Silent cyber's specter is casting a larger shadow on insurers

The new normal for big cyber events mobilizes carriers

By Anthony Dagostino, Jess Fung and Mark Synnott

Anthony Dagostino
specializes in cyber risk mitigation and management.
Willis Towers Watson, New York

Jess Fung
specializes in cyber modeling and analytics.
Willis Re, Seattle

Mark Synnott
specializes in cyber reinsurance.
Willis Re, Chicago

Cyber-related losses are making headlines, reinforcing the need for insurers to prepare as the specter of silent cyber exposure grows. How can insurers manage this new normal?

In 2017, significant cyber events such as the NotPetya malware attack and the Equifax data breach grabbed international headlines and put the spotlight on cybersecurity, just months after Willis Re conducted its first insurance industry survey studying the perceived dangers of silent cyber risk (i.e., coverage under policies not specifically designed to cover cyber).

For insurers, the resultant claims and losses in lines as diverse as property, marine, and directors and officers (D&O) liability have left their mark.

Significant levels of expected cyber-related losses across all five lines of business surveyed (see About the survey, below) were evident in the 2018 Silent Cyber Risk Outlook global survey. Over 60% of respondents say they will likely incur more than one cyber-related loss for every 100 non-cyber covered losses over the next 12 months in *all* lines of business except workers compensation — compared with less than 50% who envisioned this in *any* line of the classes of business surveyed in 2017.

The shift in perceptions over the past year is most pronounced in the other liability line of business. In 2017, only 35% of respondents perceived the silent cyber risk factor as greater than 1.01, but in 2018 this percentage increased to 62%. Of these, close to 30% assigned a risk factor of 1.10 or greater, a figure matched for the property line of business (*Figure 1*, next page). In workers compensation, while the perceived risk level is lower than in the other classes, it has risen nonetheless, with about a third of respondents assigning a silent cyber risk factor of over 1.01.

About the survey

The Willis Re 2018 Silent Cyber Risk Outlook global survey included close to 700 participants from over 100 insurance companies and groups around the world as well as a number of Willis Towers Watson employees. The survey focused on five lines of business. Three repeated from last year: first-party property, other liability (which this year incorporated auto) and workers compensation. Two are new: errors and omissions (E&O) and D&O.

All respondents were asked to assess the extent to which, over the next 12 months, cyber exposure would increase the likelihood of a covered loss. Using a range of responses of 1% or less (no more than one additional cyber-related loss for every 100 non-cyber-related losses) to 100% (an equal balance), these were converted into a silent cyber risk factor — for example, 1.01 or less in the case of one cyber-related loss or fewer per 100, or 1.5, representing 50% more covered losses.

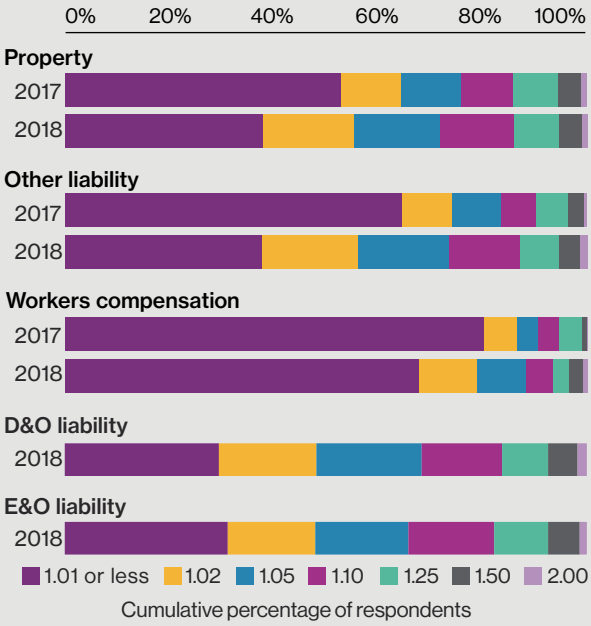
Over 60% of respondents say they will likely incur more than one cyber-related loss for every 100 non-cyber covered losses over the next 12 months in all lines of business except workers compensation.

