Decode cyber risk

2018 Silent Cyber Risk Outlook

Silent cyber risk concerns growing across the board

2018 marks the second year of Willis Re's market survey about silent cyber exposure – potential cyber-related losses due to silent coverage under insurance policies not specifically designed to cover cyber risk. Since our 2017 survey, there have been some headline silent cyber losses in lines as diverse as property, marine, and directors and officers (D&O) arising out of events such as the NotPetya malware attack and the Equifax data breach. How have these events, and an increased awareness of the potential for silent cyber losses, affected market perceptions?

In 2018, our survey sample comprised 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 focus for the survey was five lines of business: first-party property, other liability (which this year incorporated auto), workers compensation (all of which were included in 2017), and two new lines – errors and omissions (E&O) and D&O.

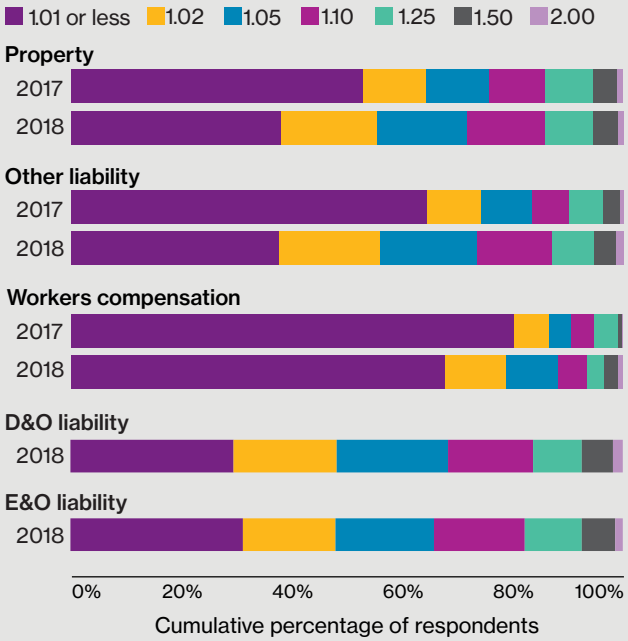
In addition, this year we also asked questions about large cyber loss events, exploring the extent to which respondents think the specified lines of business are correlated in the event of a large cyber event (1:100 or worse) and what return periods respondents would attach to a series of recent cyber events, including NotPetya and Equifax.

What the numbers mean

To recap, we asked all respondents to assess the extent to which, over the next 12 months, the cyber aspect of exposure would increase the likelihood of a covered loss. Based on the available range of responses – <1% (less than one additional cyber-related loss for every 100 non-cyber related losses) to 100% (as many cyber-related losses as non-cyber-related losses) – we then converted these into a silent cyber risk factor (for example, 1.01 or less, indicating one or fewer than one cyber-related loss for every 100 non-cyber-related losses, and 1.5, representing 50% more covered losses).

Willis Re

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



Results by insurance line

The results show that there has been a significant increase in the expected level of cyber-related loss across all lines of business in the past 12 months. As shown in *Figure 1*, where year-on-year comparisons are available, in 2017 less than 50% of respondents estimated the silent cyber risk factor as greater than 1.01 in *any* line of business. By contrast, in 2018 60% – 70% of respondents estimated the silent cyber risk factor as greater than 1.01 in *all* lines of business apart from workers compensation. The contrast is most pronounced in other liability. In 2017, only 35% of respondents perceived the silent cyber risk factor as greater than 1.01 – in 2018 this percentage had increased to 62%. Moreover, close to 30% of respondents for property and other liability, and over 30% of respondents for D&O and E&O viewed the silent cyber risk factor in 2018 as 1.10 or greater. While there remains considerable uncertainty over the potential extent of silent cyber loss activity, as illustrated by the broad range of color bands in Figure 1, it is clear that the market views silent cyber as a more significant threat in 2018 than it did in 2017.

The increased concern might be due to actual large-scale events such as WannaCry and NotPetya, which demonstrated the potential for cyber-related losses in multiple lines of business. It might also be due to a growing appreciation of the insurance-related implications of our reliance on digital technology – a reliance that is only going to increase in the years ahead.

