PUBLISHED AUGUST 2021

Silent Cyber
CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Silent Cyber

Published August 2021

As cyber risks continue to emerge, insurers are facing losses from unintended coverages, despite explicit coverage of cyber perils in their underlying written policies. With each day, the world faces emerging cyber threats, including infrastructure attacks, identity theft, data breaches, hackers, and malware. This unintentional, non-affirmative coverage—or "silent cyber" risk—can be devastating to insurance and reinsurance companies.

While silent cyber is not a new issue in the property and casualty industry, it has become much more pronounced as businesses continue to be more connected than ever and the frequency of high-profile cyberattacks has increased. For instance, the NotPetya global cyber catastrophe in 2017 resulted in billions of dollars in losses to affected businesses.

Due to the potentially devastating financial impact on the insurance market, global rating agencies and regulators are increasingly scrutinous with regard to the risk of silent cyber and the debilitating effects it could have on an insurer. For example, the insurance credit rating agency AM Best announced it "expects companies to be proactive and forthcoming with their own evaluation and measurement of the exposure and accumulation of their cyber liability exposure."[1] More clarity on coverages (or lack of) would be beneficial for all stakeholders.

A greater concern for insurers is not the affirmative coverage of cyber perils, but the potential silent cyber risk underlying traditional insurance policies. In other words, insurers are concerned about the risk that a cyber event could trigger unexpected payouts under existing policies where the cyber risk was not considered and/or priced.

Wording of policy terms has not evolved at the rapid pace that technology has. This has led to ambiguity as cyber coverage may be available under policies that were not originally designed for this exposure. Businesses have increased their dependency on technology and have welcomed the use of online networks. Although technology increases the efficiency of business operations, there is a trade-off because of the increased exposure to technology misuse, ultimately harming the business and its customers. Many evolving cyberattacks were not even anticipated when the insurance policy forms were written in the pre-digital era.

1 "What is Silent Cyber Risk"; *Insurance Business;* Nov. 26, 2018.

If a policy does not have named perils coverage, there is a potential for coverage for anything not explicitly excluded. Typically, ambiguity in an insurance policy is viewed in favor of the insured, as the carrier is the author of the insurance contract wording and therefore responsible for clarity of coverage. Even policies written to provide affirmative coverage of cyber perils face silent cyber risks. As cybercrimes continue to emerge, the covered perils must keep up.

The systemic nature of cyber risk means silent cyber is becoming prevalent in virtually every type of insurance policy and line of business. Further, cyber attacks do not rely on geographical boundaries, and therefore could be one of the largest sources of accumulation risk in the insurance industry.

Insurers in the global insurance market have made initiatives to begin the "affirmation" process of cyber risk. Affirmative cyber coverage is expanding as the demand for cyber insurance products increase and exposures continue to grow, providing ample opportunities for the market. Further, offering affirmative cyber coverage can incentivize insureds to improve their cyber "hygiene," ultimately reducing losses.

Managing Silent Cyber Exposure

It is difficult for insurers to assess their silent cyber exposures due to the complications surrounding cyber risk. Determining exposure is complicated by ambiguous policy wording, disparate data systems and sources, and the ever-evolving nature of cyber risk. Therefore, the insurers may not have charged adequate premiums to address the extent of their exposure and cover this aspect of the risk. Additionally, given the developing nature of cyber risk and also the development of relatively new insurance products, assessing silent cyber risk requires new skill sets and knowledge for companies and their underwriters.

There are two major aspects of silent cyber risk: unintentional coverage and unpriced coverage.

Unintentional coverage occurs when insurance policy language does not explicitly address the potential for loss caused by a cyber incident or a cyberattack. For example, consider a hypothetical cyberattack that hacked the industrial control system of a dam. Such an attack could result in millions of dollars of property and flood damage covered by the policy language where flood is the covered cause of loss. In this example, many lines of business covering the dam and its operator could have potential exposure to silent cyber losses due to unintentional coverage. In today's connected world, even many cars and homes have significant cyber exposure.

Coverage that is extended without having been initially incorporated into its pricing occurs when there is no adjustment made to the policy pricing to account for the potential unintentional cyber risks or cyber risks that were assumed to be very insignificant. In the dam flooding example, there would be unpriced coverage if the pricing did not consider the potential rise of frequency and severity of floods due to third-party liability resulting from cyberattacks. Over time, pricing would respond to cyber claim emergence regardless of the original recognition of the coverage. That is, the cyber claims will drive up the price of the policies.

