# Cyber-risks and Liabilities

**July/August 2022**

## Maintain Cyber-security When Employees Travel

Now that most COVID-19 restrictions have lifted, many employees are resuming business travel. While the return to normality is welcome, it may increase organisational cyber-security risks. Travelling employees often carry valuable data and may not always be careful about securing their devices, making them prime targets for cyber-criminals.

Research by safe.co.uk found that 29% of Britons have had their mobile phone stolen or go missing during a work trip. A further 7% have had laptops stolen. In the hands of cyber-criminals, these devices—if compromised—could result in a major security breach, with dire consequences for an organisation.

As such, it's vital that your employees take steps to maintain cyber-security when travelling. Consider these tips:

- **Establish wi-fi policies**. Wi-fi sharing can leave devices discoverable to the public, including malicious actors. Encourage employees to use a 4G mobile network when travelling. Otherwise, have clear policies in place outlining what is and isn't acceptable when using public wi-fi. For example, sensitive activities, such as banking, should never be conducted over public networks.
- **Encourage employees to be vigilant.** When using devices, staff members should be constantly vigilant. Remind employees to work with their back against a wall or barrier when using a laptop to prevent others from looking at their screen. Better still, consider installing a privacy screen filter.
- **Protect against worst-case scenarios**. Even the most vigilant employee can accidently lose a device or have it stolen, so backup measures are essential. Reduce the chances of data being compromised by setting up device authentication, including complex PIN and password combinations or face recognition. For an additional layer of protection, consider full disk encryption.
- **Utilise a virtual private network (VPN)**. VPNs are secure, encrypted network connections. Such networks can help reduce the risk of cyber-attacks by establishing a secure connection between users and the internet. Consider creating VPNs and requiring employees to utilise these during travel.
- **Establish response plans**. Ensure employees know what steps to take should a device be compromised. Prompt action is essential to lessen the chance of a cyber-breach.

For more information on cyber-security, contact us today.

## Ways to Protect Operations From Ransomware Attacks

Ransomware is now the most significant cyber-threat facing the UK, according to the National Cyber Security Centre. Unlike lone threat actors, ransomware groups often reinvest a portion of their profits into hiring and training talented cyber-criminals, making them more dangerous to organisations. Protect yourself from ransomware attacks with these three tips:

- **Keep all software up to date**. Cyber-criminals can exploit security vulnerabilities, so timely patching is one of the most efficient and cost-effective ways to minimise cyber-security risks. If possible, automate software security scanning and testing to proactively spot any security flaws.
- **Require multifactor authentication (MFA)**. Utilise MFA for as many services as possible, particularly access-critical systems. Further, require all accounts with logins to have strong, unique passwords.
- **Implement user training**. Train all staff on cyber-security best practices. Phishing attacks can install ransomware, so raise employee awareness about the risks of visiting suspicious websites, clicking on suspicious links or engaging with phishing emails.

Contact us today for more guidance on ransomware attacks.

# Risk of Enterprise Connected Devices

Enterprise connected devices (ECDs) are used in many UK businesses to interact with, hold or process data. They include technology like smartphones, office cameras and vehicle telematics devices. While ECDs may improve operational efficiency, their use can expose organisations to increased cyber-security risks. When compromised, ECDs could allow cyber-criminals to gain access to corporate networks for espionage purposes, disruption or financial gain.

One common ECD type is the Internet of Things (IoT), which describes physical objects with embedded software that connect and exchange data with other devices and systems over the internet. Examples include smart watches, smart TVs and virtual assistants like Alexa. IoT technology is becoming increasingly popular. In fact, database company Statista predicts there will be over 75 billion IoT devices worldwide by 2025. With so many such ECD devices available, they are attractive prospects for cyber-criminals. Not only are they easily accessible over the internet, cyber-security is often an afterthought.

ECDs can be attacked in one of three ways:

- **Communication channels—**Attacks can originate from the communication channels that connect ECD components with one another.
- **Applications and software—**Attacks can originate from vulnerabilities in ECD software or network services.
- **Devices—**Attacks can be made on the devices themselves due to vulnerabilities in their storage firmware or physical interfaces.

It's vital for organisations to implement measures to mitigate the risks from ECD use. Consider these tips:

- **Improve passwords.** Avoid using the default password supplied with a device. Instead, give each ECD its own secure password to make it harder for cyber-criminals to gain access.
- **Patch regularly.** Keep on top of software or firmware patches. Better still, only buy ECDs that have built-in patching capability.
- **Implement verification.** Only allow employees access to ECDs for legitimate business purposes. Additionally, put in place solid verification steps to check users before they're given access.

Although ECDs are common in many workplaces, it's wise to make sure you have a comprehensive cyber-security plan established before relying on them. Such devices can be used by cyber-criminals to compromise other systems on a network, so make sure you're adequately protected.

For more ECD-related guidance, contact us today.