COVID-19 has changed how we think about cyber risk

We're pleased to share the results summary for the 2020 Willis Re survey that explores how today's pandemic risk is influencing cyber risk and cyberinsurance.

Introduction

COVID-19 has affected virtually every aspect of our daily lives. As insurance touches almost everything we do, it is not surprising that the pandemic has also had a major impact on our industry. This is especially true for cyberinsurance. With offices closed and people working remotely, we are even more reliant on digital technology for business and so many other functions. This means more cyber risk.

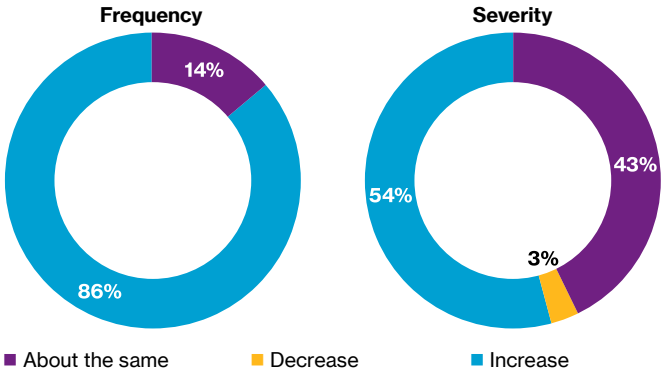
We therefore decided to make COVID-19 the focus of our fourth annual cyber survey. How has the pandemic changed the way we view cyber risk, and how do we see this risk going forward?

We received nearly 1,000 responses from 56 countries, the largest and most geographically diverse number in the history of our survey, covering buyers, risk managers, underwriters, claims staff, actuaries and brokers with a wide range of experience levels (see breakdowns at the end of this report). The results show that just as COVID-19 has reshaped how we view so many other aspects of life, it has also had a marked impact on how we view cyber risk.

COVID-19 and cyber exposure

An overwhelming majority of survey respondents (86%) think the frequency of cyber attacks will increase as a result of COVID-19 (Figure 1), and over half (54%) think the severity of those attacks will also increase. This may be down to the sudden and wholesale transition to working from home for many, which has been accompanied by an increase in vulnerability for businesses that did not have either the IT capacity or IT expertise to support this transition or otherwise had inadequate data governance or security controls. While respondents from all geographic regions broadly agreed on the frequency numbers, there was some disparity in views about the likely increase in severity, ranging from a low of 37% in Europe to a high of 68% in Asia Pacific (APAC).

Figure 1. **How do you think the overall level of cyber attacks is likely to change as a result of COVID-19?**



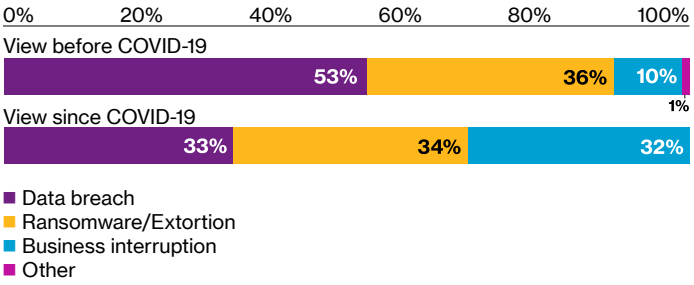
Willis Re

Figure 2 shows there is currently no clear consensus on the biggest driver of cyber-related losses over the next 12 months. Pre-COVID-19, over half the survey respondents (53%) felt that data breach would be the biggest driver of cyber-related losses, but now opinion is evenly split among data breach, ransomware/extortion and business interruption. Concerns about business interruption have grown at the expense of data breach, with the former rising from 10% to 32% as an expected driver of cyber-related losses. These findings were broadly consistent by geographic region. It might have been expected that with the growing publicity surrounding ransomware, this would increase as an expected driver of cyber-related loss; however, business interruption has been prominent in the news as a leading driver of economic loss arising out of the pandemic (although not necessarily insured loss), which might explain the perception that it will drive more cyber-related losses over the next 12 months.

