Inside Counsel

Cybersecurity Attacks Are on the Rise

BY AMANDA CICCATELLI
JULY 5, 2017

As telecommuters grow in number, so does the potential for cyber breaches caused by lax cyber security habits.

Global cyber security attacks such as the Wannacry ransomware outbreak make headlines, but small and medium businesses are also vulnerable to cyber threats originating from their own employees, especially those who work remotely. As telecommuters grow in number, so does the potential for cyber breaches caused by lax cyber security habits.

In fact, a new report from the FBI's Internet Crime Complaint Center (IC3) puts the financial loss from cybercrime in the United States at more than $1.3 billion in 2016, a rise of 24 percent. And, 43 percent of Americans spent at least some time working remotely last year, according to Gallup's State of the American Workplace report.

With so much of the world's business conducted online, it's inevitable that cybercrime is on the rise. But businesses can take proactive measures to safeguard against potential cyber threats, including ensuring they have adequate cyber liability insurance coverage and educating their staff on best cyber security practices for working remotely. Examples include: implementing smart and safe password practices; using VPN software which allows remote workers to securely access the Internet and; turning off Wi-Fi on your devices when you don't need it, which prevents them from automatically connecting to available Wi-Fi hotspots.

CONTINUED NEXT PAGE

Parker Rains, VP of Fisher Brown Bottrell Insurance, recently sat down with Inside Counsel to discuss ways businesses can diminish the risk posed by cyber threats as well as the differences between general business liability and cyber liability insurance, which is on the rise.

The internet is no longer in its infancy and neither are today's hackers. "They use sophisticated techniques, from viruses to phishing, to gain access to personal data, such as financial records, email addresses, passwords, dates of birth and Social Security numbers," he said. "With the latest ransomware attack, Petya, spreading across the globe right now, we're seeing major U.S. companies like pharmaceutical giant Merck and law firm DLA Piper being affected."

As more employees work remotely, it becomes increasingly difficult for employers to enforce cybersecurity protocols. Employees working from their neighborhood coffee shop are likely using public Wi-Fi, which poses a huge risk, and hackers have several ways to infiltrate these networks.

"For example, they can create their own public Wi-Fi networks with names that look like the one a user is expecting to join—like the coffee shop's name or a nearby shop or hotel," explained Rains. "The hacker can then monitor all the victim's activity, gaining access to passwords, credit card numbers and other sensitive data. Human error leads to many loopholes in security and oftentimes employees themselves can pose the biggest security threat to companies."

So, what are some proactive measures businesses can take to safeguard against potential cyber threats?

There are many proactive measures businesses can take—and should be taking—to safeguard against potential cyber threats. According to Rains, update anti-virus and anti-malware software frequently to ensure there are no gaps in your cyber security; train employees on proper updating protocols; make sure passwords are strong; make sure your employees use different passwords across platforms and update them regularly by establishing and enforcing a strict password policy and; secure your communications by setting up a secure server to encrypt and decrypt communications within your company.

CONTINUED NEXT PAGE

In addition, Rains advises developing a detailed action plan that you can launch in the event of a cyber-attack. This will ensure your company is prepared to take actionable steps, such as communicating details of the breach to employees and implementing required employee action to minimize further damage.

"Identify various breach scenarios and ask (and answer) questions like, 'Who will deal with the technology aftermath?' and 'Who will inform clients?' he explained. "Document your responses and share your plan with employees. It's important to test the plan and revisit it regularly—at least annually—to make sure it's up to date."

Lastly, be sure you have adequate cyber liability insurance coverage. A lot of business owners don't realize that cybercrime isn't covered by their general business liability policies. A general liability policy covers against any general third-party claims of things like bodily injury or property damage, but it doesn't extend to things like workers' compensation claims or cyber-attacks.

Further reading:

- Legal Departments Can Take the Lead When Workplace Disaster Hits
- Traveling with a Laptop: What In-House Counsel Should Know
- Is the "Halo Effect" Making Angels Out of Infringers?
- LinkedIn Spars With Data-Mining Company Over Access to Profiles