CYBER INSIGHTS

HENDERSON INSURANCE

NAVACORD®

Cyber Security Tips for Business Travellers

Organizations face heightened cybersecurity risks when their employees travel. Business travellers are prime targets for cybercriminals, as they often carry valuable data and may not always be careful about securing their devices.

This article discusses key cybersecurity exposures for business travellers and outlines steps employers can take to mitigate these risks.

Cybersecurity Threats While Travelling

Business travellers' laptops, smartphones and tablets are particularly susceptible to data breaches, loss and theft. Some common cyberthreats that business travellers may encounter include:

- **Unsecured Wi-Fi networks**—While convenient, public Wi-Fi networks are unsecure and can allow cybercriminals easier access to connected devices (as well as the data stored on them) than private Wi-Fi networks.
- **Publicly accessible computers**—Business travellers sometimes find the need to use their login credentials to access accounts on public computers. However, public computers often lack sufficient security capabilities and may even be infected with malware.
- **Stolen or misplaced devices**—Theft or loss of devices is a major threat to business travellers, as this can result in the exposure of important data. Devices could be lost or stolen in airports, hotel lobbies, conference rooms or rental cars.

How Employers Can Mitigate Cybersecurity Risks

Neglecting cybersecurity when employees are on the road or abroad can be detrimental to a business. In fact, the latest Cost of a Data Breach Report from IBM and the Ponemon Institute found that a single data breach costs a business $4.24 million on average.

Here are some measures employers can implement to minimize cybersecurity risks for business travellers:

- **Establish Wi-Fi policies.** Employers should have policies in place requiring employees to confirm the network name and precise login procedures with the appropriate staff before connecting to public Wi-Fi networks in airports or hotels. Sensitive activities, such as banking or confidential work-related projects, should not be conducted on public Wi-Fi networks. Auto-connect should also be disabled so devices don't connect to Wi-Fi networks automatically.
- **Enforce Virtual Private Network (VPN) use.** Via a VPN, all online traffic is routed through an encrypted virtual tunnel. Such a network can help can reduce the risk of cyberattacks by establishing a secure connection between users and the internet. Employers should create VPNs and require employees to utilize these networks whenever possible, especially during business travel.

- **Conduct physical security training for digital valuables.** Most travellers let their guards down once they arrive at their destinations, but that can be one of the times they're most susceptible to theft. Employers should encourage business travellers to never leave their devices unattended. Employees should also be instructed to utilize strong passwords or multifactor authentication capabilities (if possible) and lock devices in hotel safes upon leaving their rooms.
- **Encourage employees to pack minimal devices.** Leaving unnecessary technology at home can help reduce the chance of theft or data loss. As such, employers should only permit employees to bring devices that are essential to completing their job duties on the road or abroad.
- **Require regular software updates.** Cybercriminals typically look for security flaws in outdated software. Updates are sent out to patch any holes in the software and reduce the opportunity for cybercriminals to attack. Employees should be required to update software on all their devices regularly.
- **Establish response plans.** Employers should have specific response plans that outline steps to take when devices containing confidential information are compromised, lost or stolen on the road or abroad.

Conclusion

Business travellers often carry sensitive personal- and work-related data on various devices, leaving them vulnerable to cyberattacks. However, taking the proper precautions while travelling can help them keep their devices and data secure.

For more risk management guidance, contact us today.

LET US HELP YOU MANAGE YOUR RISK

Regina
Moose Jaw
+1 (888) 661-5959

www.hendersoninsurance.ca
www.navacord.com
HII@hendersoninsurance.ca