Respondents are also now more attuned to the potential for a catastrophic loss arising out of a cyber "event." Figure 3 shows that pre-COVID-19, 13% — or around one in eight respondents — felt a $10 billion-plus insured cyber event was likely within the next five years; now one in three does.

From a regional perspective, concern about a $10 billion+ insured cyber event in the next five years is strongest in APAC where close to one in two respondents thinks this is likely. It is mildest in Europe: While concerns have risen in line with other regions, only one in five respondents in Europe thinks such an event is likely. Overall, however, the pandemic has highlighted how collectively dependent we are on digital communication to do business and conduct our daily lives. It has also shown the widespread and devastating economic impact of an unexpected "tail" event that pays no attention to geographical boundaries. These factors might explain a greater appreciation of the potential for a large systemic cyber loss.

Figure 2. **In your view, what will be the biggest driver of cyber-related losses over the next 12 months?**



Note: Percentages may not equal 100 due to rounding.

Figure 3. **In your view, what are the chances of a major cyber-related catastrophe event (US$10B+ insured loss) over the next 12 months?**

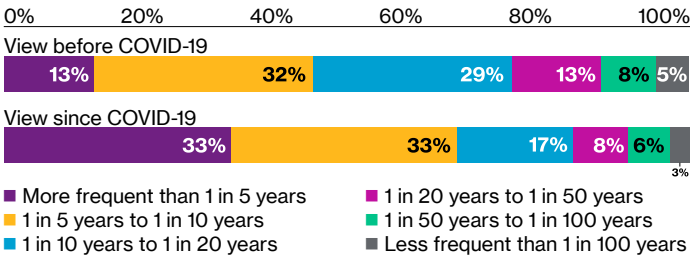
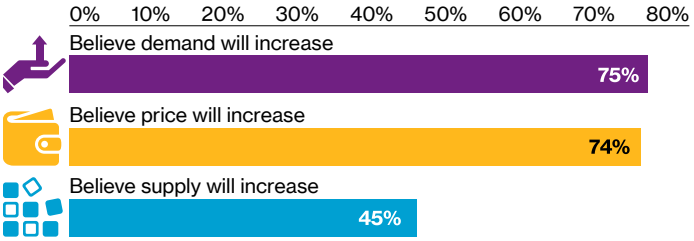


Figure 4. **Do you agree COVID-19 will cause increases in the demand, supply and pricing of cyberinsurance?**



COVID-19 and cyber coverage availability

A greater appreciation for cyber risk should also mean a greater appreciation of the need for cyber protection. This is borne out in Figure 4, which shows that 75% of respondents think COVID-19 will lead to an increase in demand for cyberinsurance. Europe was the only region where respondents felt the increase in demand would be less significant, at 62%.

The greater perceived demand for cyberinsurance does not, however, look like it will be accompanied by a commensurate increase in supply. Only 45% of respondents feel the supply of cyberinsurance will increase going forward, perhaps reflecting a concern about the increasing scale of cyber risk that remote working presents and maybe also a general shift toward more cautiousness in insurers' underwriting appetite for cyber. At 35%, North American respondents were the most cautious about an increase in supply, with APAC respondents being the most optimistic at 65%.

Irrespective of geography, a large majority of respondents (74%) think pricing for cyberinsurance will increase. This conforms with the hardening market we now see affecting cyber and a broad range of other lines of business.

COVID-19 and silent cyber

We also returned to silent cyber (i.e., unspecified cyber coverage in policies not originally designed to cover cyber risk) in our 2020 survey. Despite moves to eliminate silent cyber exposure through exclusions or clarificatory policy language, respondents see silent cyber as an issue that has been exacerbated by COVID-19.

