Kelly Castriotta, managing director and global cyber underwriting executive at Markel

Vigilance Demanded

The lack of specificity in commercial insurance policies as they relate to damage from cyber crimes is still too prevalent. Brokers, insureds and their carriers face a mandate to communicate clearly and craft appropriate coverage. By Alex Wright

When traditional property and liability policies were first set up, they were designed to explicitly cover only those exposures.

But as a result of technological advances, a new risk has come to the fore: cyber. It affects every business, large or small, and ranges from ransomware attacks to social engineering.

As companies have grown further and faster than before, accelerated by the need to digitize in the wake of the COVID-19 pandemic, so they have left themselves ever-more exposed to cyber threats, which in turn have increased in both severity and frequency.

Added to that, because cyber is a relatively new risk, there's a shortage of accurate historical loss data, meaning it's difficult to assess and price for. Because of its systemic nature, cyber risk can quickly spread to all parts of the business, and it's continually changing, making it even harder to pin down, with a lack of definition around what constitutes specific cyber events such as cyber terrorism, cyber war and even ransomware.

"Cyber risk is present in just about every insurance policy now," said Tracie Grella, AIG's global head of cyber insurance. "But because it hasn't been factored into the underwriting of standard policies such as property, or properly identified, assessed, priced for and put into the aggregation model, it presents a huge systemic risk that can't simply be ignored."

The issue has been exacerbated by the introduction of a host of new data protection laws such as the European Union's General Data Protection Regulation, the Illinois Biometric Information Privacy Act and the California Consumer Privacy Act, as well as tighter monitoring by ratings agencies. This has put additional strain on both insurers and their policyholders to strictly adhere to these new requirements.

Silent cyber, in which particulars of cyber coverage are not specifically mentioned in policies, first manifested in the WannaCry, Petya and NotPetya cyber attacks of 2017, which devastated everything from shipping ports and supermarkets to advertising agencies and law firms. The resulting losses from the encryption of master files and subsequent Bitcoin ransom demands for restoring access were the costliest on record, surpassing $3 billion.

Since then, there have been multiple arising coverage disputes, most notably the case of U.S. food company Mondelez, which sued its insurer Zurich, alleging it was wrongfully denied a claim under its property policy for losses sustained in the NotPetya attack. However, the argument for silent cyber coverage was undermined by a war exclusion clause.

"Cyber risk has implications across the board," said Rich Sheinis, data privacy and cyber security partner at Hall Booth Smith, P.C.

"When a client suffers an event, whether that be a ransomware attack or a business email compromise, often their policy isn't geared up to deal with the potential losses they will incur, and there's a disconnect between what their policy actually covers them for and the appropriate coverage they would need."

Despite the introduction of specific cyber policies to cover the risk, many insureds still expect to be covered under their property and liability policies — and yet, they are not. This phenomenon is known as silent cyber or non-affirmative cyber: Where potential cyber-related events or losses are not expressly covered or excluded within traditional policies.

Therefore, carriers may end up having to pay arising claims that were both unexpected and not priced for properly. Because of the confusion around coverage, policyholders also run the risk of having unexpected coverage gaps.

As a result, the insurance industry, led by Lloyd's of London, has taken the position that all property and casualty (P&C) policies must now either implicitly exclude or include cyber coverage, with the mandate coming into force at the start of 2020. The New York State Department of Financial Services' cyber security insurance risk framework, announced in February this year, is expected to have a similar effect on U.S. insurers.

"From a broker standpoint, failure to have clarity on cyber risk within policies can cause coverage disparity over what events are and aren't covered," said Kelly Castriotta, managing director and global cyber underwriting executive at Markel.

"For insurers, it can cause accumulated losses not necessarily priced for, and for the policyholder, they may not have the right coverage to offset the operational disruption as well as the physical damages and losses caused by a cyber event."

To be prepared for a cyber event, underwriters and insureds need to understand how ever-evolving risks and legal frameworks will affect their policies. They also need to keep themselves appraised of the scale of the problem and understand the the most common misconceptions and coverage disputes around silent cyber.

