National Cybersecurity Awareness Month: *Understanding the Potential for Cyber Events*

If you are managing a business or organization, it is critical to realize that exposure to cyber risk is higher than ever.

Now in its 17th year, National Cybersecurity Awareness Month (NCSAM) begins this year on October 1. The campaign, a joint public/private venture between the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA), is held each October to raise awareness about cybersecurity and help Americans understand how they can use technology more safely and securely at home and in the workplace. Cyber risk awareness is more important than ever, given the COVID-19 pandemic and corresponding work-from-home environment, which has blurred the lines of Cyber security for many organizations.

Cyber Threats are a Click Away

This year's theme is "Do Your Part. #BeCyberSmart." In today's work-from-home environment, cyber attacks are rapidly increasing and contain hidden malware (destructive software) that can be activated on networks used by families for work, school, and play. This situation gives cybercriminals an entrée to employer, home or school networks and data through everyday online activities like visiting websites, opening emails, and clicking on links and attachments – which is why it is so important to "#BeCyberSmart."

In a recent study, IBM found that the cost of a data breach in the United States is $8.64 million—more than double the Property & Casualty Insight worldwide average ($3.86 million). IBM's research also shows that companies with fewer than 500 employees (small and mid-size firms, the majority of U.S. businesses) suffered over $2M million in losses on average during a Cyber event —a financial outcome that can devastate smaller businesses typically earning $50 million or less in annual revenue.[1]

In this COVID-19 environment, "Phishing" schemes, in which an unsuspecting worker may take a scammer's "bait" by opening a malware-tainted message or clicking on an infected link, have exploded. The September 2020 "Phishing Attack Landscape Report," published by Great Horn, reports that 53% of cyber executives have seen an increase in phishing attacks since the start of the pandemic and face an average of 1,200 phishing attacks a month. In fact, phishing attacks have become the most common vector for delivering many types of malware that trigger "Cyber Events."[2] This includes Business Email Compromise-enabling malware that seeks to scam money and data, and the most costly and devastating cyber event type at present, "Ransomware" attacks." In a ransomware attack, the user's network and all stored data and files are held "hostage" until the scammer's conditions are met.

The Human Factor

Schemes known as "Business Email Compromise/Email Account Compromise" (BEC/EAC), which are more sophisticated forms of phishing or social engineering attacks, are proliferating.

In BEC/EAC events, the scammers rely on system weaknesses and human error to gain access to a company's email systems. Once there, they seek to orchestrate a transfer of funds or access private information (including employee wage and banking information) by distributing email requests that impersonate trusted individuals (vendors, other employees, etc.) known to the organization and their individual target. Attacks of this kind have been reported in all 50 states and in nearly 200 countries. In fact, the average BEC target is now $80k, up from $54k in 2Q 2020, with some malicious groups seeking targets of $1M+.[4] It is because of scams like these that Americans are continuously reminded during National Cybersecurity Month that an individual action, something as simple as opening a compromised email, can result in data breaches, identity theft, and other cyber events. This is why vigilance at all levels within an organization is key to ensuring cybersecurity in the workplace, wherever that workplace may be.

Damages and Other Losses

Consider this: an employee of a company received a business email that appeared to be sent from a known and reliable vender. Without hesitating, the employee opened the message and clicked on an embedded link. The employee's computer, along with the business's entire network, became "locked" and a ransomware message popped onto the screen demanding $7,500,000 in cryptocurrency (Bitcoin) to be paid within 96-hours, or the network and its files would be destroyed. Because the company had not effectively backed-up its system, it was now at the mercy of the attacker.

Ransomware (aka Cyber Extortion) victims face losses that can go well beyond the cost of the ransom payment. With business interrupted, they may lose revenue and have penalties lodged against them from regulators, payment card companies and other groups or clients. They may face liability from third parties and gradually lose respect within their industry and with their clientele (leading to reputational loss). In fact, the cost of the average ransomware event has jumped to $4.44 million in 2H 2020.[5] Unfortunately, many companies do not have the technical resources or experience needed to effectively respond to a ransomware attack. This is where USI comes in.

Through its vast network of regional, national, and international cyber solution specialists, proprietary tools, and expertise in privacy and network risk, USI is well equipped to assess the threat at hand, work with carriers, and guide clients toward the best course of action. These are important components of the USI ONE Advantage®.

Luckily, the company in our example had previously engaged USI to assess its exposures to cyber loss. After analyzing the organization's assets, disaster recovery/incident response plans, data controls, and in-force insurance policies, USI structured a comprehensive cyber/privacy insurance program to address the firm's exposures. Following the ransomware attack, the company, its USI representatives, and insurance carrier experts, determined that paying the ransom would be the most reasonable course of action (as compared to rebuilding its network at prohibitive cost and timeline). The payment was facilitated through the cyber insurance program previously implemented by USI, which covered the ransom and all associated costs up to the policy's limits. Once the ransom was paid, the client's data was fully restored, and its business resumed.

Staying One Step Ahead

With National Cybersecurity Month underway and as the COVID-19 work-from-home environment continues, now is an ideal time to learn more about your company's cyber risks and how to mitigate them. To review best practices and access helpful resources, visit the National Cybersecurity Month website at https://www.cisa.gov/national-cyber-security-awareness-month.

To learn more about USI's Cyber Risk Management Services, reach out to your USI representative or contact us at pcsolutions@usi.com.

Sources:

1 - https://www.techrepublic.com/article/ibm-finds-cyberattacks-costing-companies-nearly-4-million-per-breach/
2 - https://www.securitymagazine.com/articles/93194-new-research-shows-significant-increase-in-phishing-attacks-since-the-pandemic-began-straining-corporate-it-security-teams#:~:text=Cybersecurity%20threats%20are%20on%20the,1%2C185%20phishing%20attacks%20every%20month
3 - https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
4 - https://www.zdnet.com/article/average-bec-attempts-are-now-80k-but-one-group-is-aiming-for-1-27m-per-attack/#:~:text=The%20average%20sum%20that%20a,industry%20report%20published%20on%20Monday.
5 - https://securityintelligence.com/posts/ransomware-attacks-how-to-protect-data-encryption/

This material is for informational purposes and is not intended to be exhaustive nor should any discussions or opinions be construed as legal advice. Contact your broker for insurance advice, tax professional for tax advice, or legal counsel for legal advice regarding your particular situation. USI does not accept any responsibility for the content of the information provided or for consequences of any actions taken on the basis of the information provided. ©2020 USI Insurance Services. All rights reserved.