Results by industry group

We also asked respondents to estimate the risk of silent cyber losses in various industry groups. There has been a marked increase in perceived risk across all industry groups – even workers compensation. In 2017, only 17% – 22% of respondents viewed the silent cyber risk factor for workers compensation as greater than 1.01 across the range of industry groups. In 2018, the equivalent range of percentage numbers had increased to 26% – 37%. Still comparatively modest, but a noticeable uptick.

Respondents are more concerned about industry groups in other lines of business, as shown in *Figure 2*, page 3. In 2017, only two industry groups in property (*IT/Utilities/Telecom* and *Financial Services*) and no groups in other liability had over 50% of respondents estimating a silent cyber risk factor of greater than 1.01. In 2018, all nine industry groups in both property and other liability had over 50% of respondents estimating a silent cyber risk factor of greater than 1.01.

In 2017, there was a noticeable difference in the perceived risk of silent cyber between property and other liability, with the former leading the latter in all nine industry groups where the silent cyber risk factor was greater than 1.01. In 2018, this gap has shrunk considerably, with property ahead in six groups and other liability ahead in two groups with one group tied. One possible reason for the closing of this gap between property and other liability might be the range of cyber loss events that occurred in 2017, which may well have increased awareness about the potential for silent cyber losses across both multiple lines of business and industry groups.

In property, *IT/Utilities/Telecom* remains an outlier with 42% of respondents now viewing the silent cyber risk factor as 1.10 or greater, perhaps reflecting continued concerns about threats to utility infrastructure. However, there has been a broad increase in concern about silent cyber exposure in other industry groups which has caused a narrowing of the differential with *IT/Utilities/Telecom*. This might be due to the wide-ranging, almost indiscriminate impact of cyber attacks such as WannaCry

and NotPetya across multiple industry groups. In other liability coverages, respondents viewed all industry groups as higher risk than in 2017, although there was no clear outlier. *Hospitals/ Medical Facilities/Life Sciences* led the way with 34% of respondents now viewing the risk factor as 1.10 or greater, a sharp increase on 2017's figure of 19%. *IT/Utilities/Telecom* and *Financial Services* registered similar percentages, although the increases on 2017 were not quite as marked. Significantly, all three groups represent major repositories of personal information.

