Claims®

COVERING THE BUSINESS OF LOSS

October 2018
Volume 66 . Number 10
PropertyCasualty360.com

An ALM Publication

P. 20 MASTERING CYBERSECURITY

+

Cyber criminals target government entities
P. 25

Changing face of cyber claims
P. 30

Recovering from a cyber event
P. 34

Claims Luminary of the Year
P. 36

Managing new technology
P. 39

By Jenean Meier

Cybersecurity Starts in the Workplace

According to research sponsored by International Data Corporation (IDC), businesses worldwide will spend more than $100 billion on cybersecurity software, services and hardware in 2020. Of this amount, IDC estimates one-third will be spent by businesses in the United States.

To a certain degree, fear is driving this financial commitment. No management team wishes to be the next Equifax, Target, Sony or Yahoo, forced to report a massive data breach to shareholders, strategic partners and customers.

Of course, the damage caused by a cyberattack can extend far beyond a tarnished reputation. According to the U.S. Department of Defense Science Board's "Resilient Military Systems" report, as interpreted by Flashpoint, regarding a catastrophic Tier 6 cyberattack: "Kinetic and cyberattacks conducted by threat actor(s) have the potential to cause complete paralysis and/or destruction of critical systems and infrastructure. Under such circumstances, regular business operations and/or government functions cease and data confidentiality, integrity and availability are completely compromised for extended periods."

Preventing cyber mayhem

While there is no doubt much of the $100 billion in cybersecurity spending will be devoted to effective defenses against cybercriminals, companies should also invest in low- to no-cost common sense actions to anticipate cyber intrusions from bad actors.

Although external actors are responsible for much cyber mayhem, company insiders are responsible for 60% of cyberattacks according to a report published by IBM. Who is a company insider? The answer extends far beyond company employees. It includes anyone who possesses credentials enabling physical or remote access to a company's digital assets.

The beginning of a solution is found in the selection screen. Provide credentials to access sensitive digital assets only to individuals who have earned your confidence. What's more, provide credentials only to those individuals who absolutely need to have them. If an employee or contractor is fired from or chooses to leave your firm, block access to digital assets immediately.

shutterstock.com/vectorfusionart

As a rule, treat portable drives with the same respect given to a rattlesnake. An employee or contractor who copies digital assets onto a portable drive and later slips it into his or her pocket can do as much damage as a hacker who infiltrates your IT system from a remote location. Even an otherwise well-intentioned employee or contractor could unknowingly introduce a virus into your IT system by inserting an infected portable drive into a port.

> As a rule, treat portable drives with the same respect given to a rattlesnake.

Individuals perpetrating ransomware cannot restrict access to your company's computer system without the support of employees and contractors. Frustrate these awful criminals' efforts to hold your company's digital assets hostage by following these rules of thumb:

- Train contractors and personnel to recognize bogus e-mails and advertisements.
- Stay current on all IT protection systems, including anti-virus software.
- Instruct all individuals logged into your IT system to not click on unknown e-mails or attachments.

The high cost of "free" Wi-Fi

Employees and contractors should exercise the greatest caution before accessing your company IT system via a Starbucks, Panera Bread, train station, hotel or any other public hotspot, since 95% of Wi-Fi traffic is unencrypted. Your company's digital assets will become vulnerable if the hacker deviously working at the next table or across the lobby penetrates your corporate server. Following are a few rules of thumb to manage this risk:

- As Facebook users have lately realized, there is no free lunch. This includes any network labeled "Free Wi-Fi." Don't accept this particular form of charity, and instead create your own personal hotspot with your wireless device.
- Before logging in, set all websites to "HTTP secure."
- Use a VPN before logging into a company network.
- Do not access personal financial accounts via a Wi-Fi hotspot. In fact, anytime a user name and password are required to gain access to a website, put the time to better use by stretching your legs and walking to the counter to order a cup of coffee and nice piece of cake.

Finally, hopeful optimism is not a positive personal attribute when it comes to cyber attacks. Since there is every chance your company will someday be the victim of cyber crime, all individuals with access to your company IT system should be placed on high alert.

Jenean Meier (jmeier@kmrdpartners.com) is a claims advocate at KMRD Partners, Inc., a nationally recognized risk and human capital management consulting and insurance brokerage firm located in the Philadelphia region and serving clients worldwide.