Cyberattacks Continue to be a Threat in 2021

By: Jaki Ferenz, Vice President, Avalon Risk Management

A global pandemic did not stop cybercriminals from engaging in their illegal activities. If anything, they became bolder in their attacks. Cyberattacks were more prevalent in 2020, and it has cost consumers and companies billions of dollars in damages. According to consumer website Comparitech, cybercrime damages are predicted to cost up to $6 trillion this year. Is your company prepared in the event of a cyberattack?

Can you afford a cyberattack?

Costs for a cyberattack can quickly rack up to millions of dollars. According to the 2020 IBM Data Breach report, in the transportation industry, the average cost of a data breach was $3.58M. The average cost for a company with less than 500 employees is $2.35 million. This is a staggering amount of money, even for large corporations.

Common Cyber Crimes

Cybersecurity firm Varonis indicates that some of the most common cybercrimes are:

- Social Engineering
- Ransomware

Social engineering happens when people are manipulated into performing specific actions or divulging confidential information and can be done through various schemes. The most common type of social engineering is phishing. Phishing is the number one type of threat action involved in data breaches (Verizon's 2020 Data Breach Investigation Report).

Phishing is the fraudulent practice of sending emails that appear to be from reputable companies/individuals to deceive people into revealing confidential and personal information such as credit card numbers. The email usually contains a malicious link or an infected attachment. Unfortunately, smaller organizations tend to receive malignant emails at a higher rate.

Here is an example of a phishing email. An accounts payable employee received an email from an agent who they had worked with for several years. The agent advised they had changed banks and to send payments to the new bank. The accounts payable employee followed the email's instructions and issued payment for a new invoice to the new bank. A couple of weeks later, the agent advised that payment was never received. After some investigation, the company determined they had been hacked, and they sent the payment to a bank in another country.

Some of the most frequently used subject lines in phishing attacks are:

- Payment Status
- Invoice Due
- Direct Deposit

- Payroll
- Urgent/Important

Ransomware is a type of malware that encrypts a victim's files so the victim cannot access them. The cybercriminal then demands a ransom to restore the data and/or stop publishing sensitive data. The average ransomware payment rose 33% in 2020 to $111,605. Ransomware damage costs will rise to $20 billion, and a business will fall victim to a ransomware attack every 11 seconds (Cybersecurity Ventures).

In 2020, several logistics and transportation companies became victims of ransomware attacks. These attacks affect the company, its customers as well as disrupting entire supply chains. Some of the most notable victims were TFI International, Forward Air, and CMA CGM. Ransomware attacks are not just limited to larger companies but small to medium companies as well. A recent Freightwaves article discusses how a small trucking company fell victim to a cyberattack, and the company was hit with a $300,000 demand. The company thought it would not be an attractive target for a ransomware attack due to its size; however, the company was still hacked. Since they did not pay the ransom, sensitive data was leaked on the dark web.

Mitigate Your Cyber Risks

Now more than ever, it is imperative for companies to protect themselves against the threat of cybersecurity regardless of company size. Here are some tips that can help mitigate your cyber risk:

- Implement a Cyber Security Framework – Identity, Protect, Detect, Respond, Recover
- Educate and train employees on cybersecurity
- Install anti-malware and other anti-virus software
- Ensure proper configuration and patch management of your applications
- Manage user privileges
- Use secure protocols – Encryption, VPN
- Unique user IDs and complex passwords
- Multi-factor authentication
- Vet carriers and other third parties who access your systems
- Control devices and remote access
- Add cybersecurity to your contracts
- Get the proper insurance

Insurance for Cyber Risks

It is crucial to think about what you would do if your customer data were compromised. Would you be able to afford the expense of notifying your customers if there is a security breach? What if they decide to file a lawsuit because of the breach?

You need to review your cyber risk insurance and determine if you have the right coverage for your business. We hope you can join me, Mike Brown and Keith Sanchez on March 23rd as we host a cyber webinar, "Cyber Hackers Are Working Hard! Is your Policy Working for You?" Click here to register.

If you cannot join us on March 23rd, a recording will be available, but registration is required!