Figure 2. **Silent cyber risk factor by industry**

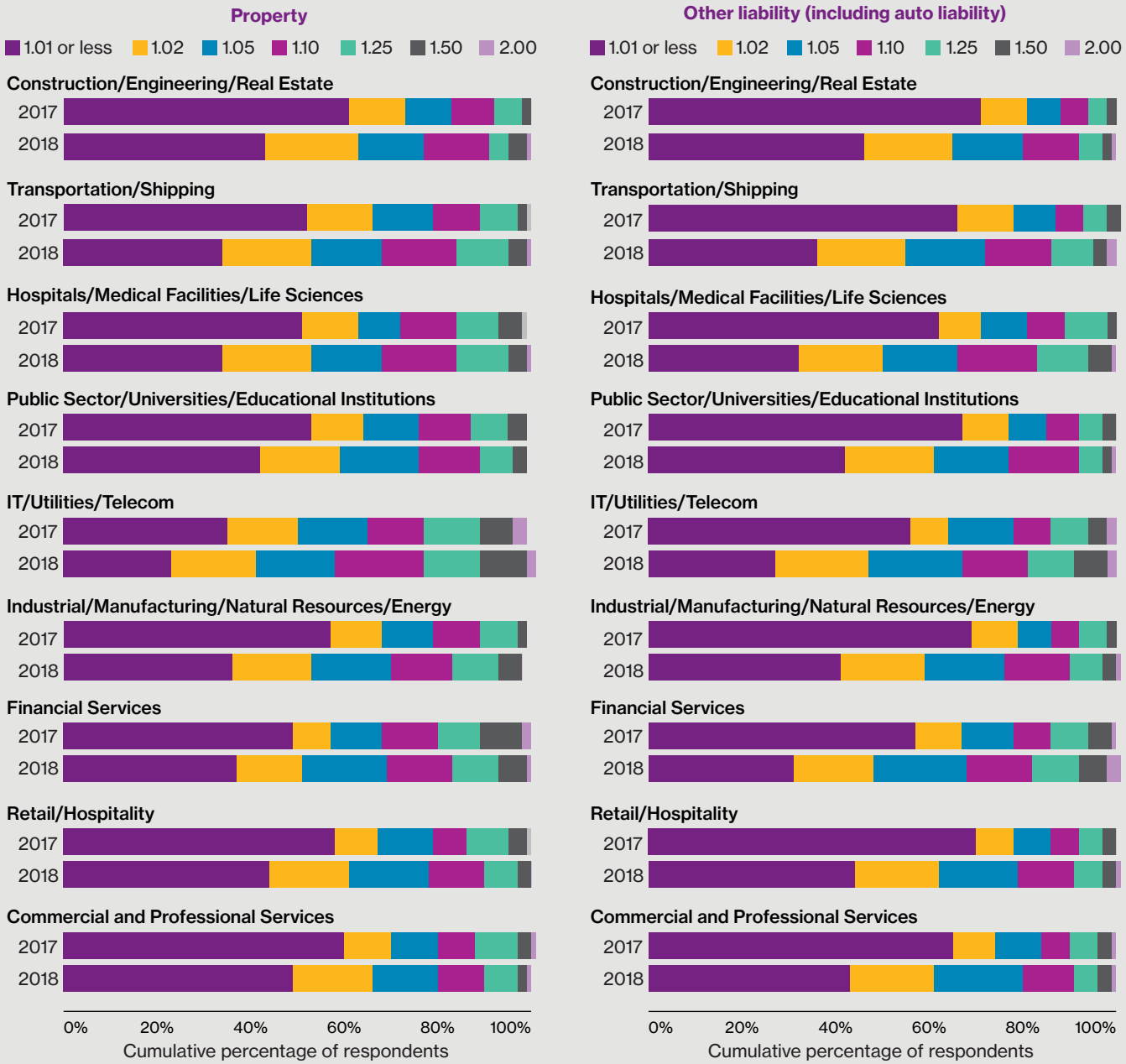
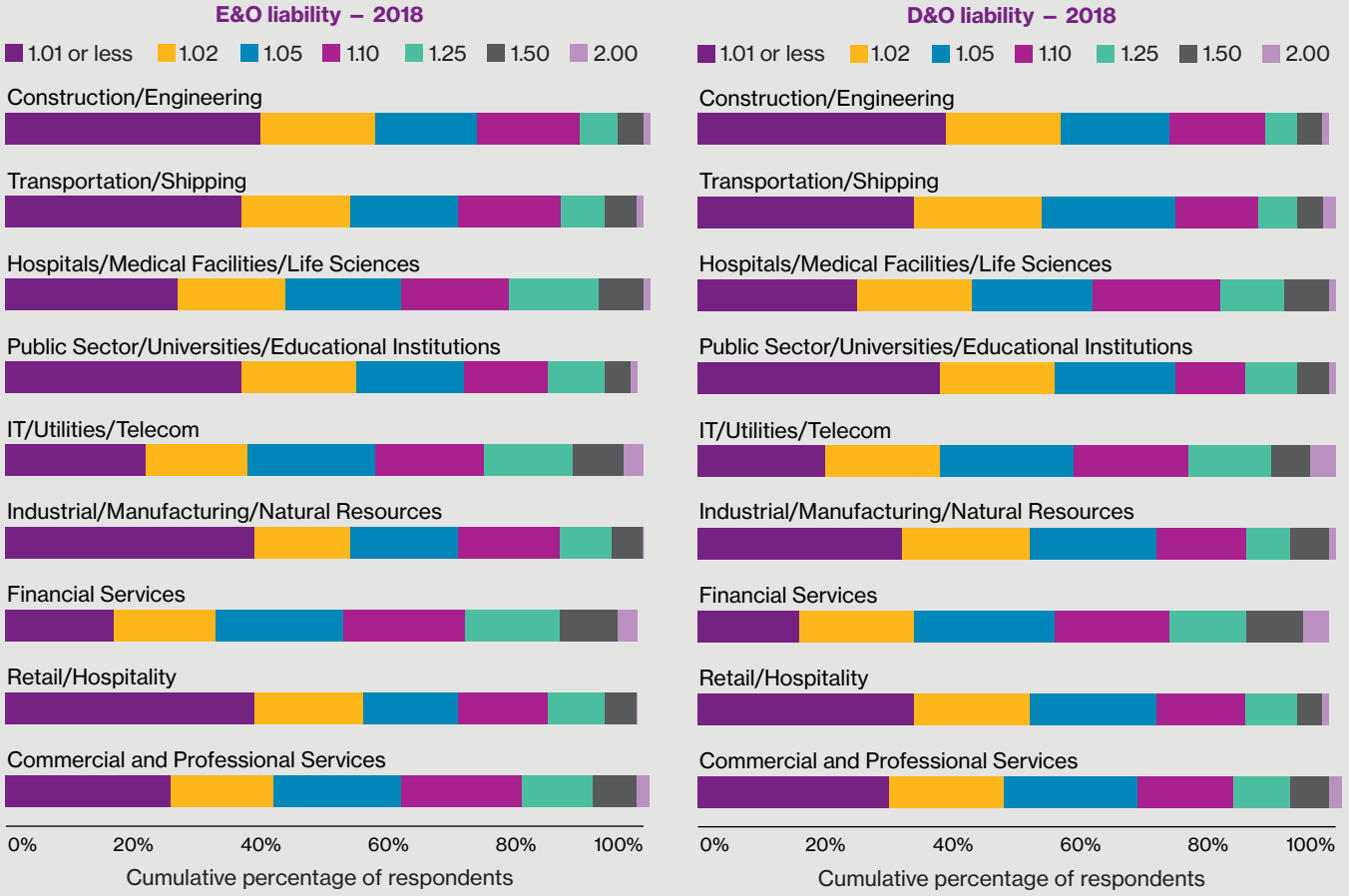


