Silent Cyber.

Threat or Opportunity

How Silent Cyber became a leading risk, and how insurers can reduce exposure.

Silent Cyber Defined

"Silent cyber" is the most talked about new term in global commercial insurance. In the past year, every major insurance periodical, reinsurer, and broker has commented upon its existence. But while many have articulated the dangers silent cyber presents, few have presented a prescription for solving its challenges. In this review, we'll attempt to demonstrate a way forward for primary insurers and reinsurers to manage this complex threat.

To discuss those opportunities we must first understand the problem. What is silent cyber risk?

Silent cyber is the possibility that an insurer of a non-cyber insurance policy will assume risk triggered by a cyber peril such as a ransomware attack, denial-of-service attack, or data breach that would otherwise be insured under a full cyber insurance policy. Importantly, the policy in question must be silent about cyber: neither mentioning cyber risk nor excluding it. The policy must also cover damage to property, business interruption and/or insure liability exposures that might be triggered by other perils. It is these coverages, combined with omittance of cyberspecific language, that produce the conditions for silent cyber risk.

Silent Cyber Bites Insurers

With that basic definition in mind, it will be illustrative to look at how the insurance industry has responded to cyber risk to date.

The first cyber insurance policies, issued in the 1990's, were limited in scope. Over time, as new risks emerged and demand for insurance grew, insurers offered increasingly complex insurance policies. That expansion of coverage allowed insurers of other traditional commercial Property & Casualty (P&C) insurance policies to remain silent, hoping that cyber policies would come to the rescue if there were claims.

The mode of complacency was shaken in 2017, when a series of attacks on major global businesses rocked the insurance industry. The NotPetya and WannaCry ransomware viruses affected large, global businesses like FedEx, Merck, Mondelez, WPP, and Maersk, among others. In each case costs ran to tens or hundreds of millions of dollars. At the high end, total losses for some companies were reported to have exceeded $1 billion.

Costs were driven not only by direct damage, such as infected computer hardware, but also business interruption losses. Property/Business Interruption insurers covering the affected companies likely did not underwrite cyber risk under their policies, nor did they charge an explicit premium for the risk. Alarm bells began sounding in insurer board rooms across the world.

First Party Cyber Perils/Exposures	Third Party Cyber Perils/Exposures
Damage or Loss of Electronic Data	Release of Confidential Data of Others
Ransomware/Damage to Computers	Network Security & Privacy
Phishing/Social Engineering/Funds Transfer	Libel, Slander arising out of Release of Data and Media Materials
Business Interruption/ Contingent Business Interruption	Fines and Penalties of Regulators as a Result of Lost Laptops or Data
Loss of Trade Secrets stored Electronically	Products Liabilityfrom an IoT Device
Diversion of Goods by Electronic Methods	PCI-DSS Assessment Expenses, Fines and Penalties
System Failure arising from an Unplanned Network Outage	Breach Notification and Incident Response Costs arising from Contractual Obligations

Litigation and Dispute

With ambiguity about cyber taking many possible forms in different commercial insurance policies, there are equally numerous ways in which policyholders and insurers can come into conflict in the claims process.

In the highest profile examples stemming from the NotPetya attacks, victims including Mondelez International, DLA Piper, and Merck have had, or hinted at the possibility of having, claims denied in non-cyber policies. Merck received payment from claims under its affirmative cyber policy worth a small fraction of its total losses from the incident, but is reported to have over $1 billion of coverage in a property tower that it may claim.[1] This would almost certainly set off a complicated dispute, with different policy wordings throughout the coverage tower. DLA is currently in a dispute with Hiscox over the denial of a claim under its general insurance policy after the NotPetya attacks.[2]

