THE FEDERAL RESERVE BANK
OF CHICAGO

ESSAYS ON ISSUES
2019 NUMBER 426
https://doi.org/10.21033/cfl-2019-426

Chicago Fed Letter

The growth and challenges of cyber insurance

by Andrew Granato, senior research assistant, and Andy Polacek, senior research analyst

Cyberattacks have grown in frequency and cost over the past decade, with high-profile cases, such as the 2013 Target data breach, the 2017 Equifax data breach, and the leak of Democratic National Committee emails during the 2016 election making national headlines. Ransomware attacks, intellectual property theft, and fraud cost companies billions in recovery expenses, fines, and lost revenues every year. More firms are purchasing cyber insurance as a way to cover losses and expenses resulting from cyber incidents.

However, cyber insurance alone is not a panacea, and even firms that have cyber insurance may not be as protected as they think. Unlike traditional lines of business such as private auto insurance, where standardized policies provide liability or collision coverage, cyber insurance policy language is not standardized. The types of risks covered under cyber insurance vary significantly across policies and businesses, and insurers do not always agree on what loss events are covered under those policies. The features of cyber events, including a limited loss history, the unreliability of past data when predicting future events, and the possibility of a large-scale attack where losses are highly correlated across companies and/or industries, make it difficult to write comprehensive policies. In this *Chicago Fed Letter*, we examine the extent to which cyber insurance can help protect businesses and the wider economy from the costs of cyberattacks and how institutional factors and legal uncertainties may obstruct the development of this market.

What is cyber insurance?

Most observers trace the history of cyber insurance back to Steven Haase, who helped AIG write the first internet security liability policy in the spring of 1997. The first cyber insurance policies were geared toward information technology companies responsible for managing networks and systems used by other businesses and consumers. But the cyber insurance market has since expanded, and current cyber protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage (sometimes called nonaffirmative cyber exposure). We define and discuss each of these in turn.

> Even firms that have cyber insurance may not be as protected as they think.

Third-party liability cyber insurance reimburses said entities for the costs incurred by their clients because of data breaches, malware infections, or other cyberattacks in which the insured entity was at fault. Third-party liability coverage is the cyber equivalent of medical malpractice, where businesses are insured against harm they inflict on their clients by their action (or, as is usually the case with cyber risk, inaction). Many early policies were of this form.

In the mid-2000s, cyber insurers began offering first-party expense coverage, which expanded insurance offerings to any company that uses technology. First-party expense cyber insurance reimburses companies for the costs of a cyberattack that directly affects their business. First-party policies can be broad or very specific, depending on the needs of the company, and may cover post-cyberattack expenses such as credit-monitoring and other data breach expenses, hiring crisis management consultants to restore brand reputation or negotiators to handle ransom payments, and data recovery costs.

Silent cyber risk is a third type of cyber insurance coverage that is not a cyber insurance policy at all, but a term that refers to potential cyber-related losses stemming from traditional property and casualty (P&C) policies not specifically designed to cover cyber risks. Consider a scenario where a hotel's computer system is infected with malware, which sets the sprinkler system off, damaging the interior and causing a patron to slip and fall. If cyber perils are not explicitly excluded, the hotel's traditional property and casualty coverage would be expected to cover the damage to the hotel caused by the sprinklers and the medical bills of the injured patron. Silent cyber is steadily becoming less of a risk for insurers as they transition to P&C policies that either explicitly exclude or include losses caused by cyberattacks. For example, by January 1, 2020, AIG will finalize their transition to affirmative cyber coverage across their commercial insurance lines, effectively eliminating most silent cyber risks to their business, while removing the implicit cyber-risk coverage from their existing customers.[1]

> Current cyber protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage.

Cyber insurance is a rapidly growing business, but it is still a relatively small part of the overall U.S. P&C insurance market. Today U.S. businesses can get cyber insurance either as a standalone policy or as part of their general P&C coverage in a packaged policy. Standalone and packaged policies, respectively, accounted for $1.1 billion and $922 million in 2018 premiums. While the amount of written cyber insurance premiums has more than doubled since 2015, the cyber insurance market is still small, accounting for less than 0.5% of all U.S. P&C business.[2]

Cyber insurance adoption rates vary significantly across firms and industries. About 58% of large businesses have a standalone cyber insurance policy, compared with just 21% of small businesses. Industries with the highest adoption rates were education (66%) and healthcare (62%); technology and communications firms had a 51% adoption rate. Industries with lower adoption rates included financial institutions (27%), manufacturing (30%), retail (39%), and utilities (41%).[3]

Challenges of writing cyber insurance

As the cyber market has matured, insurers have refined how these policies are underwritten and priced. However, there are fundamental aspects of cyber insurance that make it difficult for insurers to write and price policies that cover a broad swath of risks. We discuss some of these challenges below.

