Is Your Industry a Target for Ransomware and Other Cyberthreats?

Cyber risk awareness is more important than ever. Cybersecurity has become increasingly complex for employers, as many are welcoming employees back to the workplace while still supporting remote work environments. As part of National Cyber Security Awareness Month (NCSAM), USI Insurance Services is offering cybersecurity webinars in October focusing on healthcare, public entities, construction, and transportation.

Cyberthreats are increasing for all organizations, but many business leaders don't realize they must implement prevention and mitigation tactics tailored for their specific industries and organizations. In other words, one size does not fit all. An incident response plan (IRP) for a construction company, for example, might be fundamentally different for a healthcare facility.

Amid the disruption of situating employees back in the workplace while still supporting remote work, ransomware attacks increased by 148% month-over-month in the first quarter of 2020, and the upward trend is continuing.[1] The steady increases include the number of cyberattacks and ransoms demanded by hackers. Malicious emails are up 600% in 2021, and the largest ransomware payout this year was made by an insurance company at $40 million, setting a world record.[2]

As a result, insurance underwriters are taking a more thorough and technical look at an organization's cyber exposures and loss controls.[3] Organizations 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 those with average risk profiles may face higher premiums and retention and policy exclusions. Organizations will have no choice but to tighten their cyber loss controls and improve their risk profile before insurance companies will even consider taking on the risk.

Some industries have more difficulty tightening cyber loss controls than others. For that reason, cyber criminals are targeting "nontraditional" industries with historically weak controls, such as healthcare, public entities (including municipalities and educational facilities), transportation and construction. In the sections that follow, we'll focus on one cyber risk vector, ransomware, and how it impacts these industries. (All organizations can access important data and insights about cyber risk in USI's Cyber and Executive & Professional Risk Solutions Addendum to the 2020-2021 Market Outlook.)

Healthcare

Healthcare Hackers Demanded an Average Ransom of $4.6M in 2020[4]

In the healthcare industry, increased investment in technology and a growing focus on data sharing, coupled with outdated infrastructure — including underfunded IT departments and legacy medical devices with little-to-no cybersecurity features — have exponentially increased the number of potential infiltration points for cyberattacks. These factors add to the complexity of the three main considerations when confronted with a ransomware attack:

- **Extortion response.** Research shows that 60% of healthcare organizations say they would pay hackers for the decryption key in event of a ransomware attack[5] — even though organizations in the U.S. can be sanctioned for paying ransoms to certain groups by the Office of Foreign Assets Control (OFAC) or another entity. It's not difficult to understand why healthcare is a targeted industry: with patient lives on the line, continuity of care is essential.

Continued on next page

- **Business interruption or shutdown.** During a ransomware attack, information systems are shut down, and staff members' work is hindered by the denial of access to crucial information systems they rely on for decision making. It's critical to improve detection and response tools to isolate and remove machines from the infected network while continuing operations. It's also essential to educate and train the entire workforce on what to do in the event of an interruption or shutdown.
- **Reputational damage.** Harm to patients can damage a healthcare facility's reputation beyond repair, so healthcare providers should put protecting patients from cyber risks at the core of their cybersecurity strategy. Failing to protect critical technology infrastructure ultimately may mean failing to protect patients.

Cyber Risk Solutions for Healthcare

Healthcare facilities should secure appropriate cyber extortion insurance to seek to cover the costs of a ransomware event as well as to provide network/forensic assistance. For example, a senior manager in a healthcare management firm opened an email from an established vendor that said: "Your computer is now blocked. You have 96 hours to pay or your files cannot be recovered. Our ransom is $500,000 in Bitcoin." The ransomware spread quickly and, according to the message, if the firm did not pay, its files would either be destroyed or remain inaccessible.

USI professionals worked with the management team to review all options, including the ransom amount and remediation cost, which totaled approximately $500,000 in ransom, $100,000 to secure the Bitcoin + $300,000 in forensics and other expenses. Since the firm had cyber coverage, the cost for the above incident was paid less the retentions (i.e., $900,000 minus a $50,000 SIR).

This is only one example of how ransomware can threaten your organization, and many considerations remain for healthcare facilities. Join our cyber webinar for healthcare organizations to learn best practices before and after a cyber event.