To manage risks, insurers typically review their policy forms continuously and carefully for all lines of business. It is also an important consideration of how policies written coordinate with the reinsurance coverage purchased by the insurer for these potential cyber losses. For example, do the insurer's reinsurance policies exclude losses caused by a cyberattack? If so, the insurer could face a catastrophic loss due to lack of protection. The previous example of the flood damage caused by the cyber attack on the dam raises the question of whether the policy should explicitly list or exclude cyber as a named peril.

One aspect of silent cyber risk is an expectation gap between an insurer and the insured on coverage written in the traditional lines that do not explicitly include or exclude cyber risk. Due to this misperception of coverage, there may be increased friction and legal action against the (re)insurers. Further, when ambiguous policy wording exists, some court rulings have favored the insured, and therefore the potential legal judgments could add to the costs of silent cyber risk.

After their first unintended cyber claim payment, some insurers might either exclude or sub-limit cyber risk from new standard policies and renewals. Granting affirmative full cyber limit coverage for an additional premium in such legacy policies has not been common and has developed slowly. By observation of some large insurance companies, the 2017 total amount of cyber-related business interruption claim payments were greater under property insurance policies than under stand-alone cyber policies or an endorsement.[2] To limit silent cyber exposure, companies can either explicitly exclude it from policies, or offer a cyber standalone policy (or an endorsement). These actions may take several years as companies adjust underwriting and policy forms but is an essential element for creating clarity, ending the ambiguity around the coverage, and helping insurers best manage their exposure.

In a competitive insurance market environment, it can be difficult for insurers to address silent cyber, as they have concerns over losing business to their competitors. Despite this fact, several participants in the marketplace have taken strides to address their silent cyber exposures. In July 2019, Lloyd's of London unveiled a plan ordering its syndicates to explicitly affirm or exclude cyber coverage to avoid any silent cyber complications. The Lloyd's mandate was phased and aimed to address all policy types by July 2021.[3]

In January 2018, Insurance Services Offices (ISO) of Verisk Analytics introduced standardized cyber insurance forms.[4] Further, major market participants have moved to address silent cyber. In 2019, AIG stated that it will begin to account for silent cyber by affirmatively covering or excluding cyber risk in virtually all of its commercial property or casualty policies by 2020.[5] These changes require great effort, and it may take time for other carriers to follow suit.

Challenges to Quantifying Silent Cyber

There are challenges in changing policy language and coverage issues to address pricing silent cyber risk. Because cyber risks are expanding and evolving at a rapid pace, it is difficult to expect or predict what future types of losses and claims may look like. Anyone with a computer, time, and creativity could cause trouble. There are many cyberattack software tools available for sale on the "dark web." Every individual and entity that engages the internet must be careful about their online security and behavior. A simple lapse in judgment or protocol in place for company employees could cause a major data breach,

2 "Future of Insurance to Address Cyber Perils"; *Insurance Thought Leadership*; Oct. 31, 2018.
3 *Recent Clarifications in Traditional Insurance Lines*; Marsh JLT Specialty; June 2020.
4 "ISO's New Cyber Insurance Program Implemented in 42 States and U.S. Territories"; Verisk; March 19, 2018.
5 "AIG to affirm or exclude cyber cover in P&C policies from January 2020"; *Commercial Risk*; Sept. 6, 2019.

releasing personal consumer information or critical internal company information and create consequential catastrophic business interruption and losses. Further, a loss could occur if the protocols were in place, as cybercrimes are becoming more and more sophisticated and far-reaching. Continuous surveillance of potential targets and vulnerabilities, rigorous security measures and protocols, monitoring, and a reactive plan and practice can all help lower the risk and reduce possible consequences.

Cyber risk assessment requires data that is not typically collected in traditional property and casualty insurance exposure datasets. For example, underwriting for medium and small policies typically follow a very streamlined process. To address the complexity of the issues and to attempt to quantify the silent cyber risk, collective expertise from various perspectives such as underwriting, actuarial, claims, risk engineering, and information technology (IT) experts is needed. During the insurance underwriting process, it would be optimal to collect information regarding an insured's website and any supply chain dependencies they have. When underwriting a risk, an insurer would typically learn more about the insured's cybersecurity strength and effectively communicate this to the pricing actuaries. If an insurer were to specifically exclude cyber perils from their policies, an insured might need to request an endorsement for cyber coverage. This method would trigger a more thorough underwriting process because the underwriters will need to explore the insured's cyber exposure.