First, there is only a limited loss history for insurers to use when setting prices for cyber insurance premiums and coverage loss limits, and this introduces risk. When insurers set auto insurance premiums, for example, they can rely on a long history of accidents and damages to model the probability that a driver with a specific set of characteristics will get in an accident and then set premiums to cover this expected loss. Cyber insurers, working in a fast-developing market, instead rely on a number of indirect factors to try to price policies appropriately, including market estimates of the cost of cyberattacks, questionnaires to determine the riskiness of the insured, their own (often limited) underwriting experience, and pricing by other insurance companies.[4]

Pricing a new insurance product carries risks: For example, Mohey-Deen and Rosen (2018) explore how underpricing of another, then new, line of business, long-term care insurance, contributed to the insolvency of Penn Treaty. Penn Treaty used overly optimistic financial assumptions derived from their "experiences with other products," and when those assumptions turned out to be wrong, the company became "the second largest insolvency in insurance guaranty fund history."[5]

Second, cyberattacks are constantly evolving as both private and state-sponsored hackers develop new methods to infiltrate networks. The rapid evolution of hacking capabilities and strategies makes it difficult for insurers, which rely on clients having relatively consistent risk profiles, to assess the true risk of a potential client being hacked. The increased sophistication of hackers is evident, in that both the frequency and costs of cyberattacks have risen in recent years: In the U.S. the reported cost of the average cyberattack rose 29% from $21.2 million in 2017 to $27.4 million in 2018. Despite this, the cyber-insurance market remained profitable for underwriters.[6]

Third, cyberattacks are highly scalable as they can potentially hit thousands of companies simultaneously, causing large interrelated losses for insurers. Due to the design of the internet, there are highly important central nodes. This type of network centralization creates two problems for cyber insurers. One type of problem would occur if an important service, such as a large cloud computing platform used by many policyholders, went down. The insurer may then have to pay claims on all of its policyholders at once. A similar dynamic can be seen in natural disasters, where private insurers are often reluctant to offer flood insurance, because if a single house in a neighborhood was hit by a flood, it is likely that many houses around it were also hit at the same time. For example, in the 1920s, following a series of catastrophic floods along the Mississippi River, private insurers began explicitly excluding flood coverage from their home insurance policies, eventually resulting in the creation of the National Flood Insurance Program (NFIP) to fill the gap.[7]

A fourth type of problem cyber insurance faces is the possibility of cascading failures caused by a cyberattack. One common example of a cascading failure is an attack on a power grid, where the destruction of a piece of critical infrastructure leads to failures across the rest of the grid. Cyberattacks using self-reproducing malware can also spread across a network of computers. Such an attack occurred in 2017, when a piece of malicious Russian code dubbed NotPetya targeted Ukraine. By exploiting a vulnerability in Windows to gain control over unpatched computers, NotPetya then used this access to gain passwords of other machines on the network and jumped across the globe, causing over $10 billion in estimated damages.[8] Such an attack could happen again, and it could be worse next time.

The difficulties in properly pricing cyber insurance products and the looming possibility of a large-scale cyberattack encourage insurers to write policies that limit the amount of coverage a business can get, as well as the risks that are insured. Given the restrictive nature of some policies, some businesses may overestimate the amount of cyber coverage they actually have.

Cyber insurance coverage uncertainties

In July 2019, FM Global, a commercial property insurer, conducted a survey of chief financial officers (CFOs) at companies with over $1 billion in revenue. The survey found that 71% of the CFOs reported they believed that their insurer would cover "most or all" of the losses their company would suffer in a cyberattack. However, those same CFOs identified damages they expected to suffer in such an event that are not covered by typical cyber and property insurance policies. Almost half of CFOs said that they expected fallout from a cyberattack to include a devaluation of a firm's brand; more than one-third said they expected increased investor scrutiny, a decline in revenue, and an introduction of regulatory compliance problems; and a quarter said they expected a decline in market share and share price. None of those costs are normally covered in cyber insurance policies.[9]

This apparent disconnect speaks to the importance of pursuing increased clarity when underwriting cyber insurance coverage, as disputes about coverage between insurers and policyholders are percolating in the legal system. Lawsuits around the country reflect current ambiguities about the nature of responsibility for cyberattacks and data breaches.