In the most visible dispute yet, Mondelez had a substantial property insurance claim denied by its insurer, Zurich, under the policy's "war exclusion" clause, since the attacks were purported to be linked to Russian government-backed operatives.[3] Observed together these disputes show that even a single cyber attack has the potential to ripple through the insurance industry in ways few could have expected. The invocation of the war exclusion by Zurich was called "unprecedented.[4]" More such unusual disputes are likely as long as non-affirmative cyber coverage persists. It's reported that in addition to property and BI claims, "claims under errors and omissions, and also kidnap and ransom policies" have been made stemming from the NotPetya attacks.[5]

And while it's the global, nation-state-backed attacks that frequent the headlines, the impact of silent cyber is felt after individual attacks, too -- and in no less devastating fashion for the victims. In recent one case involving a hotel and resort company that was hacked and had customer data stolen, the company's claim under their commercial general liability policy was denied.[6] The insurer, St. Paul Fire & Marine Insurance Co., cited that the policy covers only losses due to first-party damages, such as an employee accidentally divulging information, not those due to a third-party attacker. A similar case involving Sony and Zurich was decided nearly ten years ago.[7]

Other cases involving CGL and property policies range from a grocery store's dispute over whether its customers' credit cards constitute property to a healthcare solutions company successful argument that exposed medical records were "publicized," and thus covered under its policy, even though no third party was known to have accessed the records.[8]

Disputes like these have been reported because of litigation or disclosures by the attack victims to their shareholders in the case of public companies. Many others are likely to have been settled out of court. The problem is pervasive. Yet strong industry-wide action has been slow to develop.

Standard Insurance Type	Silent Cyber Risk not Excluded
Property Insurance	Ransomware/Damage to Data
Business Interruption	Disruption of Delivery of Services, Goods
General Liability	Defamation, Libel, Trade Secret Loss
Cargo Insurance	Electronic Diversion of Goods to Thieves
Products Liability	IoT-based Disruption of Medical Devices, Self-Driving Cars
Crime Insurance	Phishing, Social Engineering, and Electronic Transfer
Directors & Officers Liability	Class Action Lawsuits Alleging Failure to Manage Cyber Risk Properly
Employment Practices Liability	Electronic Loss of Personnel Records Indicating Discrimination, Harassment

1. "JLT wins Merck as NotPetya cyber dispute uncertainty continues." Reinsurance. October 29, 2018.
2. Cyber Security Source Staff. "Update. DLA Piper insurance dispute - 'nothing to do with war exclusion.'" The Cyber Security Source. March 28. 2019.
3. Darlington, Olivia and Felix Zimmerman. "Extent of cover for 'silent cyber' losses - a novel approach." Simmons & Simmons Elexica. January 15, 2019.
4. Ralph, Oliver and Robert Armstrong. "Mondelez sues Zurich in test for cyber hack insurance." Financial Times. January 9, 2019.

Another Act in a Bad Storyline (For Now)

The commercial insurance industry has seen this play before. In the past fifty years, it has seen numerous unexpected mass claims. The list is like a business conduct dishonor roll: asbestos, employment practices, lead paint, sexual predation. All have cost insurers billions of dollars without any premium having been explicitly charged or paid.

Just like with prior claim trends, this cyber risk is very visible, but market dynamics discourage strong action. Insurers worry that if they are the first to put cyber exclusions on their policies they will lose large parts of their business to insurers who take no action. No business or organization wants to buy a policy with a cyber exclusion when all the other insurers may still offer coverage because they are silent about cyber risk. And insurance brokers, in doing their best to help their clients, are quick to point out these differences, making the market very efficient.

So in the face of great uncertainties around silent cyber risk insurers have for the most part done nothing. Most policies still are still silent.

Change is on the horizon, though. Recently, the Prudential Regulation Authority (PRA), the UK's insurance regulator, took a strong position on silent cyber, effectively upping the ante for all insurers. Their statement, issued in January 2019, demands that insurers "develop an action plan by H1 2019 with clear milestones and dates by which action will be taken" to reduce the unintended exposure to non-affirmative cyber risk. The pressure is on. And the PRA does not just impact UK companies — it also regulates Lloyd's of London, the hub of global reinsurance. Through Lloyd's, the PRA position impacts the reinsurance market's largest customer: the $250 billion U.S. Commercial P&C Insurance industry.