Public Entities

Ransomware Attacks Against Municipal Governments Increased 60% YoY 2019-2020, While Attacks Against Universities Increased 100% [6,7]

Public entities are often an easy target for ransomware attacks, especially with the rise of virtual classrooms due to the pandemic. Many schools and municipalities do not have the necessary funding to invest in cybersecurity tools and training.

- **Extortion response.** Based on available data, most public entities are not paying ransoms. In 2020, 26.7% of public entities refused to pay the ransom, while 12.7% did pay, and the median ransom amount in 2020 was $389,000. [8] In 2019, the city of Baltimore chose not to pay a $75,000 ransom demand, and the city spent over $18 million on recovery. New Orleans, after refusing to pay their ransom during an attack in December 2019, spent about $7 million on recovery.
- **Business interruption or shutdown.** The negative impacts of these events are obvious to the organizations and individuals involved and can include massive costs to recover. The Baltimore ransomware attack mentioned above crippled government systems for months, disrupting everything from water billing to real estate transactions. A separate attack caused the county's school system to shut down for 115,000 students. The interruption impacted student academic performance, lesson plans, and communication between teachers, students and parents.
- **Reputational damage.** An organization's reputation is commonly defined during a crisis, such as a ransomware attack, and a competent response can have a positive long-term impact. Public-sector organizations have become more aware of the value of a favorable reputation and, as a result, are gradually treating the management of reputation as a concern of strategic importance.

Cyber Risk Solutions for Public Entities

One way to limit the success of cyberattacks is to enable multifactor authentication, keep software up to date and patched, and train staff to only open emails or click on links from trusted sources. For example, a large municipality was concerned with ransomware risk exploding in "nontraditional" sectors including cities and municipalities. The city council and municipality leadership wanted to implement cyber risk controls (including Answerlytics™) to protect its network against threats, such as ransomware and social engineering, which are endemic to municipalities.

After implementing the solutions, the municipality was able to update its board of directors on system risks and remediation, comply with contract requirements, save more than $750,000 on software costs, and remove a potential $2.5 million exclusion due to 50% co-insurance on its cyber policy.

Join our cyber webinar for public entities to learn best practices before and after a cyber event.

Continued on next page

Construction

1 Out of 6 Construction Firms Reported Experiencing a Ransomware Attack in 2020[9]

Ransomware attacks often focus on companies that will be immediately impacted by the disruption. Construction companies are likely being targeted because of their limited awareness of cyber risks and their lack of cybersecurity. In addition, ransomware can cause a substantial interruption to the complex supply chain of construction projects.

- **Extortion response.** The average ransom paid by construction companies increased by 171% from 2019 to 2020 to more than $312,000 on average per event.[10] About 74% of companies in the construction industry said they would consider paying a ransom, which is a higher percentage than any other industry surveyed.[11] Construction companies are singled out by cyber criminals because they tend to be cash-rich and constantly under the gun to meet delivery targets — so they are considered vulnerable and willing to pay.
- **Business interruption or shutdown.** The construction industry is heavily reliant on the ability to deliver projects on a deadline. Almost every construction contract has a hard completion deadline. The consequences for failure to meet the completion deadline may include termination of the contract for default or other costly outcomes. Therefore, construction companies should have adequate cyber and business interruption coverage to avoid costly delays.
- **Reputational damage.** Reputation is especially impactful for construction companies — it affects how successful they are when bidding for projects and the overall health of their organizations. A reputation for not finishing on deadline, especially if the reason is a ransomware attack, can be catastrophic to the business.

Cyber Risk Solutions for Construction Companies

Cyber criminals can inflict harm by breaching intellectual property, stealing critical data, and causing downtime, resulting in financial losses and project delays. Further investment in cybersecurity, insurance and best practices can help.

Construction firms commonly rely on service providers for everything from electronic bill payment to material sourcing and distribution. Contractors' systems may be integrated within construction organizations' networks. As a result, an attack launched through a contractors' system represents an easy way to gain access to a more valuable organization.

Not surprisingly, a common coverage gap for construction companies is poorly managed IT security. For example, USI risk management professionals and our Answerlytics cyber partners helped a construction firm evaluate its in-house data logs and identify and address two emergent threats. This made a significant financial impact by improving SIR by $500,000 versus the quoted amount ($1 million SIR) due to implementing managed security services, including a 24/7 security operation center and endpoint detection and response functions.

