Loss Controls: The Key to Mitigating Cyber Risks in a Challenging Market

COVID-19 remains a top risk for 2021, second only to business interruption and closely followed by cyber incidents, according to a new survey of nearly 3,000 risk management professionals.[1]

Even before the pandemic, business interruption and cyber incidents were growing concerns for organizations, prompted by the increased reliance on technology and an increasingly interdependent global supply chain. COVID-19 has worsened these existing risks, while creating its own unique challenges.

At the outset of the pandemic, organizations across all industries were forced to embrace technology as a means of business continuity, whether to allow employees to work remotely or to provide transparency and efficiency in the supply chain. And while technological advancements have enabled many companies to safely operate during a pandemic, reliance on third-party technology providers and a displaced workforce have created new avenues of risk. These two factors alone have the potential to trigger a destructive chain reaction in the event of a disruption or cyber incident.

The recent SolarWinds incident is just one example of this evolving risk. By targeting a specific piece of software used by thousands of organizations and government entities to manage IT security and administration, hackers created a significant vulnerability for those organizations and exposure to future ransomware and cyberattacks. Events like the SolarWinds breach demonstrate that without proper loss controls in place, a cyberattack or technical failure at one organization can result in severe business interruption for thousands of organizations in the supply chain.

At the same time, ransomware attacks have become more targeted and costly. NetDiligence reported in its 2020 *Cyber Claims Study* that the average ransom demand increased from $72,000 in 2018 to $175,000 in 2019. In the same time frame, ransom demands crossed the million-dollar threshold, with one firm reporting a ransom of $18.8 million in 2019.

While ransom demands attract the most attention, the biggest cost for ransomware is business interruption. While the average ransom was $175,000 in 2019, the average *total cost per incident* was $275,000, according to the NetDiligence report. In fact,

business interruption losses accounted for 60% of the total cost of cyber insurance claims in the past five years.[2]

The convergence of these events demonstrates how imperative it is for organizations to develop and implement robust cybersecurity and cyber loss control programs. Companies need to adequately assess and identify cyber exposures and risks (both internal and external), as well as understand the full impact these exposures and risks would have on the business's operations, finances, and reputation. Furthermore, organizations must have processes and practices in place to adequately detect, prevent, respond to and recover from cyber incidents and risks — not only to protect the organization, but to help secure the coverage necessary to survive a cyber incident.

Cyber Insurance Responds

Traditionally, cyber insurance was a cost-effective way for organizations to transfer risk: simply purchase a cyber policy and let the insurance company deal with the fallout. However, recent increases in cyber incidents and mitigation costs have led to a historically hard market for cyber insurance, making it increasingly difficult and expensive for organizations to purchase coverage and offset risk.

[1] Allianz Global Corporate & Specialty, *Allianz Risk Barometer 2021*. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
[2] Allianz Global Corporate & Specialty, *Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk, 2020*. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyber-Risk-Trends-2020.pdf

Continued on next page

As we recently outlined in our cyber risk addendum to our 2020-2021 Commercial Property & Casualty Market Outlook, underwriters are taking a more thorough and technical look at an organization's cyber exposures and loss controls. Insureds with poor cyber controls will likely experience higher premiums and reduced insurance capacity, or higher self-insured risk (SIR), assuming insurance carriers are willing to even take on the risk. Even organizations with average risk profiles may face higher premiums and retention and policy exclusions.

In a hard cyber market, carriers are not likely to offer terms to organizations that don't have loss controls in place. Understanding the risks is the first step to improving cyber security and presenting the best possible risk profile to underwriters.

Improving Risk Profile

Facing increased underwriter scrutiny, insureds will have no choice but to tighten cyber loss controls and improve their risk profile before insurance companies will even consider taking on the risk. While traditional brokers remain focused primarily on preventing and remediating cyber incidents, USI helps clients take the *additional* step of improving their risk profile for better and more affordable coverage by addressing the sources of cyber loss.

There are service providers that can help companies address their cyber exposures and improve their risk profiles, but many companies don't know where to even begin. USI bridges the gap between these service providers and cyber insurance by helping clients identify exposures and prioritize solutions. We then connect clients to our curated, trusted network of non-insurance risk management solution providers. This combined and customized approach helps clients address specific, emergent risks and reduce associated costs, as well as present an optimized risk profile for underwriter consideration.

Following a recent cyberattack, a midsize healthcare system ($350 million in annual revenue) contacted USI for help with reducing its ransomware exposure. USI presented two cutting-edge solution

providers to the client, and within 60 hours of engaging the chosen provider, the client had the results of a detailed analysis. The provider was able to help the client limit regulatory and attack surface exposures, remediating $14 million in potential exposures.

How USI Can Help

USI's cyber risk experts specialize in identifying and prioritizing risk to help clients understand their unique cyber exposures. We work with clients to reduce those exposures and provide adequate coverage by reviewing existing policies and benchmarking limits and retention, thereby identifying weaknesses in the current program structure. We provide additional support and resources to clients *pre-placement* to help them improve their cyber risk profile and secure favorable coverage and placement.

Cyber risk is no longer an inconvenience — it's a balance sheet issue for organizations across all industries. In the current risk environment, failing to procure proper insurance coverage and align cyber resources could be the demise of your organization. Contact your USI representative to learn more about the cyber solutions designed to mitigate your risk and protect your organization in the event of a cyber incident.

The USI ONE Advantage®

To analyze our client's business issues and challenges, our property & casualty team leverages USI ONE®, a fundamentally different approach to risk management. USI ONE integrates proprietary business analytics with a network of local and national technical experts in a team-based consultative planning process to evaluate the client's risk profile and identify targeted solutions. Clients then receive tailored recommendations for improving their total cost of risk. To learn more about USI ONE and the USI ONE Advantage, contact your local USI team today.