Variations by industry

The indiscriminate nature and reach of cyberattacks such as WannaCry have also caused insurers to reevaluate their potential liability in different industries. In 2017, a majority of respondents (i.e., over 50%) rated only two of the nine industry groups included in the survey as having a silent cyber risk factor of greater than 1.01 for property coverage, while none of the industries met this threshold in other liability. In 2018, a majority of respondents attached at least that level of risk to all industries in both classes. Furthermore, the largest number of respondents now see other liability posing the biggest silent cyber risk (greater than 1.10) in two industries: hospitals/medical facilities/life sciences and financial services. Over a third of respondents believe the silent cyber risk factor in medical fields is 1.10 or greater, a sharp increase from 19% in 2017. Meanwhile, the perceived threats associated with important infrastructure has meant that the information technology (IT)/utilities/telecom sector continues to be seen as the biggest risk for silent cyber property coverages, with 42% judging the risk factor as 1.10 or higher.

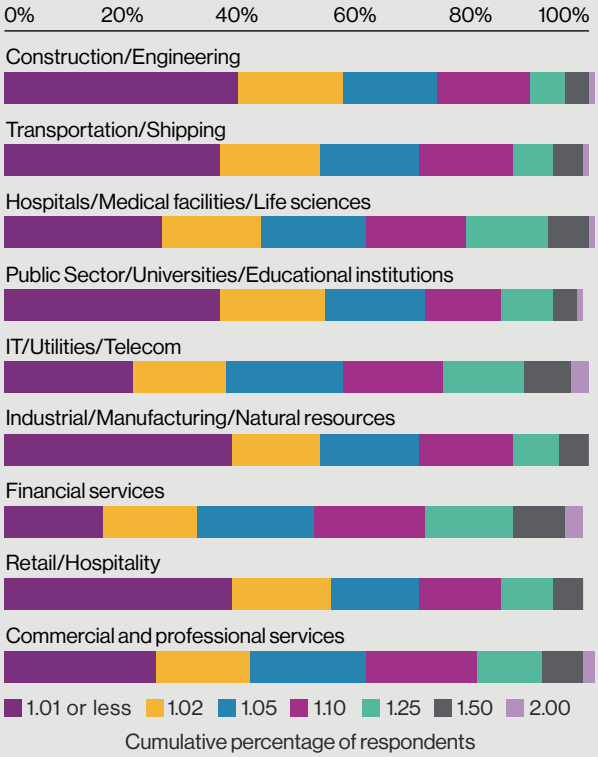
Industry-based risk perceptions in the two new classes added in 2018 — E&O and D&O — were almost universally high: Over 30% of respondents assigned an overall silent cyber risk factor of over 1.10 for both. Forty-four percent of respondents viewed the financial services risk factor for D&O as 1.10 or greater, with IT/utilities/telecom and hospital/medical facilities/life sciences not far behind. In E&O, perceived exposure was even higher *(Figure 2)*. Financial services led the way with 47%, with commercial and professional services joining IT/utilities/telecom and hospital/medical facilities/life sciences at around the 40% mark.

Figure 1. **Silent cyber risk factor by line of business**



Source: Willis Re 2018 Silent Cyber Risk Outlook global survey, willistowerswatson.com/silentcyberrisk2018

Figure 2. **Silent cyber risk factor for 2018 E&O liability by industry**



Source: Willis Re 2018 Silent Cyber Risk Outlook global survey, willistowerswatson.com/silentcyberrisk2018

