PATRIOT
GROWTH INSURANCE SERVICES

Latest Edition: Industry Insider

April 15, 2020

5 Steps to Help Address Security Risks for Your Remote Workforce

As many businesses shift to a work from home model, numerous concerns jump to the forefront of employers' minds. Maintaining good communication, productivity, and morale will likely take precedence, but employers can't afford to overlook the heightened security risks when deploying a remote workforce.

The following are several steps employers can take to manage the heightened security risks of a remote workforce:

1. **Educate employees on basic security.** It may seem like a given that employees shouldn't click on links that come from unfamiliar email addresses, but this may become a gray area if employees are using their personal emails outside of the office for work-related tasks. Employees may not realize certain emails aren't legitimate so it's important to establish basic security protocols like only using work email accounts, being more vigilant than ever of phishing scams, and only using secured, personal Wi-Fi-routers. Employees should also avoid using USB sticks whenever possible. While they're popular because they make it easy to transfer data from one device to another, they're also rife with security problems.
2. **Make it mandatory for employees to use a VPN**. Virtual private networks (VPNs) allow public networks (like employees' Wi-Fi at home) to access private office networks. VPNs are useful for enhancing security as they can encrypt data transferring back and forth, conceal the employee's IP address, and hide their location from would-be hackers.
3. **Prepare IT workers for internal cyberattacks**. While VPNs increase security, they're not infallible. Many employers already use VPNs for their office locations so IT departments are used to attacks coming from external sources trying to gain access. When employees connect their personal devices from home to the company's VPN, any attempted breaches will appear to be coming from within the network itself. Being alert for this shift will allow IT workers to put security measures in place to catch and thwart any attempted breaches through employees' personal devices.
4. **Utilize secured cloud services**. Employees' devices are going to be the least secure location for information, but many don't have alternate storage options for work files and data. Using secured cloud services can give employees a location to save, upload, and exchange data without relying on employees' unsecured local storage.
5. **Update passwords**. Employees know they need to use strong passwords for their personal apps that access sensitive data such as banking, insurance, and so on, but they may not put such security emphasis on their work logins. Many grow complacent that the office's existing security will protect them. Moreover, having to use complicated, protracted passwords on a regular

basis can feel burdensome. However, remote devices are at a much greater risk for security breaches than those within the office. Now, more than ever, employees need to update their passwords to be alphanumeric without common words like *password* or *qwerty*. Requiring two-factor authentication (2FA) to gain access to networks can also help ensure the validity of who is utilizing it.

All businesses know security is a critical component of a successful risk management plan, but COVID-19 has forced many companies to shift to a remote workforce with little notice. This means many didn't have adequate time to test network security or train staff on best practices to reduce their risk of falling victim to phishing emails, malware, ransomware, and more. Patriot Growth Insurance Services understands that the risks businesses face are greater than ever during these uncertain times.

Contact us to learn how Patriot and our partner agencies can help protect your company.