Figure 2. *(cont.)* **Silent cyber risk factor by industry**



Although no figures are available for 2017, perceived exposure in D&O and E&O in 2018 was greater still across the board. 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. *Financial Services* led the way with 47%, with *Commercial and Professional Services* joining *IT/Utilities/Telecom* and *Hospital/Medical Facilities/Life Sciences* around the 40% mark. Concerns about the financial consequences of a major data breach may well underpin these numbers.

Large cyber events

This year we asked two additional questions designed to get a better insight into market perception of the impact of extreme cyber events. The first related to correlation of silent cyber losses and the increase in frequency that might be expected between the specified lines of business in the case of a range of extreme (1:100 year or greater) events. *Figure 3* shows that respondents feel there are varying levels of correlation between lines ranging from a 15% – 20% increase in frequency for workers compensation, to close to 40% for D&O and

Figure 3. **Average claim frequency correlation factor**

	Property	Other liability (including auto)	D&O liability	E&O liability	Workers compensation
Property					
Other liability (including auto)					
D&O liability					
E&O liability					
Workers compensation					

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

E&O. These do not appear to be especially high levels, which might indicate the market is not irrationally concerned about silent cyber. Nor do they seem to us to be low levels. While we aren't aware of any similar studies conducted for extreme natural events such as earthquake or hurricane, we would intuitively expect correlation levels across a property & casualty portfolio to be lower in these events than in a systemic cyber event because of natural catastrophe's more limited impact on liability policies. It might well be that respondents think that between-line correlation will be greater in a cyber event, but not excessively so.

The second question in the survey related to the prospective return period for events similar to a range of recent headline cyber losses. As shown in *Figure 4*, 60% – 70% of respondents view these types of events as having a return period of one in five years or less. Large and/or unusual cyber loss events might therefore be regarded as the new normal rather than the exception.

Survey demographics

As with last year, and as shown in *Figure 5*, we received responses from professionals with a broad range of experience. There was little change in the perceived level of risk from silent cyber by industry experience – more seasoned professionals with a greater first-hand knowledge of unusual or large loss scenarios view the risks posed by silent cyber as similar to those newer to the industry who may be more in touch with new technologies and how they could be used (or misused). As shown in *Figure 6*, respondents with an analytical or risk management background were more likely to view the risks posed by silent cyber a little more benignly than other functional groups. One conclusion is that this group might be more cautious in waiting for actual data before making any broader judgments.

Summary and next steps

It's clear from our 2018 survey results that market concerns about silent cyber are growing across all lines of business and all industry groups. Over the coming months, we will be using the data to update and better parameterize the silent cyber module of our PRISM-Re cyber model that assists Willis Re clients in assessing this hard-to-quantify but potentially significant exposure. We also plan to repeat our survey in early 2019 to provide further insights into evolving market perceptions about silent cyber.