"So in the face of great uncertainties around silent cyber risk insurers have for the most part done nothing. Most policies are still silent."

What Can Insurers Do?

With silent cyber risk looming ever larger and regulatory change on the horizon, inaction will cease to be a feasible option for the industry.

One possibility for insurers is to simply underwrite the silent cyber risks and charge appropriate premiums. The industry has already coined a term of art for this avenue: "affirmative cyber." While underwriting the risk is the most logical response, there are at least three distinct problems facing large incumbent insurers. First, not all commercial insurers underwrite cyber insurance directly. They may not offer a stand-alone cyber insurance policy or know how to underwrite the risk — that makes tackling silent cyber a non-starter. Second, offering affirmative cyber requires writing mini-policies— endorsements to the current major insurance policy categories shown in the table on the previous page — all of which requires immense legal and

5. Evans, Steve. "Petya cyber industry loss passes $3bn driven by Merck & silent cyber: PCS." Reinsurance News. November 7, 2018.
6. Schiavone, Joseph, Vincent Proto, Lori Zeglarski, and Robert Vacchiano. "Cyber Insurance Update: Recent Developments in Coverage for Cyber Claims." New Jersey Law Journal. November 30, 2018.
7. Farrell, Emily MacDonald and Ralph P. Raphael. "Insurance Coverage Issues Created by The Internet." Lexis Practice Advisor Journal. February 28. 2019.
8. Ibid.

regulatory scrutiny.

Third, bringing these solutions to market will be a huge endeavour for P&C insurers because of the manner in which they organize themselves. P&C insurers build towers of authority and business acumen based on the type of insurance policy: departments for Property Insurance, Products Liability Insurance and so on. Each of these units has their own piece of cyber risk, and would require a unique approach to cyber underwriting. But they are rarely staffed with cyber underwriters. The ability of these insurers to cross-institutionalize their know-how will be a huge test.

It's easy to see why silence has been the most attractive option.

None of these challenges is insurmountable, but putting effort behind traditional underwriting practices will not be enough. Carriers need a scalable solution to underwriting cyber risk, and that means automation. As technical as it sounds, there are already solutions available from a number of InsurTech-based cyber underwriters that use digital inspections and data sets in order to underwrite what is, essentially, digital risk.

Cyber underwriters, like Corvus, have developed software and artificial intelligence that examines independent data sets and scans IT Security assets of an organization. These processes do not require permission, nor are they invasive. While they cannot view through firewalls, the scans can assess an organization's IT security the same way that the "bad guys" do — looking for out-of-date software, specific threat intelligence, information on sale on the dark web, and much more. From this information, it is possible to develop a "score" for cyber risk in a more objective manner than can be achieved by the traditional method of long questionnaires with answers that are frequently inaccurate and out-of-date.

The scope of what can be assessed through these means is ever-growing. The use of artificial intelligence is increasing the precision of these scans and thereby enhancing their value for underwriting. In the coming years we will see more advanced capabilities leading to faster and more accurate underwriting, enabling insurers to incorporate the information they get from scans into the development of affirmative cyber language for commercial policies like Property, Products Liability, Crime Insurance, and Cargo Insurance.

Put briefly, the solution for insuring digital risks is to use digital tools. Software makes assessments of a company's risk scalable for millions of accounts and helps underwriters in allied product lines to become confident in their assessment of cyber risk.

While the specter of silent cyber risk will continue to haunt commercial lines, insurers can significantly reduce their exposure to silent cyber by affirming as much risk as possible with the aid of InsurTech tools.

"Putting effort behind traditional underwriting practices will not be enough. Carriers need a scalable solution to underwriting cyber risk."

To learn about Corvus Smart Cyber Insurance™ policies, contact Mike Karbassi, Head of Cyber Underwriting:
MKarbassi@corvusinsurance.com | (617) 564-1595