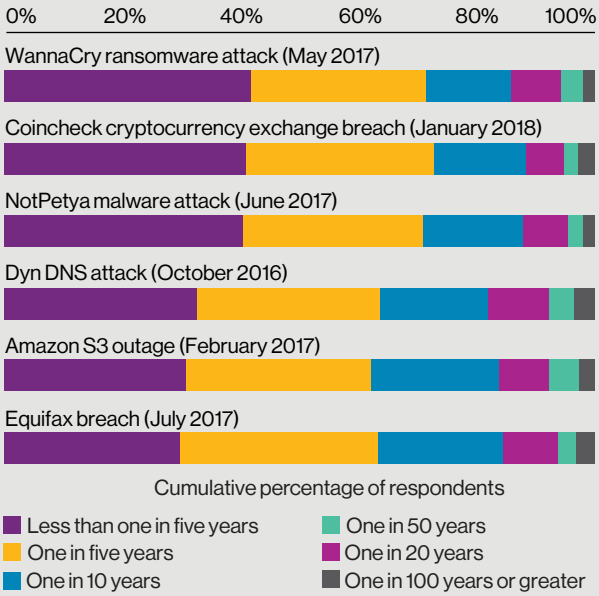
A new normal for cyber events

Recent experience has clearly left many more insurers on their guard, and most don't expect any letup in larger incidents that could test their silent cyber readiness. Between 60% and 70% expect events similar to recent headline losses to occur at least every five years or less *(Figure 3)*.

Further evidence of this apparent new normal comes from a **recent study of cyber resiliency in international businesses** conducted by the Economist Intelligence Unit (EIU) and sponsored by Willis Towers Watson. This found that a third of the companies surveyed had experienced a serious cyber incident — one that had disrupted operations, impaired financials and damaged reputations — in the past year. And significantly, most placed high odds on another one occurring within a year.

Many insurers are wary of the correlation among business lines that can be caused by regular large cyber events. Indeed, it seems quite possible that because of this correlation, a large cyber event could present a greater threat to insurers than, say, a natural catastrophe, which

Figure 3. **Recent cyber event return period**



Source: Willis Re 2018 Silent Cyber Risk Outlook global survey, willistowerswatson.com/silentcyberrisk2018

Many insurers are wary of the correlation among business lines that can be caused by regular large cyber events.

has a limited impact on liability policies. Insurers expect E&O and D&O to have the most significant correlations. There's the potential for an extreme cyber event to result in a simultaneous increase in claim frequency of up to 40%.

How to manage this new normal

What can be done to manage the longer-term threat of silent cyber risks that this new normal brings?

First, insureds can take preventive action to bolster their cyber resilience and minimize the vulnerability to, and impact of, breaches or malicious attacks on their businesses. However, there's both bad and good news.

The worst of the bad news is that, worryingly, the EIU/Willis Towers Watson study found that only 13% of companies rated themselves as good at applying lessons from past security incidents. Linked to this, most of the senior executives questioned also felt they still had a long way to go in filling cyber-talent gaps and in creating a cyber-savvy workforce. As we have frequently argued in the many articles we've written on cyber risk, supported by analysis of our broking clients' claim statistics, the biggest threat to most companies' cybersecurity remains their own employees who can fall prey to lapses such as opening phishing emails.

A recent study by ESI ThoughtLab, and sponsored by organizations including Willis Towers Watson, showed more senior executives coming around to this point of view. Nearly 90% of those surveyed cited untrained staff as their greatest cyber risk, confirming that organizations can do more to ingrain cybersecurity into their cultures. Building on the growing recognition that not all answers to cyberthreats rest with technology, tools such as our own Cyber Risk Profile Diagnostic are helping companies bring a more holistic approach to how they measure their cyber maturity, prioritize areas of vulnerabilities to improve upon and allocate their budget.

Executives don't believe they're spending enough

On the positive side, most senior executives, according to the EIU/Willis Towers Watson study, think the 1.7% average revenue their companies are spending on cybersecurity and cyber resilience isn't enough. Half say that the risk level faced merits spending up to 10% more annually on risk mitigation, while 23% argue the increase in investment needs to be even greater. And high on the list of priorities are training, rewards and incentives that build a stronger internal cyber-resilient culture.