SILENT CYBER: A TOP-TIER CONCERN

Failure to craft appropriate, understandable policies should be considered a threat just as dire as the ransomware attacks themselves.

"Silent cyber remains a top-tier concern for the insurance market, on a par with the ransomware epidemic," said Michael Phillips, chief claims officer at Resilience. "This has been driven by the rapid growth in technology and the race to digitization. At the same time, the insurance industry is rushing to keep pace, both in understanding clients' risks and making sure they know exactly what product they are buying. The stakes are higher than ever before, and that's why insurers and underwriters need to have a handle on the problem."

One of the biggest misconceptions is that companies wrongly assume their property, commercial general liability or employment practices liability policies will protect them from cyber events or losses, specifically where it relates to property damage, bodily injury or business interruption.

Others simply don't understand what a cyber policy covers.

"Many companies haven't purchased cyber insurance, because they don't understand what they would be covered for under it," said Elisabeth Case, a managing director in Marsh's cyber practice. "Another problem is that they don't know how such a policy would apply to their particular exposure or situation, so when they get hit with a ransomware attack, for example, they turn to their traditional policies, which were never intended to cover those risks in the first place."

The most common disputes arise from phishing or social engineering scams, where a company or its client is deceived into sending money to a criminal enterprise. Often because the insured doesn't have a specific cyber policy, though, they won't be covered.

"In a best-case scenario, a cyber incident may trigger coverage under multiple insurance policies and increase the available total limit

SUMMARY

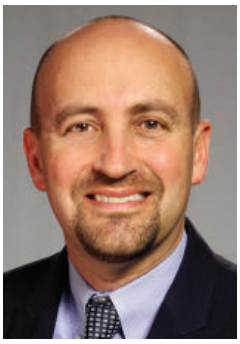
- ***Despite the prevalence*** of cyber threats, directors, officers and C-suite executives are still too much in the dark on the impact of silent cyber in their policies.
- ***With Lloyd's leading*** the charge, insurers are increasingly excluding cyber from property and other policies.
- ***The overall field*** of cyber threats, including ransomware, continues to expand and multiply.

to respond to a covered event," said Adam Lantrip, CAC Specialty's cyber practice leader. "In a more common scenario, multiple insurance policies may be triggered but not coordinate with one another, and the policyholder spends more on legal fees than the cost of having purchased standalone cyber insurance in the first place."

Other disputes range from physical damage caused to computers by cyber attacks to data being stolen and then published, said John Farley, managing director of Gallagher's retail brokerage cyber practice. They extend as far as kidnap and ransom too, he said.

"We've seen coverage disputes arise from kidnap and ransom policyholders that suffered ransomware attacks," said Farley. "Those policyholders argued the kidnap and ransom policy language was not specific enough to limit coverage to people held hostage and pushed for coverage for extortion payments made to hackers for their data that was held hostage."

Another issue is that policy language around cyber isn't standardized. That can lead to big discrepancies between not only different insurers but also



"Today, the focus is clearly on cyber extortion and business interruption. Markets will likely continue to respond to these new cyber exposures by further honing the cyber exclusions on their policies to limit their silent cyber exposure."

— Jason Krauss, *cyber/E&O thought and product leader, Willis Towers Watson*

activity, many insurance companies are striving to eliminate silent cyber using endorsements or modified policy wordings to either limit or fully exclude coverage for cyber events."

Lloyd's has led the charge on this front, with the Lloyd's Market Association and the International Underwriting Association at the fore.

Since issuing its first marketing bulletin in 2019 mandating that all policies need to be clear on whether coverage is provided for losses caused by a cyber event, a host of new clauses have been added, requiring syndicates

"Many companies haven't purchased cyber insurance, because they don't understand what they would be covered for under it. Another problem is that they don't know how such a policy would apply to their particular exposure or situation."

— Elisabeth Case, *managing director, cyber practice, Marsh*

individual policies within their books of business.

"The language in insurance policies continues to evolve," Castriotta said. "The problem is that it isn't standardized in the U.S. market, so it requires expert brokers to ensure that the policy meets the needs of the client but also gives a clear statement on cyber coverage and whether it's affirmative or not."

