Cyber-risks and Liabilities

November/December 2022

5 Cyber-security Risks for Businesses

In the digital world, cyber-crime has increased in both frequency and complexity. Modern cyber-criminals are adept at spotting even small lapses in cyber-security. In fact, 39% of UK businesses reported a cyber-security breach in 2021, according to the government's Cyber Security Breaches Survey. The key to preventing such attacks is to understand how they happen. As such, it's vital that you recognise potential cyber-exposures and implement strategies to prepare for them. Consider the following five cyber-security risks:

1. **Poor patch management**—Patch management is the process of acquiring and applying software updates to a variety of endpoints, including mobile devices, computers, servers and embedded devices. If new software updates are not swiftly installed, cyber-criminals may exploit weaknesses. Reduce your cyber-incident risk by readily fixing any software vulnerabilities and implementing a patch management programme.
2. **Phishing**—Phishing attacks exploit people, aiming to trick individuals into doing the wrong thing, such as clicking a suspicious link that downloads malware onto their device. According to government data, 83% of all cyber-breaches in 2021 stemmed from phishing attacks. To lessen the risk, implement email filtering and blocking mechanisms and conduct staff phishing awareness training.
3. **Weak passwords**—Thanks to automated password-cracking tools, cyber-criminals can rapidly guess passwords lacking in complexity. Ensure employees set strong passwords using the National Cyber Security Centre's (NCSC) three-random-word technique. Additionally, set up multifactor authentication (MFA), where employees must provide a second piece of information before logging in.
4. **Malware**—Malware comes in many forms. For instance, spyware monitors internet activity to steal information, and adware infects a user's computer through pop-up adverts. To combat all malware types, consider installing anti-malware software and remind employees never to download files from untrustworthy sources.
5. **Ransomware**—Cyber-criminals use ransomware to deny a user access to files until a ransom is paid. Address this growing tactic through holistic cyber-security measures. Furthermore, back up sensitive information on external servers regularly. This way, you can easily restore it should the worst happen.

For more cyber-security guidance, contact us today.

Protect Your Customers From Cyber-enabled Crime

The NCSC recently published guidance that could help you protect your customers and brand from a range of cyber-enabled crime, including fraud. The new guidance is aimed at organisations with an online presence, particularly those with online customer accounts.

The guidance takes two forms. Firstly, the NCSC's "Authentication methods: choosing the right type" advice outlines how to select an appropriate authentication method for customer accounts. Accounts authenticated by password alone can be vulnerable to cyber-attacks; however, by following the guidance, you can help ensure robust protection for customers.

Secondly, the NCSC's "Takedown: removing malicious content to protect your brand" advice outlines how to protect your brand from being exploited online (eg false product representations or fake endorsements). The guidance also explains how to remove malicious content, such as phishing sites.

Taken together, the NCSC's two guidance documents are designed to help you better protect your customers and users from cyber-crime. For more information, visit the NCSC's website.

How to Use Public Wi-Fi Safely

Public Wi-Fi allows individuals to access online accounts, catch up on work and check emails on the go. Unfortunately, while convenient, it isn't risk-free. Cyber-criminals can attempt to hack into a device through unsecured Wi-Fi networks or eavesdrop on Wi-Fi signals to access personal information and login credentials. They may also use an unsecured Wi-Fi network to spread malware to other devices on the network. Moreover, some public Wi-Fi networks can even be fake hot spots that lure in users by having a similar name to the legitimate hot spot.

To avoid these types of situations, follow these tips to use public Wi-Fi networks safely:

- **Turn Wi-Fi off when it's not being used.** Most devices that connect to Wi-Fi have a way to turn it off. When Wi-Fi isn't needed, toggle that feature off so the device won't search for it or connect to nearby networks.
- **Use a firewall**. When possible, install a firewall on devices. A firewall is a security barrier between two networks that control the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
- **Use a virtual private network (VPN).** When utilising public Wi-Fi often, it's a good idea to use a VPN; it directs all web activity through a secure, independent network that encrypts and protects a user's data. Most internet service providers offer a VPN as a secondary service.
- **Browse securely.** Never trust wireless encryption on a public Wi-Fi network. Instead, make sure websites scramble data by enabling secure socket layer encryption in the settings of the sites being visited. Additionally, make sure websites use HTTPS, which is more secure than regular HTTP sites.

For more cyber-security tips, contact us today.