), but consistent characteristics of the policies help make pricing easier as well. Comparing workers' compensation policies, for example, across different insurers is relatively straightforward for brokers and insureds because these policy forms are fairly uniform and standardized across the insurance industry. On the other hand, cyber policies' specific coverages, triggers, exclusions, and offered limits vary greatly between insureds.[4]

The passing of the Cybersecurity Information Sharing Act (CISA)[5] federally mandates the sharing of cyber threat information and best practices guidance. While this is very helpful for proactive cyber protection in general, it unfortunately does not require the sharing of the data that the insurance industry currently uses for its more traditional lines of insurance to assist actuaries in pricing. Workers' compensation insurers can get additional aggregated industry information from the National Council on Compensation Insurance (NCCI), and general liability and auto liability insurers can get aggregated industry information from Insurance Services Organization (ISO). Without the traditional insurance data available to actuaries, small- to mid-sized insurers, captives, and self-insurers are unable to rely on traditional actuarial methodologies for this new insurance offering.

Three recent case studies: How Milliman has priced cyber

A NEW CYBER WRITER

A European cyber reinsurer with a focus on small- to mid-sized businesses started offering a cyber insurance product in the United States that is similar to its European one. Its original filing submission to states' departments of insurance (DOIs) was based on reinsurance pricing which responded to competitive rates in the market. However, the DOIs rejected a majority of the filings because they lacked actuarial support.

1 http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states

2 http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

3 http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7d2f93603bb0

4 http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/

5 http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/

For the same reasons cyber insurance buyers have a hard time comparing policies, comparing rate filings among competitors is equally challenging. With each insurer offering different cyber coverages, services, and limits, the severities, frequencies, and underwriting guidelines tend to be very different.

Relying on publicly available, generally accepted, nonspecific cyber frequency and severity information was the most straightforward way to support the premiums. There was not sufficient credible historical loss data available from the insurer, there was nothing comparable from other insurers' filings, and, as mentioned, there was no aggregate insurance industry data available. With the insurer's focus on small- to mid-sized businesses, the competitive marketplace was dictating premiums under $10,000 (depending on the size of the insured and the coverage limits). For this pricing, the Ponemon Institute's often referenced $15 million loss event is not a likely scenario for this group.

By working with a combination of the client's own reinsurance data and by data mining publicly available cyber data specific to the target insured, we were able to determine applicable frequencies and severities to demonstrate the appropriateness of the originally filed rates and successfully get approval for the premiums in all states.

A HEALTHCARE CAPTIVE

A large hospital system purchasing commercial cyber insurance with $50 million limits was considering a $1 million or $2 million deductible, which would be covered by its captive. For captive budgeting purposes, the company needed assistance to price the deductible layers.

Healthcare cyber breaches frequently appeared in the news in 2015; in fact, the year was deemed the "year of the healthcare hack." With the significant number of large dollar hacks in the healthcare industry of late, a number of sources estimate the approximate annual frequency of a cyber attack on a healthcare organization at 25%. However, determining any frequency differences between entities– an individual clinic, a large hospital system, a small rural versus large urban organization– is more difficult. Further, determining the proportion of the 25% of hacked organizations that suffered a "successful" attack (resulting in actual losses) is even more difficult, especially because publicizing a hack can result in some reputational damage. Larger healthcare systems would have more patient and employee data but might also have better cyber controls in place. Smaller targets may have less data, but it might be easier for hackers to obtain that data if smaller healthcare practitioners aren't as prepared.[6]

Using a database of publicly known cyber breaches, we were able to data mine the available information to review only healthcare organizations and breaches caused specifically by hacking, malware, and insider breaches– those deemed the most likely to result in the theft of a large number of records for malicious motives. Using the number of compromised records for these specific healthcare breaches and the average cost per lost or stolen record, we determined the loss estimates for the captive's potential retained layer.

IDENTITY THEFT COVERAGE

A multinational insurer wanted to offer identity theft insurance as a complementary service to pair with its identity theft protection and monitoring services. The insurer had an idea of the range of premium it would need to charge to be competitive yet profitable and needed actuarial pricing of its proposed coverages and limits to determine feasibility.

Personal identity theft statistics proved much easier to obtain through detailed reports from the U.S. Department of Justice/Bureau of Justice Statistics and the FBI. Additionally, competitor filings were considerably more similar for personal identity theft than for commercial cyber liability. (However, personal lines filings are a bit more constrictive and under more DOI regulator scrutiny than commercial lines filings.)

What makes the identity theft information insurance-industry friendly is that severities and frequencies are tracked not only for all thefts (including those not resulting in a dollar loss) but also separately for thefts that resulted in monetary losses. Frequencies and severities are also reviewed by victim characteristics such as age and household income and type of attack, such as through a credit card, bank account, or a new account. The distribution of general losses is even obtainable.

While data this detailed seems to be concrete, it shows how volatile cyber loss information is year over year. With only two or three data points, it is difficult to determine if an increase or decrease in any one statistic is the sign of a trend or a random fluctuation. This also highlights a complexity of cyber insurance– any future emergence of new classes or types of losses will not be captured in what little historic data there is currently available and could be considered unestimatable.

Unlike other areas of insurance, like workers' compensation and medical malpractice—for which there is a trove of readily available insurance-specific data—pricing cyber insurance is much more difficult. Cyber risk continues to emerge as a threat taking numerous different forms and constantly changing– especially for small- and mid-sized companies. While there is seemingly plenty of cyber risk data available, the insurance industry needs more and better insurance-specific data in order to price cyber insurance in the best and most accurate way possible.

6 http://www.beckershospitalreview.com/healthcare-information-technology/data-breaches-in-2016-what-can-we-expect.html

FOR MORE ON MILLIMAN'S HEALTHCARE REFORM PERSPECTIVE:

Visit our reform library at www.milliman.com/hcr
Visit our blog at www.healthcaretownhall.com
Or follow us on Twitter at www.twitter.com/millimanhealth

Milliman

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

milliman.com

CONTACT

Elizabeth Bart
elizabeth.bart@Milliman.com