Figure 4. **Recent cyber event return period**

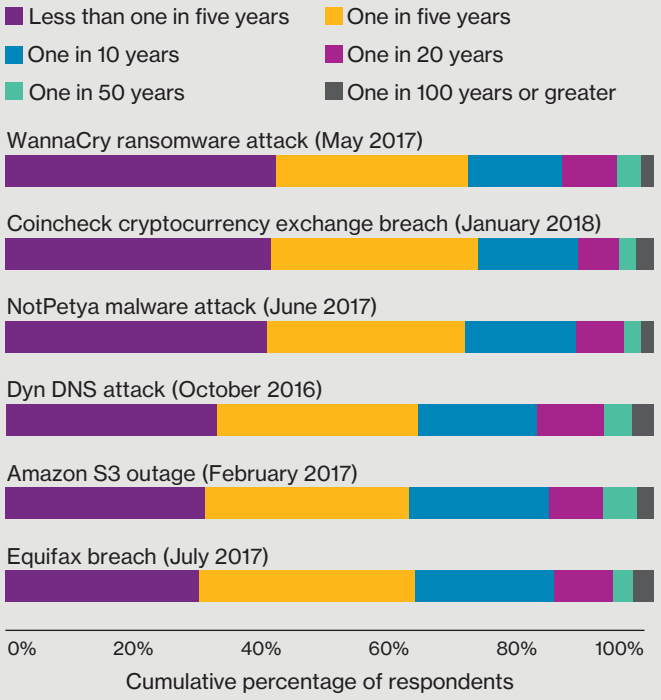


Figure 5. **Industry experience**

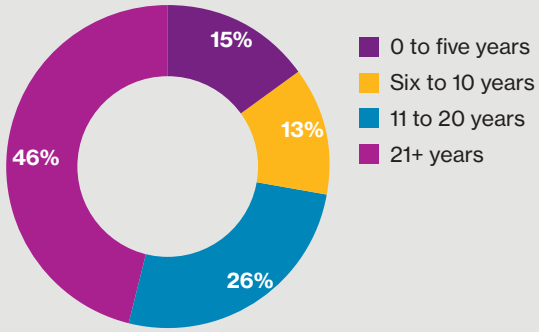
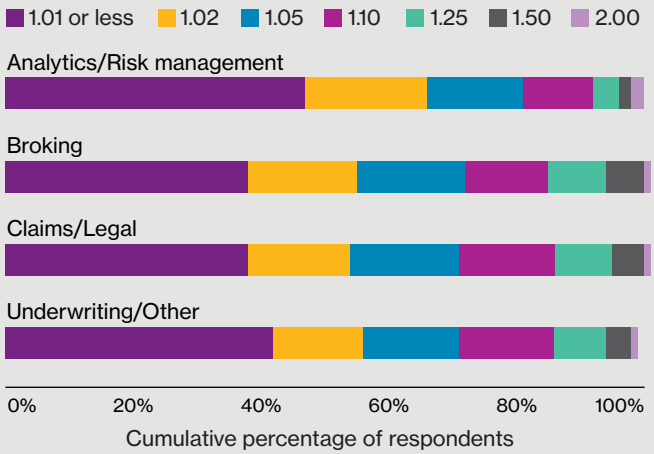


Figure 6. **Silent cyber risk factor – functional responsibility**



For more information about survey results and our observations, contact:

Anthony Dagostino
Head of Global Cyber Risk
Willis Towers Watson
+1 212 915 8785
anthony.dagostino@willistowerswatson.com

Mark Synnott
Global Cyber Practice Leader
Willis Re
+1 312 774 1948
mark.synnott@willistowerswatson.com

About Willis Re

One of the world's leading reinsurance brokers, Willis Re is known for its world-class analytics capabilities, which it combines with its reinsurance expertise in a seamless, integrated offering that can help clients increase the value of their businesses. Willis Re serves the risk management and risk transfer needs of a diverse, global client base that includes all of the world's top insurance and reinsurance carriers as well as national catastrophe schemes in many countries around the world. The broker's global team of experts offers services and advice that can help clients make better reinsurance decisions and negotiate optimum terms. For more information, visit willisre.com.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Re