Northbridge® Insurance

# RISK INSIGHTS

## 7 TIPS TO HELP PROTECT YOUR BUSINESS FROM THE RISKS OF REMOTE EMPLOYEES

**With a rapid increase in telecommuting, every device, email server, and Wi-Fi network accessed outside of the business network is a new potential access point or vulnerability for hackers to exploit. Business leaders must establish strict policies and employee guidelines to avoid a cybercrime crisis during this unprecedented push to work remotely.**

### FOLLOW THESE SEVEN TIPS TO REDUCE THREATS:

**Issue security policy guidance and rules**

Annual trainings and email reminders from the IT department are not enough to keep good cyber habits top of mind for employees. A fresh reminder can go a long way to reinforce security best practices.

**Set up a VPN**

A virtual private network (VPN) system creates an encrypted tunnel that your internet traffic travels through so it can't be seen by third parties. Setting up a VPN can seem daunting, but it only requires a couple hours to configure and isn't technically difficult. VPN with multifactor authentication should be used as it is the strongest defense.

**Require use of encryption and Wi-Fi protected access (WPA) to Secure Networks**

While no Wi-Fi is totally secure, private, password protected networks are significantly more secure than public Wi-Fi networks—especially those offered in cafes, hotels, and other public places. You can always ask a business that offers public Wi-Fi if private password protected networks are available.

**Password-protect devices used by employees and third parties**

Require employees to use strong passwords that contain letters, numbers, and special characters. Avoid using the same password on multiple devices/accounts.

**Maintain anti-virus and anti-malware software**

Remind employees to install and regularly update adequate security software on all electronic devices they use to perform work remotely. That could include a phone, tablet, laptop, etc. Some employers are eliminating bring your own device (BYOD) options and mandating that employees use only employer-supplied equipment and devices.

**Power down**

Encourage employees to power down computers when not in use. While powered off, computers are not accessible or susceptible to attacks or intrusions from the internet.

**Back-up data**

Regularly back-up sensitive information and, depending on the importance of the data, make sure it is encrypted. Secure back-ups are the best strategy to prevent critical business disruptions in case of a ransomware attack.

For more information on making your business safer, contact our Risk Services Department at **1.833.692.4111** or visit us at **www.nbins.com**.



CYBERSCOUT®