Decode cyber risk

Silent cyber risk outlook

Willis Re

Is silent cyber risk creeping up on insurers?

Insurance policies specifically designed to cover cyber risk are a growing segment of the market. However, insurers are increasingly concerned about silent cyber exposure: potential cyber-related losses due to silent coverage from insurance policies not specifically designed to cover cyber risk.

Because very little reliable data on this topic can be found, we conducted a survey about the likelihood and potential financial implications of cyber-related losses under policies where cyber risk is neither specifically included nor excluded (so-called "silent cyber"). This might include scenarios such as:

- An attack on an industrial plant's control system causing a boiler explosion that leads to massive property damage from a fire
- An attack on a transit system causing a train derailment that results in bodily injury or death
- Malware causing an elevator to fail, leading to multiple casualties
- A malware-infected GPS-linked navigation system incorrectly guiding a driver, causing a traffic accident that triggers an auto liability claim

Will the policies pay out, or won't they? That will of course depend on the policy wordings and the specifics of the occurrences, but these hypothetical examples nonetheless illustrate the danger of silent cyber events pushing up loss ratios on policies not specifically meant to cover cyber risk.

So we wanted to find out how big an issue this could be for insurers. Our survey sample comprised nearly 750 participants: leaders and experts at more than 70 insurance companies and groups around the world as well as within Willis Towers Watson. The focus for the survey was four insurance lines of business: first-party property, third-party auto liability, third-party other liability, and workers compensation.

What the numbers mean

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 — 0% (no additional loss due to cyber) 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 indicating one cyber-related loss for every 100 non-cyber-related losses and 1.5 representing 50% more covered losses.

Results by insurance line

Not surprisingly, given the lack of credible data that are publicly available, responses spanned a wide range. For example, as shown in *Figure 1,* more than 50% of respondents estimated the risk factor for silent cyber losses to property policies as 1.01 or less. However, a significant fraction estimated a much higher effect, which illustrates how much uncertainty there is over the potential extent of silent cyber exposure. The degree of anticipated risk also varied materially between lines of business. For both auto liability and workers compensation policies, more than 75% estimated the risk factor as 1.01 or less.

For the auto liability line, this may reflect a sense that accidents linked to vulnerability in technology would become product liability losses. The reason for such a low level of perceived vulnerability for workers compensation is less clear.

