Cyber-risks and Liabilities

January/February 2023

Cyber-security Trends for 2023

Cyber-security was once a consideration for IT teams only. However, the government's Cyber Security Breaches Survey 2022 found that 39% of UK businesses had experienced a cyber-security breach or cyber-attack in the past 12 months. With cyber-attacks increasing in frequency, organisations are now recognising the importance of a strong cyber-security culture across the workforce. One way to defend against cyber-attacks is to stay abreast of current trends; after all, cyber-security is a constantly evolving space.

The following are five cyber-trends to monitor in 2023:

1. **Internet of Things (IoT) vulnerabilities**—IoT devices such as smart devices and voice assistants continue to grow in popularity. In fact, management consultant company Gartner predicts that 43 billion IoT devices will be circulating globally in 2023. Unfortunately, such devices can be used as gateways for cyber-criminals to access and compromise networks. Furthermore, IoT device manufacturers don't always carry a security-first mindset. Although the government has enacted legislation to require smart device manufacturers to identify security weaknesses, it will remain vital to assess IoT vulnerabilities in 2023.
2. **The growth of artificial intelligence (AI)**—With an increasing number of vulnerabilities for cyber-criminals to target it's hard for organisations to predict where cyber-attacks will originate. AI tools can examine data in real time and recognise patterns indicative of cyber-threats. However, cyber-criminals are also utilising AI. For instance, AI algorithms can help hackers create a large number of personalised phishing emails. As such, it's important to keep up to date with the latest AI methods to stay one step ahead of hackers.
3. **Remote cyber-security**—Rapid implementation of remote working during the COVID-19 pandemic left many organisations exposed. Specifically, remote workers may have less secure internet connections, leave their devices unattended or be more easily fooled by spam messages. As a result, robust cyber-security policies for remote workers will be important in 2023.
4. **Organisational cyber-security culture**—Organisations should continue their mission to disseminate cyber-security information to employees in 2023. To ingrain a strong cyber-security culture, basic security skills—such as understanding two-factor authentication and strong password control—should be taught across the workforce.

For further cyber-trends and guidance, contact us today.

Buying and Selling Secondhand Devices

Employees sometimes access work-related systems from their personal electronic devices. While this can help get tasks done sooner, it can also leave an organisation vulnerable to stolen information or data breaches if that personal device is ever compromised, such as when it's resold. That's why it's crucial to ensure all data is thoroughly deleted prior to reselling a device. Share the following tips with employees to help avoid potential data compromises:

- Use the "factory reset" feature to erase all personal data from devices, including messages, contacts, photographs, browsing history, Wi-Fi codes, passwords and any installed apps. For assistance, check the manufacturer's guidelines for the specific device.
- Select "no" if given the option to keep personal files when erasing data unless the device is being kept.
- Check that secondhand devices are supported by the manufacturer and still benefit from regular security updates when buying such devices. Additionally, perform a "factory reset" to ensure that devices are ready for first use.

By sharing these few simple steps, employers like you can help employees keep both personal and company data secure when buying and reselling electronic devices.

For more data-security tips, contact us today.

Attack Surface Management Explained

Attack surfaces refer to the total possible entry points (also known as attack vectors) for unauthorised access into any system. The recent rise of remote and hybrid work combined with the shift to the cloud and widespread implementation of software-as-a-service (SaaS) applications have made attack surfaces increasingly prominent, complex and difficult to defend against cyber-attacks. Fortunately, attack surface management (ASM)—the continuous monitoring of potential attack vectors—can provide an organisation with an inventory of exposed assets to accelerate responses to cyber-threats.

ASM entails the following automated core processes:

- **Asset discovery**—This is a continuous process that scans for potential entry points for cyber-attacks. These assets may include subsidiary assets, third-party or vendor assets, unknown or non-inventoried assets, known assets, or malicious or rogue assets.
- **Classification and prioritisation**—Assets are analysed and prioritised by the likelihood that hackers could use them as a target. They're inventoried by their connections to other assets in the IT infrastructure, such as IP address, identity and ownership. Assets are also analysed for exposures such as missing patches, coding errors and potential attacks, including ransomware or malware. Each vulnerable asset is assigned a risk score or security rating.
- **Remediation**—Potential vulnerabilities are remediated in order of priority. It may be necessary to apply software or operating system patches, debug application codes or use stronger data encryption. Previously unknown assets may need new security standards, or it may be necessary to integrate subsidiary assets in organisations' cyber-security strategies.
- **Monitoring**—Security risks change whenever a new asset is deployed or existing assets are used in new ways. Networks and their inventoried assets are continuously monitored for vulnerabilities to allow ASM to find attack vectors in real time and give organisations a chance to neutralise threats.

ASM not only helps protect organisations from cyber-attacks, but it's also a practice frequently required by underwriters to obtain cyber-insurance—thus making it all the more vital.

Contact us today for additional risk management information and insurance solutions.