CYBER EXCLUSIONS

Underwriters have responded to the issue by expressly excluding cyber from traditional coverages to avoid any ambiguity. This has already had a significant effect, particularly in property.

"From a property policy perspective, silent cyber is quickly disappearing with the introduction of cyber exclusions," said Darin McMullen, Aon's E&O/cyber product leader. "Given increased cyber loss

to expressly include or exclude cyber as a coverage, and many non-Lloyd's insurers are following suit.

"This approach allows insurance companies to manage accumulation risk much better, which results in better underwriting and avoids unforeseen losses," said Anthony Dagostino, Lockton's cyber practice lead. "Unfortunately, for the policyholder, it also sometimes results in less coverage available for cyber perils, especially in insurance lines like property and stock throughput."

Andrew Lipton, vice president, head of cyber claims at AmTrust Financial, said: "Expressly excluding cyber on non-cyber policies is a good step towards making sure that both insurer and insured understand each other's expectations of coverage. When insureds have expectations of cyber cover on an arguably non-cyber product and the insurer has not expressly excluded cyber cover, this is where the potential friction on this issue can start, which is something that all insurers, brokers and customers would like to avoid."

A sticking point remains, however, that silent cyber isn't on the agenda of many company boards, according to Grella. Failure to evaluate the risk, she said, can have far-reaching consequences.

"As a risk, silent cyber still isn't on the radar of most organizations," Grella said. "The problem is that they aren't assessing the risk and working out where their exposures are, how their policies will respond and whether they would be covered for an event."

Moving forward, one of the biggest problems is keeping a policy current to cover the ever-changing strategies of criminals and myriad types of cyber risk. To this end, policyholders need to first assess their cyber as an enterprise-wide risk and map out all possible loss scenarios.

Then they should look at their existing P&C policies, many of which will have become outdated, with their brokers and insurers to determine exactly what they are covered for in terms of grants, limits and retentions, and where coverage gaps exist and plugging them, ensuring that all of their policies are aligned.

It is also preferable to keep all policies under one umbrella with the same carrier that has a specialty in cyber insurance.

THE STANDALONE CYBER SOLUTION

The most comprehensive solution is a standalone cyber policy that covers most foreseeable cyber-related risks, often issued by a boutique insurer or broker. Yet there will always be emerging exposures that haven't been accounted for, particularly with the advent of new technologies such as autonomous vehicles and wearable medical devices.

Even with a cyber policy, however, there can be problems. Number one is the issue of adequacy and amount of coverage, with expenses often running into the millions, and then there is affordability, particularly for more high-risk industries such as health care and education.

"One of the key issues the market is facing is that the limits available on cyber policies are often substantially lower than in other classes of coverage," said Julian Miller, a partner at DAC Beachcroft specializing in cyber.

"The notable comparison is between cyber and property insurance, whereby if they suffer a cyber attack and are majorly impacted and have exhausted their cyber policy, then they will look across all other lines of coverage to see where they can recover the outstanding losses."

Companies also need to examine their cyber security policies and procedures to ensure they are fit-for-purpose and can prevent, withstand and recover from an event. Added to that is the adoption of company-wide risk management practices to mitigate the risk.

"As cyber threats continue to evolve, new cyber coverages come to the forefront," said Jason Krauss, cyber/E&O thought and product leader, Willis Towers Watson. "Today, the focus is clearly on cyber extortion and business interruption. Markets will likely continue to respond to these new cyber exposures by further honing the cyber exclusions on their policies to limit their silent cyber exposure."

Education can play a big part in addressing silent cyber, too.

Libby Benet, global chief underwriting officer for cyber at AXA XL, said: "In our industry, the topic of how a cyber event can give rise to a loss under a traditional policy is not yet widely understood. We have an opportunity to step up and educate underwriters on this topic through internal company training or through professional associations like PLUS or CPCU. We also need to educate risk engineering or risk management about these concepts."

Great strides are being made in defining coverage language . But as cyber continues to evolve as a risk, disputes and misconceptions will only be perpetuated, meaning that all parties need to stay alert to all eventualities. **&**

ALEX WRIGHT is a freelance editor and writer based in the UK. He can be reached at riskletters@theinstitutes.org