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

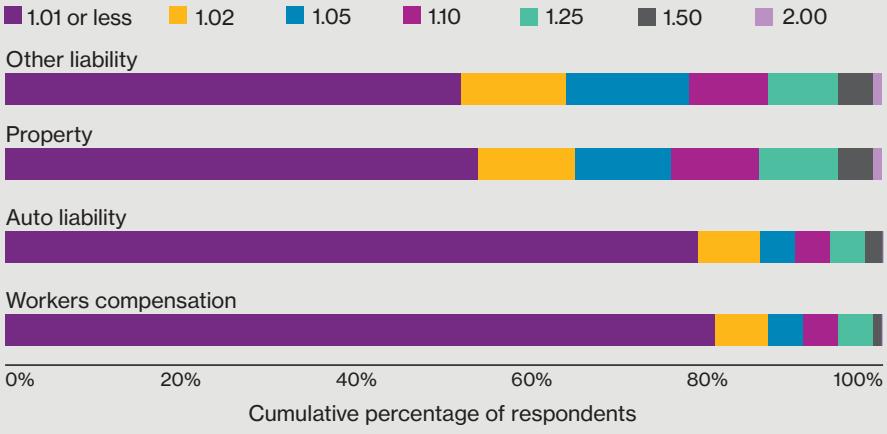
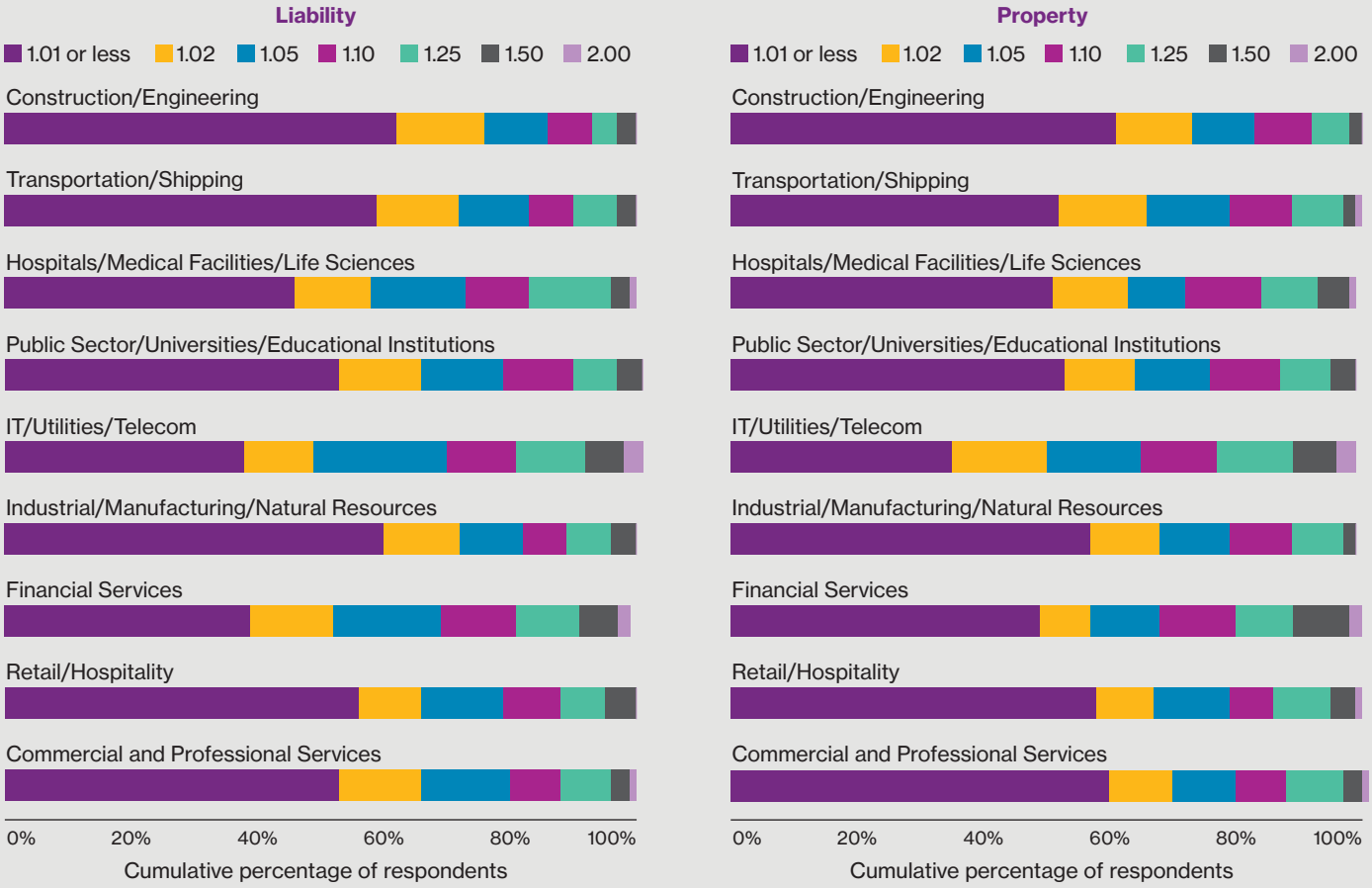


Figure 2. **Silent cyber risk factor by industry**



Given the spread of responses, while the median risk factor for the higher risk lines of other liability and property coverages is a modest 1.01, the mean is significantly higher. The mean risk factor is 1.07 for other liability and 1.074 for property policies. What effect would this imply? Suppose the loss ratio for a book of property business was 60% with all cyber-related losses completely excluded. Assuming that silent cyber losses follow the same severity distribution as other losses, silent cyber exposure might bring this loss ratio to 60.6% using the median view – or 64.4% using the "wisdom of crowds" average view.