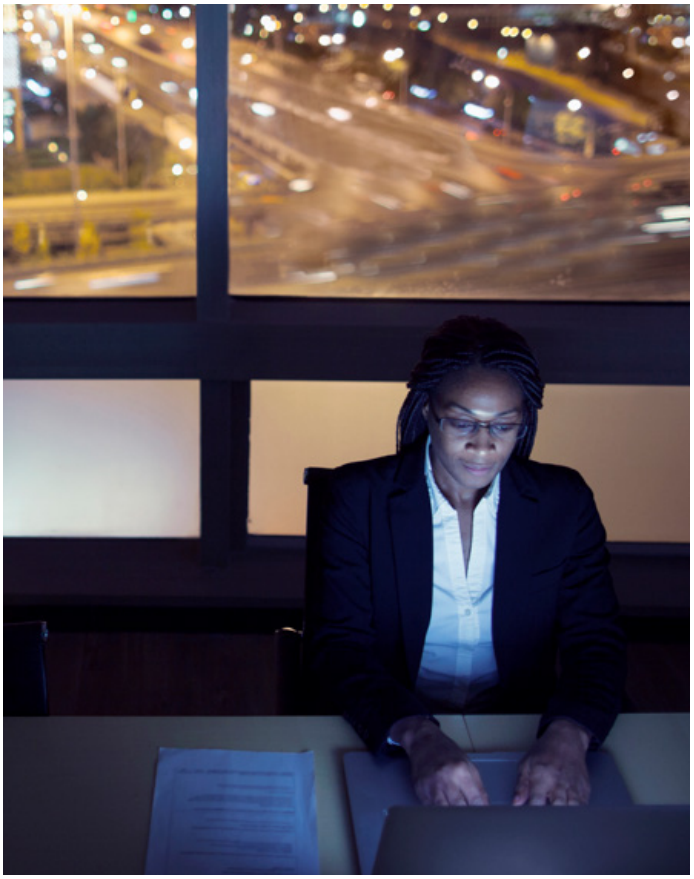
What's galling for insurers is that despite the recent significant growth in availability and take-up of specific cyberinsurance coverage, executives place insurance last among their priorities for additional spending, with an expected allocation of 14%. That said, 14% would still represent a significant sum and may reflect the fact that many larger companies already have cyberinsurance.

Second, regulators may also have a part to play in at least minimizing the potential risk from silent cyber coverage. The Prudential Regulation Authority in the U.K., for example, issued a supervisory statement in July 2017 that laid out expectations for P&C insurers (but not life) to make pricing and exposure adjustments for silent cyber risks to align them with their stated risk appetite.

Three ways to manage silent cyber risk

Finally, here's what insurers can do to manage silent cyber risk. Clearly, one answer is to persuade more organizations to buy more cyberinsurance, regardless of what ambivalence the figures above might suggest. Another is to clarify policy language that was often written in the pre-digital era and is ill-suited to address many of today's cyber-related risks. A third strategy for insurers is to assess the downside risk posed by silent cyber and create transfer facilities to manage the excess risk.

As the industry's experience of the sources and causes of cyber risk further develops, expect more action and initiatives from all dimensions.



PRISM-Re™ is a vital cyber risk tool for our insurance company clients that enables them to manage their cyber portfolios and estimate downside risk arising from privacy breach and network outage following a cyberattack. PRISM-Re now provides insurers with access to stochastic modeling of cyber losses on a worldwide basis, arising from insurance policies not specifically designed to cover cyber risk. The model factors in the likelihood of a silent cyber loss and overlays this against company-specific non-cyber limit profiles and loss severity curves to generate a full loss distribution for silent cyber loss potential in isolation or in conjunction with affirmative cyber loss. For more information, contact Mark Synnott or Jess Fung.

For comments or questions, call or email Anthony Dagostino at +1 212 915 8785, anthony.dagostino@willistowerswatson.com; Jess Fung at +1 206 343 6066, jess.fung@willistowerswatson.com; or Mark Synnott at +1 312 288 7478, mark.synnott@willistowerswatson.com.