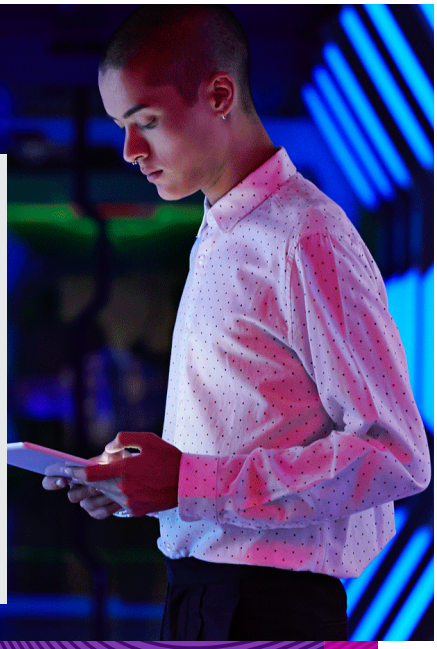


Directors' Liability Survey 2022

Cyber attack, data loss, cyber extortion

John Moran and Marc Voses, Clyde & Co

A robust 67% of respondents worldwide believe risks to their organisation's business operations presented by cyber attacks are second only to those created by the economic climate. Respondents in Europe rank cyber attack risks solidly in first place, while it is tied for first with economic climate by North American respondents, with Australasian respondents ranking the risk second behind COVID-19 and lockdown measures.

With the daily barrage of media reports on high-profile cyber events, it is unsurprising the three categories of cyber risk put to respondents account for the top three risks: with the first being cyberattacks, second, data loss and third, cyber extortion.

With this backdrop, global regulators continue to urge directors to step up and ensure cyberrisk is well examined and addressed by their businesses, from safeguarding data 'crown jewels', to implementing good cyber hygiene and ensuring management are primed and ready to respond to and recover from a cyber attack.

2021 was a wakeup call for businesses operating in core critical infrastructure sectors in particular, as governments, including China, Australia and the U.S., joined the E.U. in implementing regulatory regimes to protect core critical infrastructure assets from cyber attacks. Existing regulatory regimes are also being enforced with more regularity that are oftentimes accompanied by statutory fines and penalties for non-compliance.

A global risk unconstrained by borders

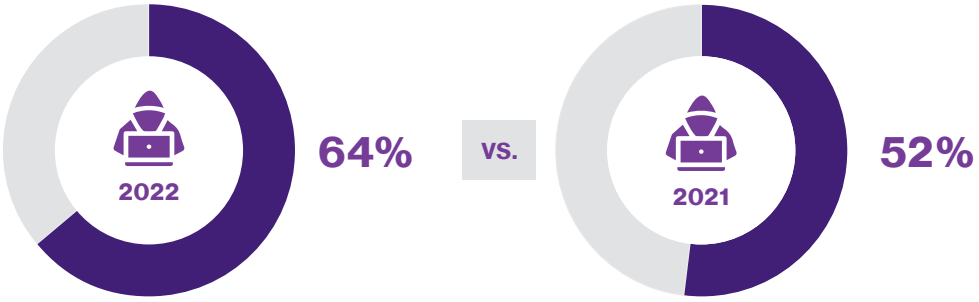
Whilst the perception of this risk differs from region to region, this year's results clearly point towards an intensifying concern of cyber attacks and data risk across the globe. Off the back of the Colonial Pipeline, JBS and Microsoft Exchange attacks, North American respondents reported a significant shift in concern about the risks of cyber incidents for directors: 64% of respondents in 2022 perceived the risk of cyber attacks as 'very significant' or 'extremely significant', as opposed to 52% in 2021.

Even higher figures were reported in Europe and Asia, however just 57% of Australasian boards judged the risk of cyber attacks as either very or extremely significant, which may be explained by the less mature regulatory environment and the less frequent targeting of companies in the region.

Future predictions

It is likely regulators will continue to assert more power in developing regimes. In Australia for example, the Office of the Australian Information Commissioner has increased activity over the last 12 months, a trend likely to continue in light of the recent litigation and may set the groundwork to commence the class action landscape for breach of privacy claims within Australia.

North American respondents reported a significant shift in concern about cyber incidents:



Perceived the risk of cyber -attacks as 'very significant' or 'extremely significant'

Evolving landscape of risk

The changing risk landscape is likely to increase concerns about cyberrisk, especially in uncertain geopolitical times. We have already seen an increased recognition of this risk, with 65% of respondents globally now recognising the threat of cyber attack as 'very' or' extremely significant', compared with 56% last year.

The threat of ransomware, for example, has become more sophisticated and this is explored more in the article: Cyber Extortion - ransomware and payment of ransoms.

In North America, state governments are increasingly enacting data privacy laws that require organizations to take control of their data and inform the public what data they collect and how they use it. Regulators, including those overseeing public companies and financial institutions, are becoming more active in pursuing those entities that suffer data breaches as a result of a failure to implement or adhere to a cybersecurity program.

We predict a continued uptick in regulatory enforcement actions, along with significant monetary fines for those organizations that suffer a cyber attack because of a failure to maintain an adequate cybersecurity program.

From the standpoint of cyberinsurance, we predict stricter underwriting requirements and increasing premiums could result in businesses being underinsured or uninsured.

In some respects, the visibility of the risks presented by cyber attacks and increased regulation have resulted in businesses improving their cybersecurity programs and addressing data collection practices.

We believe the entry of additional cyberinsurance capacity, coupled with assessing and monitoring an organizations' cybersecurity, will help reduce cyber attacks on those organizations using these products and services.

Disclaimer

Willis Towers Watson offers insurance-related services through its appropriately licensed and authorised companies in each country in which Willis Towers Watson operates. For further authorisation and regulatory details about our Willis Towers Watson legal entities, operating in your country, please refer to our Willis Towers Watson website.

It is a regulatory requirement for us to consider our local licensing requirements. The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date.

This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market and we disclaimer all liability to the fullest extent permitted by law. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this video may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson.

Each applicable policy of insurance must be reviewed to determine the extent, if any, of coverage for losses relating to the Ukraine crisis. Coverage may vary depending on the jurisdiction and circumstances. For global client programs it is critical to consider all local operations and how policies may or may not include coverage relating to the Ukraine crisis. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal and/or other professional advisors. Some of the information in this publication may be compiled by third-party sources we consider reliable; however, we do not guarantee and are not responsible for the accuracy of such information. We assume no duty in contract, tort or otherwise in connection with this publication and expressly disclaim, to the fullest extent permitted by law, any liability in connection with this publication. Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates. The Ukraine crisis is a rapidly evolving situation and changes are occurring frequently. Willis Towers Watson does not undertake to update the information included herein after the date of publication. Accordingly, readers should be aware that certain content may have changed since the date of this publication. Please reach out to the author or your Willis Towers Watson contact for more information.

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW-FINEX 519301/05/22

wtwco.com