Common cyber risks and how to build resilience

1 Phishing attacks

Phishing remains one of the most prevalent and damaging cyber threats. Cybercriminals use deceptive emails and websites to trick employees into clicking on malicious links, and divulging sensitive information such as login credentials, financial details, or personal data. The impact can be severe, leading to data breaches, financial losses, ransomware and malware installation and compromised sensitive data.

Security top tip: Employee training and robust email filtering systems are critical to mitigating this threat.

2 Ransomware

Ransomware attacks have skyrocketed in recent years, targeting businesses of all sizes. In these attacks, malware encrypts a company's data, and the attackers demand a ransom for the decryption key which would allow the targeted company to re-access their systems. Data exfiltration is also increasing, with cyber criminals stealing the data and then demanding a ransom payment for its return. Companies with limited cybersecurity measures are particularly vulnerable. The costs associated with ransom payments, data recovery, and downtime can be devastating.

Security top tip: A robust, layered approach with ‘defence in depth' security is needed to ensure cybercriminals aren't able to access everything, once they are in. Regular data backups and comprehensive endpoint protection are also essential defences against ransomware. Of course avoiding an attack should be the aim so regular phishing assessments, port scans and vulnerability testing are key.

3 Insider threats

Insider threats, whether malicious or accidental, pose a significant risk. Employees, contractors, or business partners with access to sensitive information can inadvertently or intentionally cause data breaches. For businesses without extensive monitoring and access controls, detecting and preventing insider threats can be challenging.

Security top tip: Implementing strict access controls, continuous monitoring, and employee education can help mitigate this risk.

4 Malware and viruses

Malware and viruses can infiltrate business systems through various vectors, including email attachments, visiting malicious websites, and opening or downloading compromised software. These malicious programs can steal data, disrupt operations, and provide backdoor access to cybercriminals.

Security top tip: Ensure antivirus and anti-malware solutions are up-to-date and employ advanced threat detection techniques such as Monitoring, Detection & Response platforms (MDR).

5 Weak passwords and authentication

Weak or reused passwords are a common vulnerability that cybercriminals exploit to gain unauthorized access to systems and data. Some businesses struggle with implementing and enforcing strong password policies.

Security top tip: Utilizing multi-factor authentication (MFA) and educating employees about password security can significantly enhance protection against unauthorized access.

Common cyber risks and how to build resilience

6 Social engineering

Social engineering attacks manipulate individuals into performing actions or divulging confidential information. These attacks can take many forms, including deep fake voice notes and videos, pretexting, (Creating fake identity or scenario to trick a victim into giving confidential information or access to restricted systems) or baiting (fake free offers and downloads that contain malware or request personal details). Companies with less rigorous security awareness training are prime targets.

Security top tip: Regular training sessions and simulated social engineering attacks can help employees recognize and resist these tactics.

7 Outdated software and systems

Running outdated software and systems exposes businesses to known vulnerabilities that cybercriminals can exploit. Delayed updates and improvements due to budget constraints or operational disruptions are often leading causes for this risk.

Security top tip: Establishing a regular update and patch management schedule is crucial for maintaining a secure IT environment and avoiding issues with IT platforms as they approach end of life.

8 Data breaches and information theft

Data breaches can occur through various means, including hacking, insider threats, and physical theft. The consequences can include legal penalties, loss of customer trust, and significant financial losses.

Security top tip: Implementing encryption, access controls, and regular security audits can help protect sensitive data from unauthorized access and theft.

9 Misconfigured cloud resources

Moving to the cloud does not mean moving away from security duties: responsibility for security of cloud resources is most often shared between the customer and the provider. Using default settings, or not paying attention to configuration, can result in data storage or other resources being accessible to unauthorised users.

Security top tip: Check on the default requirements and ensure updates are carried out. Log and monitor activity, this makes it easier to detect compromises early, and to investigate what occurred. Make sure you read the agreements with your 3rd party providers and understand how their security, monitoring and liabilities are managed.