Work-From-Home Employees Are Increasing Your Company’s Overall Risk

The abrupt and sudden change to a remote workforce as a result of the COVID-19 pandemic created various lasting impacts on companies of all sizes. Within a few days’ time, companies and employees had to make an immediate transition to doing their jobs from home.

Teams without any remote working experience had to pivot and quickly adapt to their new situation. For many companies, there was not enough time to adequately address the new security vulnerabilities that were a consequence of this rapid shift. Using personal devices for work, accessing the internet through home networks, conducting meetings via videoconferencing software, and accessing company and customer data from home are all inherently risky from a cybersecurity standpoint.

Now that it appears that the shift to remote work may be a permanent situation, even on a part-time basis, companies will need to establish more substantial security solutions for their remote teams. Global research leader Gartner recently noted that securing the remote workforce “has now become the single greatest existential imperative for all organizations in the wake of COVID-19.”

Criminals quickly seized on cyber vulnerabilities

Security vulnerabilities from remote work have many implications and have already caused significant disruptions in organizations. After the rapid shift to remote work, it wasn’t long before cyber criminals took advantage of the chaos that erupted. The FBI reported a 400% increase in cyber attacks from pre-COVID-19 levels, or nearly 4,000 reports per day. Some IT security reports showed that cyber threats increased by 800% in some organizations.

Recent victims of cyber attacks include organizations of all sizes, including several high-profile corporations. IT security experts report that many of the attacks targeted corporate email and social media. Network threats included ransomware, spyware, phishing, and other malicious attacks. Meanwhile, the pandemic also resulted in a surge in schemes involving social
Engineering, defined as a cyber attack that employs deception or trickery instead of technical hacking techniques, to gain access to networks, systems or data.

**Security solutions for remote work**

Cybersecurity best practices for employees who are working from home should focus on key areas such as devices, internet connections, storing and transferring data, and videoconferencing.

- **Device security**: Device, or endpoint, security involves setting security protocols for laptops, desktops, tablets, smartphones or other devices that connect to the internet and store or transfer data.
- **Internet connections**: Many cyber attacks and hacking incidents are related to the use of insecure public Wi-Fi.
- **Videoconferencing**: There have been widespread reports of security breaches tied to videoconferencing applications such as Zoom and Cisco Webex. Hackers accessed confidential meetings and information communicated or transferred in remote meetings.
- **Storing and transferring data**: Data can be compromised when transferred via insecure channels, such as messaging apps or over unsecured networks.

IT departments are often tasked with the responsibility of establishing security plans, protocols and solutions. However, management teams should also be involved in implementing and communicating protocols and solutions for employees who are working remotely.

Companies new to allowing remote work can establish a remote-working policy as well as a cybersecurity best practices guide for employees to use while working from home on their own devices and networks.

**Protocols that help mitigate cybersecurity risks**

Here are some common security protocols that can help to mitigate the cybersecurity risks encountered when working from home:

- Access the internet from private, password-protected connections and Wi-Fi only. This can include a mobile hotspot set up by your internet provider. Avoid using open public Wi-Fi connections that can be vulnerable to hackers or other cyber criminals.
- Protect devices and endpoints with antivirus and anti-malware software.
- Maintain recommended safety protocols when using videoconferencing software, such as password-protected sessions and using the waiting room protocol to approve attendees.
- Use secure passwords and two-factor authentication for devices and apps.
• Prohibit employees from disabling passwords or other measures and from using devices that aren’t password-protected.

• Ensure that employees keep the operating systems and software on their devices updated, and prohibit the use of outdated devices, as they are a security risk.

• Take extra security precautions when transmitting data. Do not transfer data over messaging apps or over an unsecured connection.

• Make sure employees are trained to recognize corporate phishing emails and how to avoid opening malicious emails.

• Make sure employees are aware of social engineering risks and scams.

• Take extra precautions to protect confidential information from anyone outside of the company, including family members of employees who may unintentionally have access to that information.

Companies should consider developing a written guide or a visual presentation that is easy to access and distribute to employees quickly and efficiently. Employees and teams can also benefit from training and interactive sessions so that they know how to conduct cybersecurity checks. Training also reinforces a culture of security and security practices.

Implications for business insurance from remote work

The shift to remote work has also resulted in changes to business insurance considerations, largely because the type of many companies’ business activities and nature of the workforce has changed.

Your insurance professional can help you conduct policy reviews and evaluations, which are necessary especially as remote work continues for an extended period. Policies and coverages may need to be modified to reflect this significant change. Insurance agents and brokers can ensure that the policy coverage is aligned with your company’s business activities, goals, and strategies.

A number of policy and coverage types are likely to be affected with a shift to remote employees.

Cyber liability: Insureds will need to confirm if their policies will cover incidents related to networks or devices that are owned by their employees. This includes both first-party and third-party liability (for example, a breach or loss of the company’s own data versus a company’s customer data). While business liability policies may cover some data loss, a separate cyber liability policy may be needed to cover additional risks.

Crime insurance policies: Insureds should have coverage and policies evaluated to ensure coverage of criminal activity, such as fraudulent transfer of funds. These risks could change or increase when employees are working from home.
Workers’ compensation: A workers’ compensation insurance policy may have been written to cover employees at a primary work site, not at their own homes. Leaving this wording untouched could result in a big coverage gap.

Commercial property: Businesses should verify if losses related to company-owned equipment are covered if the loss occurs off company premises or in an employee’s home.

The pandemic has created a permanent change in the work culture. Gartner and other workplace researchers project that 82% of organizations will allow their employees to continue to work from home in some capacity even after the pandemic.

Companies will need to take a proactive approach to cybersecurity in order to protect themselves from the various new losses that could occur. Cyber attacks continue to grow more sophisticated and advanced in their tactics each time security measures are put into place. Modernizing security protocols, installing software patches and updates, and instituting monitoring procedures for systems access are all vital steps to protect your company.

But beyond that, a broad range of insurance coverages should be reviewed in light of new work sites and workforce procedures.

Colleen Lazanich, CIC CRM
831.824.5002 - C: 707.888.0511
colleen@cal-insurance.org

CalNonprofits Insurance Services
1500 41st Ave, Suite 280
Capitola, CA 95010
www.calnonprofitsinsurance.org

Corporate License 0827761

This message and any attachments may contain confidential information intended for a specific person. If you received this email in error, please notify the sender and delete the message. Failure to maintain the confidentiality of this email may subject you to penalties under applicable law. The recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email. Any quotes discussed in this email are contingent upon approval by the carrier.

This content is for informational purposes only, should not be considered professional, financial, medical or legal advice, and no representations or warranties are made regarding its accuracy, timeliness or currency. With all information, consult with appropriate licensed professionals to determine if implementing any recommendations would be in accordance with applicable laws and regulations or to obtain advice with respect to any particular issue or problem.

Copyright © 2020 Applied Systems, Inc. All rights reserved.