Brown & Brown

PROPERTY & CASUALTY

Cyber Risk Update

Russia and Ukraine

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently warned of Russian cyberattacks spilling over onto U.S. networks. The advice follows previous CISA warnings on the risks posed by Russian cyberattacks for U.S. critical infrastructure. As the conflict in Ukraine continues to escalate, so too are cyber threats.

The current situation is a reminder of Not Petya in 2017 and the SolarWinds compromise in 2020; both being examples of attacks that were said to have been sourced within Russia that became widespread, impacting a wide range of organizations that did not have a relationship with the originally targeted entities or connected with the conflict between Russia and Ukraine.

U.S. companies and their IT Security teams should anticipate Russian cyberattacks and assess the potential effects on their operations. Companies with operations or suppliers in the region could be impacted, but even companies that have no presence in Ukraine or Russia should watch for indirect impacts, such as Not Petya, and has implications on their suppliers, customers and partners. Like Merck, indirect cyber collateral can be just as devastating as a direct cyberattack.

In addition to the Russia/Ukraine conflict and historical cyber loss experience ensuing from such conflicts, the publication of a court decision allowing $1.4 billion of coverage under an all-risks property policy, which incorporated a War Exclusion, has brought insurability into focus. Lloyds of London has recently released four model War Exclusions with updated language focusing on and providing alternative ways of viewing cyberwar. In addition, they have refined model wording to provide markets with a greater ability to consider ways to deal with some or all of the following:

- “Physical War” versus “Cyber Operations”
- Direct War versus Collateral damage on entities that were not the intended targets
- Attribution of the source of the attack
- Attacks by non-state actors associated with a state
- Differing targets of the attack
- Aggregation of cyber risk

These concepts, which are likely to be central in discussions with underwriters, will be developed to outline positions to affirmatively cover or affirmatively exclude the impacts of nation-state cyber-attacks. Moreover, how underwriters define what is considered a direct attack as a cause of war versus collateral damage will also require close review and negotiation. With no current mandate from Lloyd’s for market participants to adopt new language, we anticipate insurers will review and potentially modify these clauses.

In addition to a close review of your cyber insurance policy language and any endorsements addressing the War Exclusion, the uncontrollable geopolitical issues, nation-state conflicts and the boundaryless increased cyber risk, will require underwriters to review and scrutinize IT security controls. The most well–protected companies should consistently evaluate their cyber exposures and effect a plan for sustained strategic investment in their cyber defenses. Some critical items that have been the focus of underwriting attention in the last year should be considered part of the cyber protection strategy. For example, enabling multi-factor authentication (which, according to CISA Director Jen Easterly, makes you 99% less likely to get hacked), patching old vulnerabilities, ensuring passwords are strong, maintaining offline and immutable backups and remembering that phishing is still the number one attack vector, even for sophisticated adversaries — can contribute to better overall security.

Brown & Brown provides advice and consulting for risk managers to help manage and direct the discussions with underwriters, IT security executives, senior management and boards of directors on these issues. We are prepared to review your cybersecurity maturity, coverage available under your insurance programs, help you identify, quantify and mitigate your insurance programs, and help you identify, quantify and mitigate your risk to cyber loss and develop the appropriate program and strategy to placement.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving property & casualty insurance program.

Brown & Brown

Find Your Solution at BBrown.com