A Leading Global Investment Management Firm

Insurance Insights

October 2019

INSURANCE RESEARCH | WHITE PAPER

Cyber Coverage: What You Don't Know Might Hurt You

By Rebekah Humphrey and Matthew Sternat

The industry as a whole has been responding to the ever-evolving cyber threat with solutions from different angles and components within the insurance value chain.

One of the major concerns for insurers has been the "silent cyber" impact—that is, paying claims from policies that originally were neither intended to respond to nor priced for cyber-related claims. Insurers have been responding by either clearly affirming or excluding cyber coverage in other commercial policies.

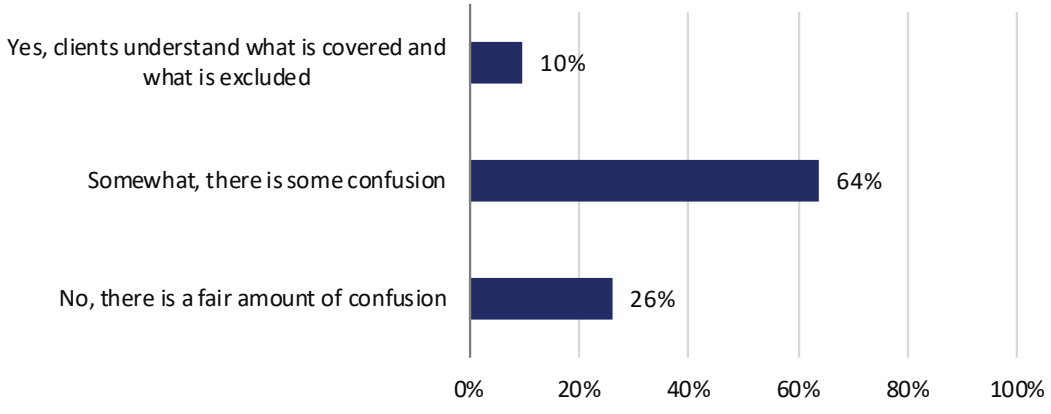
As the cyber threat continues to grow, vendors are managing their risk by requiring subcontractors to have cyber insurance as part of their contractual obligations. As this space continues to evolve, education remains a core need, as Conning notes in our Strategic Study, "U.S. Cyber Insurance Market Overview: The Evolving Response to a Pervasive Threat." Agents and clients need to be educated on their exposures and relevant coverages to understand their options and how a standalone cyber or cyber supplemental coverage can help their risk management needs.

Silent Cyber: Identifying the Real Risks and Clarifying Coverage

Silent cyber is policy exposure from cyber-related attacks that may be contained in other lines of business. While apprehension over the potential for silent cyber payouts appears to have lessened, the threat remains a concern for segments of the industry. Examples of silent cyber include a cyber-attack on a piece of manufacturing equipment that causes it to overheat and create an entire plant fire, which would fall under a commercial property policy. Within D&O, if the directors of a company knew about Internet security issues and did not address them before an attack, there would be liability loss exposure on that policy.

Broadly speaking, the industry is well attuned to the issue—with regulators, rating agencies, insurers and reinsurers taking various steps to review and mitigate silent exposures. However, there are fragmented approaches for dealing with this issue, from one end of the spectrum (no consideration) to the other (line-by-line policy wording evaluation and approval; at some companies, underwriters are prohibited from adding on cyber without approval). Some are

Figure 1 Agent Perception of Insurance Buyer Knowledge Regarding Cyber Policies



Prepared by Conning, Inc. Source: Conning 2018 Cyber Insurance Survey

comfortable with potential silent cyber because they are confident in their underwriting, diversification of business classes, managing of limits and retentions, insurance agreements, and use of data. One of the approaches for mitigating silent cyber is to either explicitly exclude or affirm cyber coverage for all commercial policies. Several companies have announced that they are employing this approach. On September 5, 2019, AIG announced that it will be either excluding or affirming coverage of cyber-related exposures over the entirety of the company's commercial property and casualty policies by January 2020. In a press release, AIG indicated that the transition will help clients more clearly evaluate their cyber exposures and choose the appropriate coverage and policies.

Additionally, in April 2019, Allianz announced that it already implemented this action for its Allianz Global Corporate & Specialty subsidiary and would be incorporating this approach for other Allianz property-casualty companies by January 2020 at the latest. The benefit is the increased transparency for the policyholder and smoother settlement of claims due to clarity of coverage. However, despite progress on this issue, several insurers have not addressed the risk head-on. The embedded risk in some of the longer-tailed lines can take years to develop (such as professional lines, D&O, etc.).

