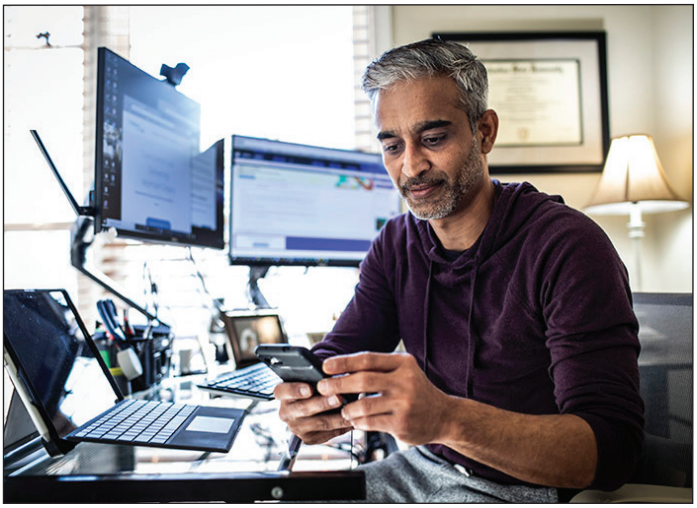
RISK&INSURANCE
Affiliated with THE INSTITUTES

10 Ways Companies Can Protect Against Cyber Attacks When Employees Are Working at Home

The increased amount of employees who work from home have heightened the potential of already prominent cyber risks. Here are 10 ways to diffuse them.

By: Annemarie Mannion | November 2021



The COVID-19 pandemic eventually will wane, but it appears some of its effects will become lasting, including more employees working from home.

The remote-work trend can make companies more vulnerable to cyber security threats, especially because home internet connections are generally less secure than those in an office environment, and employees may be more at risk of falling prey to cyber criminals, from both social and technology standpoints.

The good news, according to Gwenn Cujdik, claims manager for cyber incident response at AXA XL, a global commercial insurance and reinsurance company, is that companies are aware of the increased threats and are seeking to bolster their cyber security defenses.

"Cyber security is certainly on the radar for most businesses and companies, especially since COVID," Cujdik said. "The challenge is to make sure that their data and network are safe and secure."

Cujdik offers ten tips on how to prevent cyber attacks, especially when employees are working at home:

1) Training Against Phishing

"The human element is something that the bad guys will always try to take advantage of," Cujdik said. "That is something that even the best tools sometimes can't overcome. People fall victim to social engineering events, downloading malicious software or having their credentials compromised."

The best way to help employees understand the threat is to train them in how to recognize the dangers, understand the bigger picture of how a cyber attack can adversely impact their organization, and encourage them to ask questions or seek input if they receive a suspicious email, or have another question about cyber security.

"Training is a huge thing that we often advise companies to do," she said. "They also need to make sure they are up-to-date on the latest cyber security threats and are consistently training employees about cyber security."

She said that training done virtually is just as effective as an in-person session.

"Virtual training is great," she said. "The important thing is to conduct trainings regularly."

2) Raise Awareness

Keeping employees aware of a challenge such as cyber security can be easier when people are working in the office, but it is still possible to raise cyber security awareness for employees working at home.

"Companies can and should take advantage of the technology they have such as sending emails about cyber security or using company screen savers or pop-up banners to remind colleagues of training sessions or other efforts focused on enhancing cyber security," she said.

Many companies also host cyber-security focused events during the month of October, which is widely recognized as cyber awareness month. Holding regular coffees or other virtual events to reinforce the importance of maintaining cyber security can also help raise awareness.

"It's a great way to connect with each other and it's also a way to continue the virtual trainings that can keep employees on top of evolving cyber security threats," she said.

3) Take Advantage of Third-party Training Programs and Software

Cyber security training programs do not have to be created from scratch. Cujdik said there are many programs that simulate real-life scenarios to help employees improve their cyber security game.

"Third-party training programs for phishing help companies understand how to prevent cyber security events by simulating phishing. A lot of IT companies are using third parties to help bring awareness of phishing events."

4) Password Complexity

Cujdik said companies should require employees to use complex passwords and to rotate them. Employees should never use the same passwords for their professional and personal lives.

"Using the same password for personal use and professional work is a huge danger because it is easier for those passwords to be compromised," she said. "Cyber criminals can get access to a network and try to elevate their access from a standard user to an administrator, which essentially gives them the keys to the kingdom."

5) Multi-factor Authentication

A common example of multi-factor authentication is to use a password in combination with a code sent to a smartphone so an employee can authenticate themselves.

Cujdik said multi-factor identification is another good way to prevent a cyber attack.

"Even if a password is compromised in some way, there is a backup solution in place that catches it and keeps people from logging on to the environment," she said.

6) Endpoint Detection Response Tools & Managed Detection & Response Services

Cujdik noted that a lot of companies use endpoint detection and response (EDR) tools which may rely on artificial intelligence and other tools to keep their companies and networks safe.

She suggested taking it a step further and consider using a managed detection and response (MDR) service, which are service providers who specialize in monitoring the EDR tools.

"That's a group of professionals who are watching out 24/7 for viruses and known threats, and also for other, less common threats," she said.

"There are a lot of different pieces of malware that the EDR tools might not catch that the MDR will catch," she added. "They can alert the company that something is happening that doesn't seem normal and say 'Let's talk about this and cut it out before it gets to be something like a ransomware attack.'"

She noted that many companies are deploying Endpoint Detection and Response Tools, with the managed detection resource as an added component.

7) Patching Firewalls and VPN

"This summer we saw a big spike in vulnerability of firewalls and people trying to get in through the VPN," Cujdik said. "Having that patch and making sure that you constantly have the most up-to-date configurations for those security features is really important."

"After you install a firewall or VPN, you have to maintain it and make sure you're on top of the latest updates and patches."

8) Minimize Remote Access

Remote access to a computer should be limited to minimize intruders accessing your network through a remote desktop portal.

You should limit remote desktop access to trusted sources, such as your IT department. Many employees, especially those working off-site, may rely on their IT department to remotely access their laptops to help them solve any technical issue that may arise. While that ability is often valued by employees, Cujdik said it needs to be protected.

She suggested requiring access to remote services through a VPN and using multi-factor authentication to enforce defenses.

9) Keep Professional and Personal Use of Work Computers Separate

"When employees are working at home there can be a huge blurring between professional and personal lives," Cujdik said. "Employees want to make sure they are keeping them separate. A work laptop should be for work only. An employee shouldn't be accessing personal websites or going on the Internet scrolling websites in their spare time."

She said employers should track employees' work computer use, and let them know when a problem arises.

"You should be looking into whether employees are going to risky sites, and keeping an eye on what they are downloading, which can be done very easily through their IT department."

Employers should notify employees when they notice them using a computer inappropriately. In many instances, companies have installed firewalls that prohibit downloading software or access to risky and malicious sites to ensure employees adhere to company security policies.

If something slips through the cracks, the IT department should make sure to communicate with the individual and remind them that certain things need to be approved by the company or, for example, say 'I saw that you visited this website and that is a risky website. We want to remind you that you have to abide by company policies regarding securing our systems and network.'"

10) Back Up Data

Cujdik also advised companies to back up their data in an environment that's segregated from the network so they can recover that data if needed. **&**