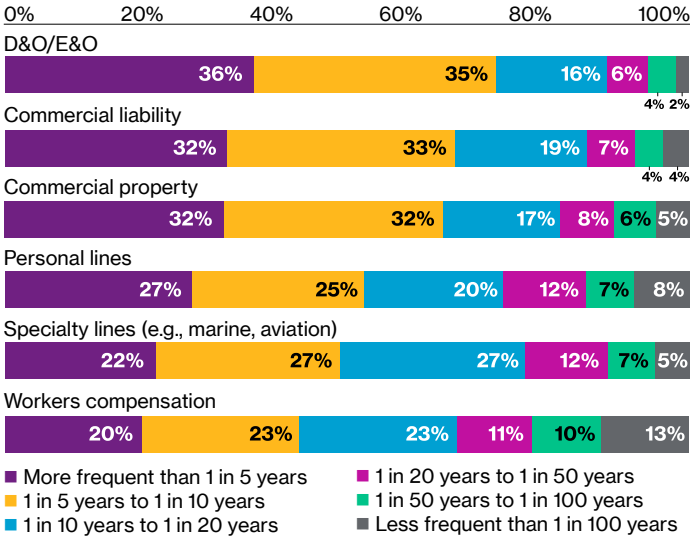
As shown in Figure 5, 57% of respondents think silent cyber exposure has increased as a result of the pandemic while only 12% think it has decreased. The numbers are broadly consistent by geographical region, with Europe possibly being a little less pessimistic than the rest of the world: 51% of respondents from Europe expect the level of exposure to increase. The challenges in the courts over business interruption coverage under property policies as a result of pandemic-related shutdowns have highlighted the need for contract clarity, and the uncertainty over liability coverage arising out of the pandemic amplifies this need. Based on our survey result, respondents throughout the world think silent cyber remains an issue.

Figure 6 shows the perceived extent to which silent cyber remains an issue by line of business. For example, 71% of survey respondents think there is a greater than one in 10 chance that over the next year a directors' and officers' (D&O) or errors and omissions (E&O) claim will arise out of unclear language related to cyber coverage. Around 65% of respondents think the same will be true for commercial property or liability policies. The problem extends more broadly to cover personal lines (52%), specialty lines (49%) and even workers compensation (43%).

Geographically, respondents in APAC expressed views consistently above these average levels while respondents in Europe expressed views consistently below them. Although comparisons with our prior surveys are not exact, concerns about silent cyber coverage in various business lines appear to be on the increase, quite possibly fueled by uncertainty as to which claims will or will not be covered as a result of COVID-19.

Figure 5. **How do you think the risk of silent cyber coverage has changed given the increased attention from regulators and lawmakers on business interruption coverage under property policies as a result of COVID-19?**

Figure 6. **What do you think will be the frequency of cyber-related losses in each of the lines of business below as a result of unclear policy language over the next 12 months?**



Note: Percentages may not equal 100 due to rounding.

Conclusions

While there are some interesting nuances by geographical region, our survey results reveal a number of consistencies in the ways in which COVID-19 has affected how we view cyber risk:

- Perceived exposure is up; we are now more wedded to digital technology than ever before. Bad actors have a wider target to aim at, and in the current environment, it is more difficult to maintain adequate levels of cyber resilience.
- The massive economic damage caused by the pandemic shows how devastating a worldwide "tail" event can be — a wake-up call for cyber insurers given the enormous accumulation exposures presented by cyber as a peril.
- Demand for cyberinsurance will continue to grow — supply may not keep up with demand, particularly if increased exposure is leading to more losses — and prices may therefore continue to increase.
- Despite some corrective actions in the market, silent cyber remains a stubborn and even growing concern. The pandemic has shown what happens when policy language is unclear or challenged — particularly when it comes to business interruption — and this has significant accumulation implications for insurers when it comes to cyber risk.

No one could have predicted the unique and devastating way in which 2020 has developed, and it will be interesting to see how economic conditions affect the cyber market as it continues to evolve at a rapid rate over the next year. In the meantime, we want to thank everyone who participated in this year's survey and look forward to offering some insights on market views in 2021, by which time life will hopefully be less upside down than it is today.