Given the speed and depth that the aggregation of loss events could trigger, silent cyber has the potential for devastating outsized losses. The NotPetya attack hitting Merck in June 2017 provides a strong example. Roughly 86% of Merck's nearly $2 billion in insurance losses from that cyber event came from non-affirmative cyber lines of business, mainly property. Property Claim Services (PCS) estimates that, of the entire $3 billion of insured losses from Petya/NotPetya, only 10% were attributed to affirmative cyber coverage, leaving the rest to come from coverage not originally designed or priced to respond to digital risks. The shift into first-party losses was the big driver of the silent cyber losses from 2017's other large-scale cyber-attacks (WannaCry, Petya) that hit on system-failure and business-interruption claims. Additionally, PCS is reporting that insured losses rise by as much as 30% as claims continue to develop.

What's Included? Examining the Effect of the War/Hostile Acts Exclusion

The extent and validity of cyber coverage under property policies have been in the limelight recently, including two cases related to NotPetya claims. Food conglomerate Mondelez International sued its insurer (Zurich) in January 2019 for denying claims stemming from the NotPetya attack under its property policy. Zurich reportedly has invoked the war exclusion. Merck also brought a lawsuit against 20 of its insurers in April 2019 for denying NotPetya-related claims, some of which reportedly were denied based on the war exclusion. The NotPetya attack was a malware attack that spread widely and caused business interruption for several large international corporations. The malware attack has been widely attributed—including by the U.S. government—to Russian state actors as an attack on the Ukraine. Russia has denied involvement.

Common in insurance policies, an "act of war" (or "hostile acts") exclusion exempts damage claims stemming from hostile or warlike actions from a sovereign power, government, military, or agent of those entities. Notably, in the majority of standalone cyber policies, the war exclusion language has a carveout that brings claims that stem from cyber-attacks to the insured's network back into coverage—exempting them from the exclusion.

While property policies are in question, cyber insurance is often mistakenly getting negative media coverage due to the current court cases. However, with education, this may turn positive for the cyber insurance industry, as a greater understanding of various policies, appropriate coverage and exclusions may be top of mind for many chief information security officers. Cyber industry contacts indicate that standalone cyber policies paid out for NotPetya claims. As coverage is tested in the courts, the industry and consumers will have more insight into some of the silent cyber issues that created coverage confusion and disputes.

Who's Invited to the Party? Establishing Policies for Third-Party Exposure

Another response has developed related to how businesses handle third-party relationships. When companies engage with other entities, their organizations become vulnerable to cyber-attacks, either from the sharing of sensitive information and data or through connections to each other's technology platforms. One example is the major attack on Target that involved infiltrating the retailer's systems through an HVAC contractor that had access to Target platforms. Another includes how several retailers' customer credit card data was hacked through a

third-party chat/service-provider tech firm. MyHeritage Genealogy's 92 million users' personal information was hacked from an archive of a third-party server.

A 2018 study by the Ponemon Institute found that 59% of surveyed companies had a data breach caused by a third party or vendor.[1] These third-party vendors are typically small businesses that often do not have the resources or experience to protect themselves from cyber intrusions. Compounding the issue, smaller businesses are more frequently the target of cybercriminals due to their vulnerability and as potential points of entry into "bigger prey."

The industry is acting on several fronts to address this exposure. The first is a risk management approach to establish protocols and procedures to which both parties must adhere. Companies are being more diligent about establishing plans and best practices around reviewing all their vendors and respective protection programs through cybersecurity risk assessments. Firms are also fostering better communication, transparency, and notification protocols as incidents occur. It requires ongoing audits, taking inventory of vendors, and dedicated oversight of third-party activities and engagements.

The second approach to mitigating cyber exposure is to insert language in third-party vendor contracts that requires these third parties to acquire cyber insurance, similar to how vendors are often required to carry liability insurance in order to land the contract. Other additional basic contract language includes third parties certifying they are in compliance with applicable privacy and data protection laws, as well as indemnification clauses if a breach occurs through a third party.