Join our cyber webinar for construction companies to learn best practices before and after a cyber event.

Transportation

Transportation Endured a 186% Increase in Weekly Ransomware Attacks From June 2020 to June 2021[12]

The transportation industry's exposure to cybersecurity threats is rapidly increasing. Internet-enabled components that facilitate fleet monitoring as well as driver or truck data logging or software can open entire fleets to cyber exposure. Cyber extortion or ransomware attacks along with business interruption due to system failure and social engineering are all rapidly emerging issues that must be addressed.

- **Extortion response.** Many cybersecurity experts discourage transportation companies from paying ransoms. Extortionists may fail to provide the promised decryption keys for file restoration, and when ransomware decryption tools are provided, only 8% restore files to their original forms.[12] However, many shipping, transport and logistics firms are willing to take the chance, given the significant impact of downtime, and some use ransomware payment vendors where allowed.
- **Business interruption or shutdown.** Logistics and transportation companies are reliant on delivery schedules to ensure profitability and customer satisfaction. It only takes one ransomware or malware attack to have a detrimental effect on logistics schedules, including systems shutdown and potentially significant delays in deliveries. In addition to direct financial damage, ransomware attacks can result in the loss of sensitive corporate information —including everything from

Continued on next page

customer email addresses to the birthdates and national insurance numbers for employees. Long-term damage and costs will arise from this kind of event.

- **Reputational damage.** The reputational risks from a ransomware attack can be harmful when it becomes known outside of an organization. The risks can range from exposure as a vulnerable entity, and therefore a ripe target for further attacks, to distrust and skepticism by customers, thus adversely impacting future business. The potential for losing trust from customers and stakeholders is high, particularly if an incident involves large volumes of sensitive data and/or delay in delivery or completion.

Cyber Risk Solutions for Transportation Companies

Transportation companies should work with their IT partners and insurance consultants to prevent cyberattacks on the front end and mitigate financial losses when such incidents occur through improved risk transfer. USI's Transportation Group provides solutions for data breach events, business interruption and network recovery, and social engineering losses associated with ransomware events.

Join our cyber webinar for transportation companies to learn best practices before and after a cyber event.

How USI Can Help

How cyber criminals infiltrate their victims can vary from one industry to the next. Therefore, it's critically important to develop cyber risk management strategies that are appropriate for your organization's infrastructure. Post-event solutions must match your circumstances and needs as well. Standard or "off the shelf" cyber policies have several inherent coverage gaps, which can mean uninsured losses for many organizations. These weaknesses can become especially pronounced in our current hard cyber insurance market.
To help clients mitigate the effects of the hardened cyber market, USI can:

- Engage strategic resources, including USI's E-risk Hub and Answerlytics curated providers, which provide cutting-edge risk management tools
- Lead a cyber risk management differentiation process, which focuses the conversation on markets around your positive cyber risk profile based on specialized criteria — not just against a class of business, a peer group, and other general data
- Leverage customized terms expertise through USI's exclusive PrivaSafe cyber program, which includes automatic expansions of key definitions such as "Computer System" to seek to encompass remote work and other evolving risks
- Provide analytical input around questions of limits, claims impact and cyber underwriting results and concerns through customized benchmarking tools for organizations above and below $1 billion in revenue.

Contact your USI representative to learn more about industry-specific cyber solutions designed to protect your organization from ransomware and other cyberattacks.

Introducing Answerlytics

Answerlytics™ is USI's proprietary cyber solution designed to reduce exposure to risk from urgent vulnerabilities and emergent threats, and bridge the gap between traditional cyber insurance offerings and the next generation of solutions. Learn more.

[1] VMware Carbon Black
[2] Business Insider, 2021
[3] USI's 2020-2021 Commercial Property & Casualty Market Outlook
[4] BakerHostetler Data Security Incident Response Report
[5] Neustar International Security Council
[6] Kaspersky Labs
[7] BlueVoyant, 2021
[8] Sungard AS
[9] CyberTalk.org, 2021
[10] Palo Alto Networks
[11] The Wall Street Journal
[12] Check Point Software Technologies