Browne Jacobson

CyberCube's Global Threat Outlook: The evolving threat of cyber operations

26 September 2023

Previous
Insurance and the Automated and Electric Vehicles Act 2018

Next
"TOBA traps" - general exposure risk under existing TOBAs

CyberCube has produced a Global Threat Outlook, outlining key threats, with analysis of global cyber 'hot zones' ahead of the fourth quarter of 2023. The report details four core considerations for insurers relating to recent activity.

Intelligence gathering and malware attacks

In its 2023 Global Threat Report, Crowdstrike has detailed various Russian activities used in its war with Ukraine, including intelligence gathering and destructive malware attacks.

Insurers should model their wordings around the potential impacts of this type of activity against insureds. For example, the use of targeted malware against major cloud service providers could result in widespread outages and service disruption to consumers. Additionally, malware events can also have a widespread effect on global servers, as in the case of the NotPetya wiper malware attack of 2017. Any such review of wordings and exposure should consider any existing provisions relating to cyber war, particularly following Lloyd's recent requirement for insurers to review the same.

Internet and telecommunications assets

China continues to engage in cyber activities, with China-nexus adversaries targeting nearly all 39 global industry sectors, including Taiwanese technology firms. This was also evidenced in June 2023, in which Microsoft discovered targeted malicious activity by Volt Typhoon. Such activity was aimed at compromising credential access and disruption to critical infrastructure and telecommunications. CyberCube anticipates more forceful and destabilising cyber campaigns are on the horizon.

Disruption of such infrastructure could result in widespread internet downtime and inaccessibility of online communications applications. Insurers should consider the potential impacts of attacks on such assets, and whether their wordings and underwriting are sufficiently robust to deal with potential widespread infrastructure failure.

Operational technology

Iranian groups have also targeted a range of government and private sector organisations across various continents, seeking to attack manufacturing and heavy industry operational technology. In April, Microsoft observed Iranian-linked threat actors targeting the water controllers of at least ten Israeli farms.

As the threat of attack on operational technology persists, the risks remain high when considering operations of physical infrastructures such as maritime vessels, aircraft weaponisation, critical energy, transportation and logistics machinery. Therefore, insurers should review their wordings and underwriting accordingly.

Cryptocurrency

North Korea's illicit financial activities have reportedly affect at least 29 countries. Notably, the increase in adoption of cryptocurrencies has also sparked more aggressive and adaptable cyber-attacks. This mostly takes the form of attacks on cryptocurrency assets and exchange systems. As a result, financial transaction providers and large banks are often the target of cash and data theft.

In consideration of upcoming regulations like the Financial Services and Markets Act seeking to regulate crypto-related activities, insurers should await and monitor the changing regulatory landscape.

Conclusion

CyberCube's report suggests the upcoming threats seek to push the limits of pre-existing war and cyber war exclusion language. Whilst there has been significant progress in addressing these events this year, insurers will need to settle on a consistent approach that balances the interests of stakeholders.

Whilst the complexities of the attribution of cyber incidents carry significant uncertainty, underwriters should aim for regularity and clarity to shield themselves and policyholders from the impact of outlier events.

Contents

Key contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

Coverage disputes and policy interpretation

Cyber liability and data security insurance

Digital and data

Financial services and insurance advisory

Policy drafting and distribution