Results by industry group

We also asked all respondents to estimate the risk of silent cyber losses in various industry groups. Auto liability and workers compensation showed little variation in estimated risk across industries – probably because the risk was perceived as low overall. However, there were significant industry differences for property and other liability policies *(Figure 2),* contrary to the aggregated responses across all industry groups shown in Figure 1 for these two insurance lines.

The *Construction/Engineering and Industrial/Manufacturing/Natural Resources* industry groupings were seen as relatively low risk for other liability losses, perhaps reflecting that these industries accumulate less personal information from members of the public and so are less exposed to data breach liability. It may be that there is a perception that the silent cyber risk is linked to the data breach risk. Industry groupings that consistently handle consumer information – *Hospitals/Medical Facilities/Life Sciences, IT/Utilities/Telecom and Financial Services* – were seen as higher risk. However, despite several large data breaches in recent years, the *Retail/Hospitality* industry group was seen as lower risk.

Interestingly, although the best-known examples of silent cyber property losses have occurred in industrial settings, respondents did not foresee especially high risk for the *Industrial/Manufacturing/Natural Resources* industry group. Instead, the *IT/Utilities/Telecom and Financial Services* industry groupings were seen as higher risk, perhaps reflecting perceived threats to utility infrastructure.

Figure 3. **Industry experience**

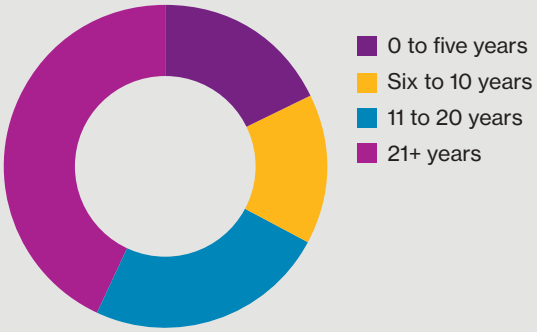
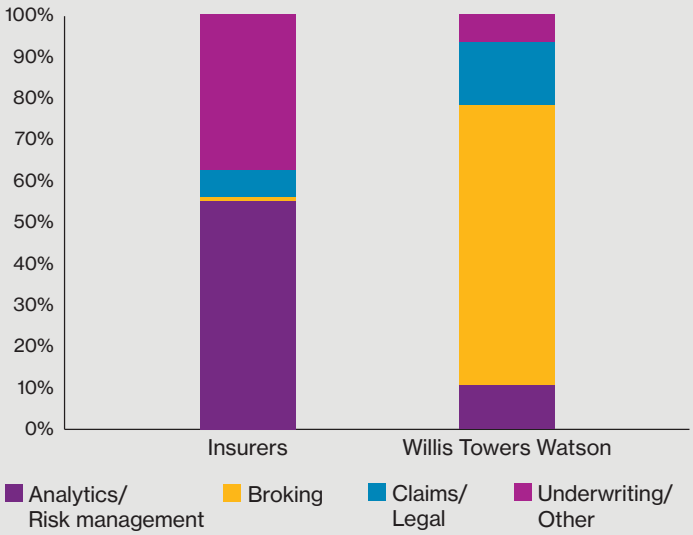


Figure 4. **Functional responsibility**



Survey demographics

Given the speed at which cyber exposures are changing, we deliberately sought responses from a broad range of experience levels *(Figure 3).* While seasoned professionals offer a depth of expertise with loss scenarios and wordings, those newer to the insurance industry may be more in touch with current technologies and how they could be used (or misused).

The survey also includes respondents from a range of functional responsibilities *(Figure 4)*. Roughly half the responses from insurers were from those in analytics or risk management, with the rest predominantly in underwriting; the majority of the Willis Towers Watson respondents were brokers.

Next steps

Over the coming months, we will be calibrating survey results for practical deployment in the measurement, management and mitigation of silent cyber risk. We also plan to extend the reach and scope of our survey with a follow-up in early 2018. The survey was conducted before the WannaCry and NotPetya attacks, and it will be interesting to see how assessments have changed in light of these and other recent events.

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 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

WTW-GL-17-RES-6081C1

willisre.com
willistowerswatson.com

Willis Re