Cyber-Risks and Liabilities

March/April 2021

Keeping Mobile Devices Cyber-secure

Cyber-security is a subject that many employers have become more aware of in recent years, but there will always be more to learn and additional adaptations to make. As technology continues to evolve, so do the methods by which a cyber-attack might take place. One key example of a potential cyber-security step that organisations may not have prioritised heavily enough is maintaining the security of mobile devices.

Just like the computers at employees' desks, mobile devices—such as smartphones and tablets—can be targeted by hackers. As remote working continues to become more common, this type of equipment is likely to be used more often, and therefore presents greater potential exposures.

Mobile Cyber-security Measures

Like any other cyber-security practice, the process of keeping mobile devices safe includes a number of key steps. In order to keep sensitive information and data secure, consider the steps:

1. **Selecting mobile devices**—One of the first steps to ensuring ample cyber-security is issuing employees proper equipment. When choosing devices, take time to assess which manufacturers meet your security needs and how different operating systems will synergise with programs used by workers. Given that technology is constantly evolving, it is also important to develop a strategy for updating devices when it becomes necessary.
2. **Configuring devices**—Before issuing devices to employees, it is important that they are set up correctly. Your organisation should ensure that phones, tablets and laptops have proper cyber-security measures installed, such as antivirus software. It may also be advisable to restrict how much control employees have over altering settings and installing additional programs.
3. **Maintaining security**—Once mobile devices have been distributed to employees, organisations must ensure that optimal cyber-security is maintained. Employers should establish clear and firm policies regarding acceptable uses of devices, and set up a system to monitor and log data in the event of a cyber-incident. Employees should also be instructed to promptly install any software updates on their devices as these patches are often intended to cover up a potential weakness that could be targeted by cyber-criminals.

The expanded use of mobile devices outside of an organisation's own premises can result in additional risks. With remote work expected to remain a trend, it is important for employers to understand cyber-security steps for devices issued to remote employees.

For more information, contact us today.

AP INSURANCE BROKERS

Minimising Physical Threats to Cyber-security

While it may be common to think of cyber-crime as only taking place through electronic means, it is important for employers to recognise that threats can attack from many different directions.

Many cyber-crimes are committed simply by a criminal gaining physical possession of an organisation's information, data or property. Even a single laptop falling into the wrong hands can result in catastrophic consequences. Minimise your organisation's risk by prioritising the following steps:

- **Restrict access**—In a place of business, it may be common for many different parties to come and go throughout the day. But, the wrong person gaining access to your premises can lead to stolen devices or a device with malicious software unknowingly being connected to your network. Require that all visitors and contractors check in at the entrance before allowing them any further access to the premises.
- **Train staff**—Employees must be properly educated on the threat of physical cyber-crimes. This training should include both on-site and off-site precautions. While at the workplace, instruct employees not to hold the door for or allow access to anyone who is not clearly authorised. If devices with access to organisational information are taken elsewhere, be sure that employees never leave them unattended.

The theft of a computer or an intrusion into the workplace is already a serious incident, but the potential damage can be exponentially exacerbated if the perpetrator is a cyber-criminal. Fortunately, proper precautions can significantly reduce the chance of falling victim to these crimes.

What To Do After a Malware Infection

While cyber-security will ideally prevent cyber-attacks against your organisation from succeeding, it is always important to have a plan in place for unfortunate circumstances. In the case of cyber-incidents, one common issue that demands contingency is a device becoming infected with malware.

In the event that an organisation does become a victim of malware, being ready to respond quickly and appropriately can limit the damage. In order to minimise the potential ramifications of a malware attack, consider the following steps:

1. Disconnect any infected devices from all network connections immediately.
2. In serious cases, consider shutting off Wi-Fi networks, disabling core network connections and even disconnecting the internet completely.
3. Reset employee credentials, such as passwords. Before doing this, be sure to verify that your organisation will not be locked out of its own systems.
4. Safely wipe any infected devices and reinstall their operating systems.
5. Prior to restoring data to a device, verify that both the device and your backup data are not infected. It is of the utmost importance that organisations are certain that both the backup and the device are safe prior to performing this step.
6. Connect devices to a safe network in order to download, install and update software.
7. Install, update and run antivirus software.
8. After reconnecting the device to your network, monitor traffic and utilise antivirus software to check for any remains of the initial malware infection.

There are many hazards and risks that employers must navigate on a daily basis. Unfortunately, even the most prudent precautions may not always be enough to prevent problems entirely. In the case of cyber-security, organisations must be prepared to understand how to react after an attack in order to prevent a moderate incident from becoming a large disaster.

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