MINNESOTA STATE BAR ASSOCIATION JANUARY/FEBRUARY 2023

BENCH+BAR of Minnesota

BUILDING A MORE ACCESSIBLE BAR

A roundtable conversation featuring members of the Minnesota Disability Bar Association

Thinking about the future of CYBER INSURANCE

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

A few years ago, I wrote an article titled "Is cyber liability insurance important for law firms?" (May/June 2018) that explored the benefits and limitations of cyber liability insurance and the need to resist relying on coverage as a cyber "get out of jail free" card. In any circumstance, cyber insurance should be viewed as one piece of a complete cybersecurity strategy; these policies are valuable not only for the coverage they offer, but as a starting point for organizations to assess and improve upon their current postures. A policy can help an organization visualize the monetary losses incurred by cyber threats. However, when it comes to collecting on a policy in the aftermath of an attack, organizations are often uncertain when it comes to determining what is covered. In recent years, the problem has only gotten worse as insurers try to combat a growing number of cyber losses.

Since the time I wrote that article, changes have been made to how providers address the complicated task of quantifying the risks of cyber events. Cyber attacks have short-term and long-term consequences and can produce multifaceted ongoing risk (for example, the Log4j vulnerability—which not only had an immediate effect but created the potential for future hacking events); furthermore, issues can arise when attributing an attack. To counteract this, insurance companies have adopted increasingly specific coverage language to limit what is included in policies.

For example, in my article, "Social engineering or computer fraud? In cyber insurance, the difference matters" (October 2022), I discussed *SJ Computers, LLC v. Travelers Casualty and Surety Company* (21-CV-2482 (PJS/JFD) (D. Minn. 8/12/2022)). This case clearly demonstrated the power of policy language, with the court ruling that the definitions contained within the Travelers policy clearly differentiated between social-engineering and computer fraud, limiting SJ Computers' coverage following a phishing attack. Organizations are frequently surprised to learn what is actually covered in their cyber policies, especially when assumptions are made about how different types of attacks are defined. The ways in which attacks are categorized can sometimes seem counterintuitive, and it is important to periodically review your policy to avoid any last-minute surprises. It's also important to recognize that the proliferating number of cyber attacks organizations now encounter, paired with the possible ripple effects of a single attack, may soon cause insurance companies to reconsider their ability to insure cyber attacks at all.

Recently Mario Greco, the CEO of Zurich Insurance Group Ltd., one of Europe's biggest insurance companies, asserted that the potential for cyber attacks to cause major disruption may soon preclude them from insurability.[1] Simply put, the unpredictable losses associated with even one cyber attack make the task of quantifying damages difficult, if not impossible. Consider an attack on critical infrastructure that impacts the healthcare sector, resulting in an inability to care for patients—or the disaster that could be wrought by a nation-state-sponsored ransomware campaign. Even as we start 2023, the war in Ukraine continues to highlight concerns regarding nation-state cyber campaigns, especially when a single event could cause a complex wave of catastrophic loss.

In response, insurance providers have worked to tighten policy language, set coverage limitations, and reduce ambiguity as much as possible. "Spiralling cyber losses in recent years have prompted emergency measures by the sector's underwriters to limit their exposure. As well as pushing up prices, some insurers have responded by tweaking policies so clients retain more losses... In 2019, Zurich initially denied a $100mn claim from food company Mondelez... on the basis that the policy excluded a 'warlike action.'"[2] Organizations often only discover gaps in their coverage when an event has already occurred.

Cyber liability insurance is sometimes responsible for creating a false sense of security in organizations and it is likely that drastic changes will continue to be made in how these policies are written and obtained. "Increased ransomware events have caused elevated losses; cyber insurance companies have responded by increasing premiums and have required better cyber hygiene requirements for policyholders such as multifactor authentication... [C]yber insurance will have to evolve in kind to keep pace with the drivers of losses."[3] Organizations will be held to a higher security standard to meet the requirements of their cyber insurance policies; rather than being viewed as a safety net, cyber policies should serve as a driving motivator for enacting proactive measures and maintaining best practices.

Cyber insurance policies can be a valuable tool in giving organizations a real-life perspective on cyber risk and the need for consistency in maintaining a strong security posture. Like any component of a healthy cybersecurity plan, cyber insurance is only one aspect of how an organization should prepare itself for the worst. And organizations must bear in mind that cyber insurance policies have inherent limitations, creating confusion for organizations when they are most needed.

As cyber threats evolve, it is likely that cyber insurance will change in turn, accounting for the immense losses that can characterize even a single attack. As Mario Greco put it, "there must be a perception that this is not just data... [T]his is about civilization. These people can severely disrupt our lives."[4] Indeed, the ramifications of an attack often extend beyond a matter of mere inconvenience. To match this risk, proactive measures to protect our cyber environments (including striving to improve internationally through governmental intervention and cooperation) should continue to be top priorities. ▲

NOTES

[1] *https://www.swissinfo.ch/eng/business/cyber-attacks-set-to-become–uninsurable-–says-zurich-chief/48161718?utm_campaign=swi-rss&utm_source=multiple&utm_medium=rss&utm_content=o*

[2] *Id.*

[3] *https://www.fitchratings.com/research/insurance/russian-cyberattacks-may-test-insurer-war-exclusion-policy-language-01-03-2022*

[4] Supra note 1.