RISK INSIGHTS Technology

Ives Insurance Brokers Ltd.

Remote Work Cyber Security

The recent significant increase in employees working from home as a result of the COVID-19 pandemic brings with it an increased risk of cyber security threats. Cyber criminals are well aware that IT departments and cyber security groups are stretched thin during the pandemic, making them more exposed to attacks.

In fact, according to a recent survey, one organization saw phishing and cyber attacks rise by 40 per cent. With 25 per cent of Canadian organizations now going entirely remote and 85 per cent going remote with at least half of their workforce, it's important to keep cyber security measures up in this new landscape of increased remote working.

Cyber Security Tips for Employees Working From Home

Take the following tips into consideration for your remote workforce:

- **Develop a remote work policy specifically for the pandemic.** Consider developing a new, written work from home policy that goes into effect only during the current pandemic. This policy can account for all special considerations that are different from your original policy, which may need to be reverted back to once the pandemic ends.

- **Connect to a virtual private network (VPN) if possible**. A VPN can provide a direct connection to the organization's normal applications, similar to if the employee was connected directly to the organization's network. This can hide the user's IP address, encrypt data transfers in transit and mask the user's location. If the organization already has a VPN, ensure that it can handle the extra bandwidth from the sudden influx of new remote users.

- **Ensure software is updated**. All devices being used for work should be secured with up-to-date firewall, antivirus, anti-malware and data encryption software.

- **Enforce basic cyber security practices.** Reinforce the importance of basic cyber security practices, such as using strong passwords and connecting to a hot spot or encrypted web connection instead of public Wi-Fi.

> Cyber criminals are well aware that IT departments and cyber security groups are stretched thin during the pandemic, making them more exposed to attacks.

- **Train how to detect a phishing attack.** Educate staff on how to recognize a phishing attempt, such as emails that request private information, use a generic introduction rather than your name, have spelling errors or use a suspicious email domain.

- **Avoid using removable media**—The use of removable media such as USBs, SD cards and discs may expose valuable resources to malware and virus replication, theft and hardware failure. Keep the use of removable media to an absolute minimum and

This Risk Insights is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

never use it as the sole storage location of valuable data.

- **Enable multifactor authentication.** In addition to a strong password, require that employees enter a code that they receive separately (such as via a predetermined mobile phone number) if possible to decrease the risk of unauthorized access.
- **Limit employee access.** Rather than allowing employees access to all programs and resources, grant them access to only the programs and resources that are essential to their duties.
- **Send contact reminders**. In the event of stolen materials or identifying a possibly malicious link, the switch to remote work may create uncertainties as to how to contact the IT or cyber security team. Send your employees a reminder with the proper contact information for IT-related questions or concerns.

For More Information

Cyber security is a serious issue for your organization and its employees. As such, it’s important that you recognize potential vulnerabilities and take steps to prevent a cyber attack on your workplace.

For more information on cyber security and working from home, contact Ives Insurance Brokers Ltd. today.