Participant demographics

Figure 7. **Geographic region**

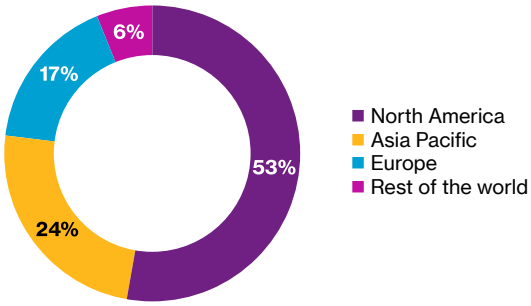


Figure 8. **Functional responsibility**

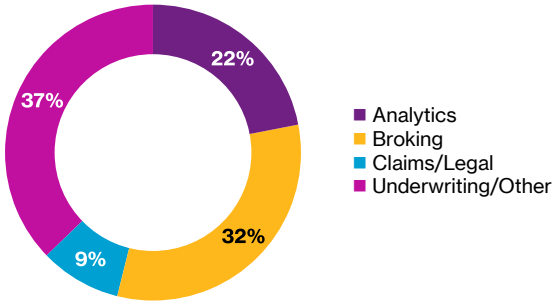
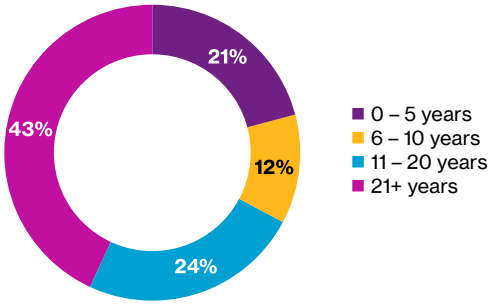
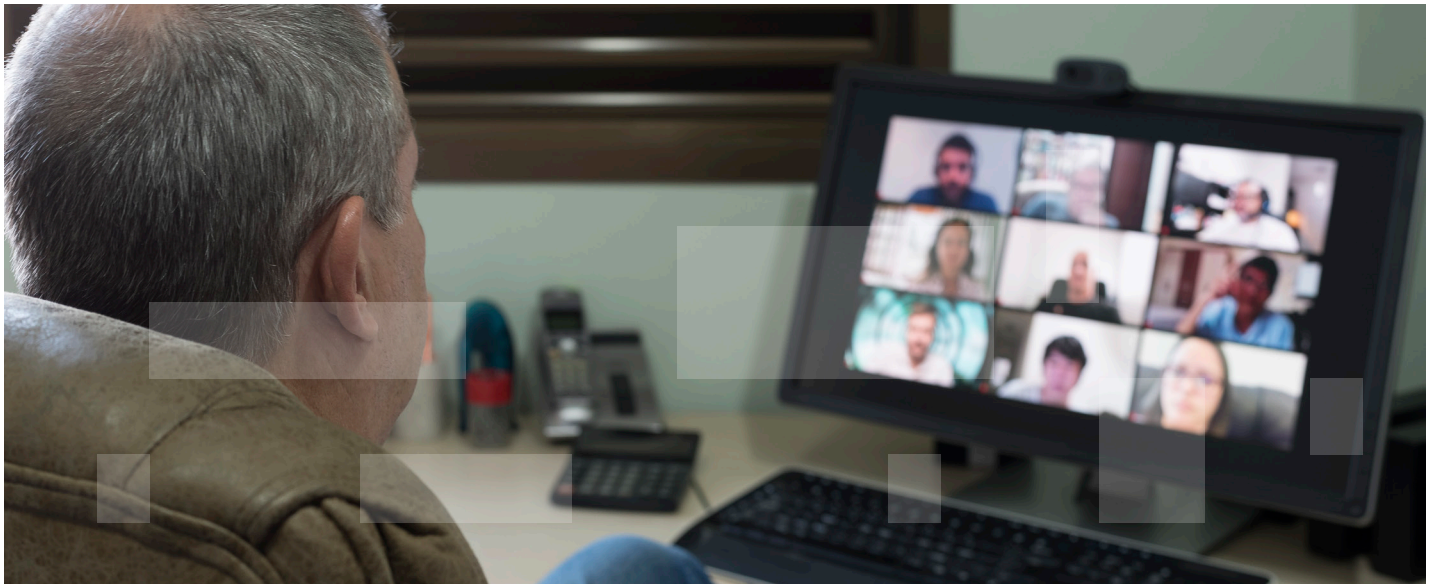


Figure 9. **Industry experience**





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

Jess Fung
Head of Global Cyber Analytics, Willis Re
+1 206 343 6066
jess.fung@willistowerswatson.com

Mark Synnott
Global Head of Cyber, 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 45,000 employees serving more than 140 countries and markets. 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

willisre.com

Willis Re