PREVENTATIVE MEASURES

Tips for avoiding cybercrimes

BY ROBERT C. WILEY

Cyberattacks are showing up increasingly in the news. Some hackers are targeting large businesses, such as Target and Amazon, as well as municipalities like cities and police departments. But most hackers are pursuing small businesses and organizations. In fact, data from Osterman Research found that small and medium businesses were increasingly victimized. The report, which presented findings on ransomware and security issues from over 1,000 small and medium-sized organizations, discovered:

- 35 percent were victims of **ransomware.**
- 22 percent had to cease business operations immediately because of **ransomware.**
- 81 percent of businesses have experienced a **cyberattack**.
- 66 percent have suffered a **data breach**.

Note that these numbers only represent reported attacks. The actual number is higher, since many victims do not report cyberattacks to the proper authorities.

These small and medium-sized businesses include real estate appraisers. The contents of most appraisal files do not hold personal sensitive information, such as Social Security numbers and bank accounts, but that doesn't preclude appraisal firms from being targets. Businesses of all sizes will remain at risk from hackers, with small to mid-sized businesses being lucrative, easy quarry.

A hacker's goal using ransomware is to hold your data hostage by shutting down access to your own files and demanding typical ransom amounts from $2,000 to $50,000 in bitcoin currency. Once the ransom is paid, they release your files. Add to that the cost of recovery and it's no wonder that within six months of an attack, 60 percent of small companies go out of business.

Here are valuable tips from the Department of Homeland Security on protecting your data from hackers and ransomware attacks:

What can I do to protect my data and networks?

- **Back up your computer.** Perform frequent backups of your system and other important files, and verify your backups regularly. If your computer becomes infected with ransomware, you can restore your system to its previous state using your backups.

- **Store your backups separately**. Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive or separate device from the network or computer.

- **Train your organization**. Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training sessions to ensure their personnel are informed about current cybersecurity threats and threat actor techniques. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails.

What can I do to prevent ransomware infections?

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or

the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites by using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files. Be wary of unfamiliar files from sharing platforms such as Dropbox.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up-to-date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website (https://apwg.org/). You may also want to sign up for CISA product notifications, which will alert you when a new alert, analysis report, bulletin, current activity or tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls and email filters and keep them updated.

Cyberattacks are a real threat to firms and professionals in the valuation industry. This concern is shared by LIA Administrators & Insurance Services and our legal and association partners. Our web consultants are appraisers who run a software business assisting valuation professionals. They report that on a weekly basis, they receive calls from businesses that think they might be under a cyberattack and are asked how they should handle it. The truth is, many individuals and businesses that have been hacked don't report it or tell anyone. I am surprised at the number of businessmen and women (whom I consider as tech-sophisticated) who have suffered from a ransom attack. This includes consultants, a well-known appraiser software company, real estate agencies, large appraisal firms, etc. We even had one of our appraiser insureds call us to say that he was hacked and that we shouldn't open any Dropbox attachments sent from his email address. It just goes to show that it's very important to take precautions and educate yourself and your business when it comes to cybercrimes.

LIA is now including an indication for cyber coverage to all our E&O appraiser clients. This policy aims to protect you and your business from the costs of ransomware, phishing, or social engineering attacks and data breaches. We offer very competitive premiums combined with broad benefits including data privacy liability, network security liability, e-media liability, notification expense/credit monitoring expense, crisis management expense, data privacy regulatory expense and cyber investigation expense. Our experienced team of underwriters work with your management team to develop comprehensive, cost-effective insurance solutions. ✪

Robert C. Wiley is President of LIA Administrators & Insurance Services. Visit our website www.liability.com to learn more.