Legal uncertainty in cyber

Adding to the uncertainties insurers face when attempting to structure policies in this new market is the relative lack of legal precedent on core issues pertaining to cyberattacks. When facing uncertainty regarding fundamental questions, insurers may decide to wait until such issues are resolved before offering policies or only write policies with restrictive coverage that are less useful to businesses.

For example, data breaches and data theft are a common source of damages from cyberattacks, yet important case law on this issue is still unresolved. Legal cases involving data breaches rest on the nature of the alleged harm: If personal data are exposed due to a cyberattack on a database, has the person whose data was exposed suffered sufficient concrete harm or does there merely need to be "substantial risk" that future harm will occur? Circuit courts are split on this issue. Several courts have found that victims of data breaches do not have standing to sue when no actual identity theft or fraud occurs, while others have found that the risk of data misuse that results from a breach confers standing. The Supreme Court has yet to directly address the issue of standing in data breach litigation. In March 2019, the Supreme Court refused to hear an appeal from Zappos.com of a Ninth Circuit Court ruling that plaintiffs who had only alleged that financial losses were imminent also had sufficient standing to sue.

This uncertainty over standing in data breach litigation is important for cyber insurers because it directly affects the probability that an insurer will have to pay claims in the event of a data breach and this, in turn, affects how they should price their insurance policies.

Meanwhile, lawsuits that are directly concerned with cyber insurance coverage have already begun to appear. One case that has particular significance for the development of the cyber insurance market, between Mondelēz International (an American food company) and Zurich Insurance Group, arose over a disagreement about a common "act of war" exclusion. In June 2017, as discussed earlier, a virus called NotPetya was released into Ukrainian information technology systems. The virus quickly spread to multinational companies, including Mondelēz, leading Mondelēz alone to claim $100 million in damages from the attack. At the time, Mondelēz had a contract with Zurich that covered "physical loss or damage to electronic data, programs or software" triggered by "the malicious introduction of a machine code or instruction." The policy contained an exclusion for "hostile or warlike action in time of peace or war," a common exclusion in such contracts.[10]

In February 2018, the White House called NotPetya a "reckless and indiscriminate cyberattack" on the part of the "Russian military" and "the Kremlin."[11] Mondelēz filed a claim for reimbursement, but Zurich denied it, claiming that the White House's declaration qualified NotPetya as an "act of war"; Mondelēz filed suit in January 2019. If Zurich successfully argues that NotPetya qualifies as an act of war, it will establish a precedent that many of the cyberattacks that companies face are not covered by their insurance. This case illustrates that not only the nature of the crime, but also the nature of the perpetrator must be written specifically into cyber insurance policies to avoid legal conflicts.

Another related source of uncertainty stems from a yet untested feature of cyber insurance law, the 2002 Terrorism Risk Insurance Act (TRIA). Created in response to the 9/11 terrorist attacks, TRIA requires P&C insurers to "make available" terrorism risk insurance and stipulates that the U.S. government will cover damages caused by certified acts of terrorism in excess of a predefined threshold. (The Secretary of the Treasury, in conjunction with the Secretary of Homeland Security,

certifies that an act of terrorism qualifies under TRIA.) In 2016, the U.S. Treasury issued guidance confirming that standalone cyber insurance policies are covered under TRIA. However, there has yet to be a TRIA-certified act of terrorism and questions remain about how TRIA might be triggered by a cyberattack. TRIA was specifically intended to cover acts of terrorism that pose a threat to human life or damage critical infrastructure, so it seems unlikely that TRIA would apply to financial losses resulting from a data breach or denial of service attack. Additionally, governments are not usually considered "terrorist organizations," so a state-sponsored cyberattack would more likely fall under the "act of war" exclusion than qualify for protection under TRIA.