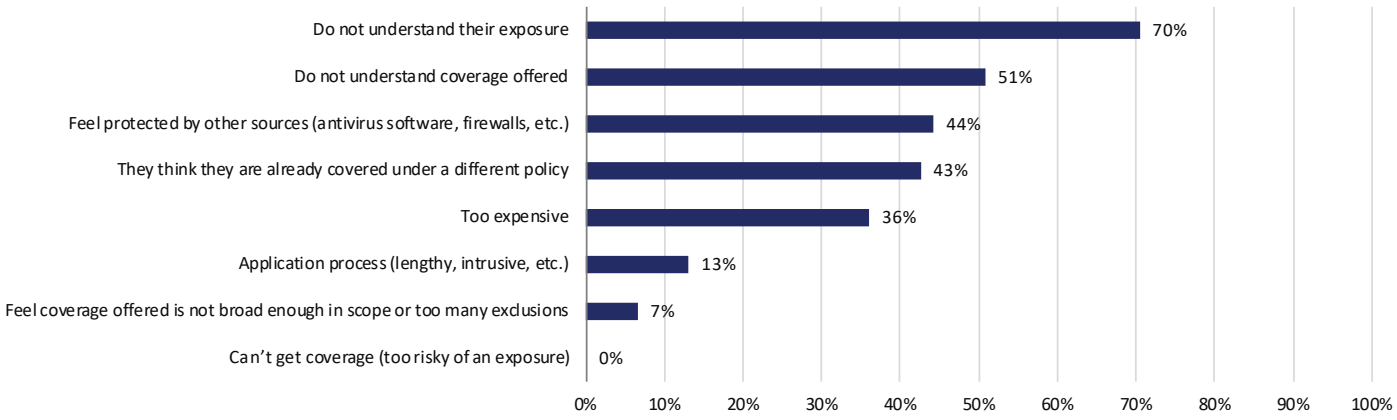
While the U.S. leads the globe in the uptake of cyber insurance and the requirement of coverage for certain contracts will help, there is still room for increased adoption and purchase of cyber policies. With the market so competitive, pricing has come down and is less a factor in driving non-purchase. Conning has found that education and awareness are the key to further uptake in cyber insurance policies.

A portion of the buyer's lack of knowledge is a limited understanding of what is and is not covered in a cyber policy. As documented in Conning's cyber insurance market overview survey, almost all agents (90%) believe there was some level of confusion, and 26% believe that there was a high degree of confusion about what is covered and excluded (see Figure 1).

Education is the Name of the Game

Additionally per our survey, agents/brokers said they believe, by far, that the biggest reason businesses are not buying cyber coverage is due to that lack of understanding of what the true exposures are. Almost three-fourths (70%) of respondents selected it as a top reason (see Figure 2).

Figure 2 Why Are Companies NOT Purchasing Cyber Coverage?



Prepared by Conning, Inc. Source: Conning 2018 Cyber Insurance Survey

The second-most selected factor (by 51% of respondents) in hindering cyber policy purchases was that clients do not understand the coverages offered. The next two reasons related to the perception that protection came from other sources: from either noninsurance solutions (44%), such as antivirus software, or other policies providing cyber coverage (43%). In fact, the first four reasons given by brokers are related to some form of buyer understanding or education about cyber coverages or exposures.

What is clear is that, even though news stories about cyber incidents are becoming more frequent, there is still plenty of room for further education and understanding of the risks that cyber threats bring to a business or individual. Cyber exposures are constantly morphing and evolving, which requires all parties involved—insurers, brokers and buyers—to remain up to date on the threats to and vulnerabilities of their company.

Rebekah Humphrey is a Director at Conning where she is responsible for strategic planning and consulting. Additionally, she provides strategic analysis and produces reports related to the property/casualty insurance industry. Prior to joining Conning in 2014, she was with wealth management firm Gilbert and Timme, LLC. Ms. Humphrey obtained her BA with a dual major in economics and philosophy from Wheaton College (IL) and earned her MA in economics from Trinity College.

Matthew Sternat is a Director on Conning's Insurance Research team, responsible for new business development and client services in insurance industry research and information services. In his earlier role at Conning, Mr. Sternat produced research and strategic studies related to the property/casualty insurance industry. He earned a BS in marketing from Boston College and an MBA from the University of Connecticut.

ABOUT CONNING

Conning (www.conning.com) is a leading investment management firm with a long history of serving the insurance industry. Conning supports institutional investors, including pension plans, with investment solutions and asset management offerings, risk modeling software, and industry research. Founded in 1912, Conning has investment centers in Asia, Europe and North America.

1. Source: Press release, "Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks," November 15, 2018, https://www.marketwatch.com/press-release/opus-ponemon-institute-announce-results-of-2018-third-party-data-risk-study-59-of-companies-experienced-a-third-party-data-breach-yet-only-16-say-they-effectively-mitigate-third-party-risks-2018-11-15

C#: 9040518