Insurers typically do not have sufficient historical data to accurately forecast their future silent cyber risk exposures and price appropriately. To date, there have been a handful of catastrophic cyber events, each impacting millions of individuals or hundreds of businesses simultaneously. To review silent cyber exposure, insurance companies can start by compiling their exposure data from various policy forms and systems supporting all their lines of business. This can be a daunting task, as many questions need to be answered during this process, such as determining whether all policy limits are exposed and how policies with exclusions and sub-limits are treated.

With some basic information, insurance companies can set a tolerance level for silent cyber risk based on the line of business' earnings and surplus. To quantify the silent cyber exposure, insurers can determine the range of potential exposures that could result from a cyber event and then overlay those exposures with their existing insurance portfolio. A number of vendors have also developed software for assessment of some cyber risks, which may add additional insight.

A major struggle is the lack of statistically significant actuarial data to model risk. Many property and casualty coverages have experienced vulnerabilities. For example, if a business is located in the U.S. Gulf Coast, there is significant and measurable hurricane risk. Cyber perils, however, do not have physical constraints, and businesses can be impacted on a global basis overnight. The lack of boundaries on a cyber peril loss can ultimately lead to large accumulation risk across all policy types.

Normally, data modelers and carriers rely on historical data; however, quantifying cyber exposure is a *forward*-looking exercise. Many losses that may have been cyber-related may not have been previously identified as such or coded as a cyber peril in the data. Therefore, there is a compounding effect of both the lack of data and the historical data not being indicative of the future silent cyber risks as technology is rapidly evolving. The immaturity of silent cyber risk makes it even more difficult for insurers to quantify their risks.

It is also difficult for insurers to compare the reasonability of modeled results for silent cyber against actual claims experience because this is not generally recorded. In the absence of data, determining the potential scale of cyber losses requires a large element of judgment. Another implication affecting consideration of silent cyber is legal judgments. It can be difficult to assess how decisions might determine the extent of coverage under non-affirmative policy wordings. Lastly, keeping models up to date in such a rapidly evolving claims environment represents a major challenge. For some carriers, a handful of legal claims could drive the loss ratio. This has a potential to create a lack of credibility for analyzing the experience.

Conclusion

Ultimately, the way to address silent cyber risk is to examine the ambiguities and provide affirmative and specifically priced cyber coverage. In some lines of insurance business, at least initially, there may be explicit exclusions. Many cyber experts view future cyber catastrophes that have a much larger and more significant ramifications than what has been experienced so far as not "if" but "when." As cybercrimes continue to escalate, the availability of more claims data will allow the production of more sophisticated models to help insurers and reinsurers better understand the possibilities presented by cyber as an insurance product and the risks posed by cyber as a peril. In most developed global markets, cyber insurance will become one of the key growth areas for insurers over the next decade.

While the time to achieve public attribution associated with significant cyberattacks from governments has been decreasing—as seen with the Solar Winds' Orion, Colonial Pipeline, and JBS cyberattacks—Wannacry and NotPetya each took months of investigation before public attribution from the United States and United Kingdom. In that timeframe, cyber claims may have been paid out, but the insurer may have wanted to or still want to invoke exclusions or deny the claim as a result of the findings from the public attribution. Additionally, the choice to invoke such exclusions creates uncertainty in the courts when it comes to whose evidence and definitions will be the primary evidence around the attribution. The incidents in Table 2 are examples with press releases and quotes from government officials, but there is very little information provided as to how those conclusions were arrived at.

Actuaries and the War Exclusion / Cyberterrorism

These coverage clauses and endorsements will be increasingly important for all stakeholders and for actuaries practicing in the cyber insurance space as the impact of potential systemic, war-related, and military-related cyber incidents will influence both the pricing and reserving of losses falling under cyber policies. When these unique events cross the line from cyberterrorism to acts of war and invoke exclusions under the policies, they will likely be litigated in the courts, as is the case in the *Mondelez International, Inc. v. Zurich American Insurance Company* property insurance suit. The uncertainty around payouts associated with these litigated coverage cases will add complexity to the overall reserving process. Further, actuaries would do well to have a clear understanding of the types of cyber event scenarios to exclude from their pricing analyses if the cyber incidents are outside of the purview of the written cyber policy based on the policy wording.

Over time, greater clarity from the cyber insurance industry around the ambiguities noted above is essential. In the interim, it is important that actuaries working in the cyber insurance space be aware of the nuances and uncertainties created by these coverage conditions and the nature of cyber incidents.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**