The future of cyber insurance

Currently, the cyber insurance market only covers a small percentage of the overall losses caused by cyberattacks. Measuring the complete impact of cyberattacks on the U.S. economy is difficult. However, the White House Council of Economic Advisers developed a model using the stock market reactions of firms that had experienced "malicious cyber activity" to estimate the cost of cyberattacks. Using this model, they found cyberattacks cost the U.S. economy between $57 billion and $109 billion in 2016, equivalent to 0.3% to 0.6% of GDP.[12] During that same period, U.S. insurance companies incurred $356 million in claims from policyholders, equivalent to less than 1% of estimated losses.[13] Compare this to natural catastrophes, where 50% of losses between 2015 and 2018 were paid by insurers.[14] This difference in insured losses illustrates the room for growth in the cyber insurance market. But for the cyber insurance market to bridge this gap and continue to grow, it must overcome the challenges we have discussed here.

Insurance companies are already beginning to write cyber insurance contracts that more explicitly define what is or is not covered, and this trend should help limit lawsuits and disputes over cyber coverage. Court decisions should help insurers and policyholders clarify language in their contracts. However, the Mondelēz v. Zurich case provides an important litmus test for the future of cyber insurance. Alleged state-sponsored cyberattacks have grown in frequency in recent years, and some argue that these present the greatest cybersecurity threat to the U.S. economy.[15] As long as uncertainty exists over what qualifies as an "act of war" in the context of cyber insurance, it will be difficult for insurers and policyholders to agree on contracts with all parties sharing a clear understanding of what is covered.

Even as insurers acquire additional historical data on cyber loss events, the modeling of cyber risk will continue to present challenges. At the heart of the problem of modeling cyber insurance is that yesterday's attacks do not necessarily inform us about tomorrow's risks. In order to help insurers accurately price future cyber risks, predictive cyber-risk models will have to be developed.

Finally, the cyber insurance industry needs to consider how to deal with the possibility of large loss events. Better modeling of cyberattacks should help insurers measure their accumulation of interrelated risks, and improved cybersecurity standards and practices may help businesses avoid such catastrophic attacks to begin with. Looking at the ways in which the insurance sector has provided comprehensive insurance coverage for natural catastrophes may provide a way forward for the cyber insurance market.

Summary

Cyber insurance is a small but growing market. As cyberattacks become more frequent and more damaging, people and institutions are searching for cyber coverage that protects them from these risks. However, the cyber insurance industry faces significant challenges, including a lack of historical data, a lack of ability to predict the future of cyber risk, the possibility of large cascading loss events, uncertainties among market participants about what is specifically covered under such policies, and legal battles over fundamental issues. The future growth of the market will depend upon how these issues are resolved.

Notes

[1] Available online, https://www.businesswire.com/news/home/20190905005481/en/AIGFinalizingTransitionAffirmativeCyberCoverageGlobal.

[2] Data from S&P Global Market Intelligence and authors' calculations.

[3] Data on large/small businesses are available online, https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf. Data by industry are from Marsh PLACEMAP, available online, https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html.

[4] See Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, 2019, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, Vol. 5, No. 1. Crossref, https://doi.org/10.1093/cybsec/tyz002

[5] Zain Mohey-Deen and Richard J. Rosen, 2018, "The risks of pricing new insurance products: The case of long-term care," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 397. Crossref, https://doi.org/10.21033/cfl-2018-397

[6] Available online, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf#zoom=50.

[7] Alejandro Drexler, Andrew Granato, and Richard J. Rosen, 2019, "Homeowners' financial protection against natural disasters," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, No. 409. Crossref, https://doi.org/10.21033/cfl-2019-409

[8] Available online, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[9] Available online, https://newsroom.fmglobal.com/releases/cyber-insurance-may-create-false-sense-of-security-among-senior-financial-executives-at-worlds-top-companies-suggests-fm-global-survey.

[10] Cited material in this paragraph is available online, https://www.insurancejournal.com/news/international/2019/01/11/514553.htm.

[11] Available online, https://www.wired.com/story/white-house-russia-notpetya-attribution/.

[12] Available online, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[13] Based on insurance statutory filings from S&P Global Market Intelligence. Data include both standalone and packaged policies, but not claims paid by surplus line insurers that are not required to report financials to the NAIC.

[14] Data from Munich Re NatCatSERVICE for all North American losses.

[15] Available online, https://www.insurancejournal.com/news/international/2019/03/27/521824.htm.

ISSN 0895-0164