Cyber-risks and Liabilities

November/December 2023

Mitigating Ransomware Attacks

Ransomware is malicious software designed to prevent victims from accessing their computers. Typically, a ransomware infection locks computers entirely or encrypts data, and hackers demand payment to restore access. Ransomware attacks are growing in both frequency and severity. In fact, 1 in 54 organisations in Europe fell victim to a ransomware attack during the second quarter of 2023, according to research by software company Check Point. This represents a significant 21% year-on-year increase.

With ransomware becoming increasingly prevalent, your organisation must take rigorous steps to bolster its resilience. It may be wise to work on the assumption that some malicious software will infiltrate your defences and take steps to limit its impact. Consider the following risk mitigation strategies:

- **Keep up-to-date backups**. Back up all important files and regularly test your backup plans to ensure potential problems are spotted before they result in data loss. Additionally, create offline backups and keep these in an off-site location or a cloud service designed for this purpose. Always scan backups for malware before restoring files in case hackers have infiltrated your network and infected them.
- **Limit exposure**. Leverage strategies to reduce the likelihood of malicious content reaching your devices. Specifically, use email filtering to scan messages for red flags and utilise intercepting proxies—applications that sit between a web browser and web server—to analyse traffic or block access to internet services.
- **Protect devices**. Centrally manage organisational devices to ensure only permitted applications are used and consider configuring a host-based firewall that's directly installed on devices rather than networks. Additionally, install security updates as soon as they become available and use the latest operating system for devices.
- **Prepare for breaches**. Develop a robust cyber-incident response plan. Specifically, identify your critical assets and determine how these could be impacted by ransomware attacks. Detail how you plan to restore operations and respond to ransom demands. Remember, always keep a hard copy of your plan on a system unconnected to your main IT network for safe access in the event of breaches.

Contact us today for further cyber-security and risk mitigation strategies.

riskhub
the business resilience people

Help Employees Understand Social Media Safety

How employees manage their social media accounts could directly impact your organisation's security. Although posting confidential company information is one obvious way employees could cause harm, their entire digital footprint could be exploited for malicious gains. As such, it's wise to promote social media safety among workers. Consider sharing the following tips:

Use two-step verification (2FA). To make it more difficult for criminals to hack their social media accounts, employees could set up 2FA, a system that requires two distinct forms of identification (eg a password and a code sent to their smartphones).

Check privacy settings. Employees should regularly check their privacy settings to understand who sees the information they post and to scrutinise any posts they've been tagged in. Employees must carefully consider the contents of all posts and avoid including anything too personal, as such information can be used for identity theft or other crimes.

Keep passwords safe. Employees should use strong passwords, change them regularly and refrain from using the same password for everything.

Act with caution. Employees should trust their instincts and avoid accepting invites or clicking on suspicious links if something feels untoward.

Contact us for further cyber-security tips.

Cyber-hygiene Best Practices

Cyber-hygiene refers to habitual practices that ensure critical data and digital systems are handled safely and protected from cyber-attacks. Cyber-hygiene is increasingly vital for organisations of all types and sizes, not least because 32% of businesses and 24% of charities experienced a cyber-security breach or attack in the past 12 months, according to government data. Organisations that fail to leverage cyber-hygiene best practices could leave critical systems vulnerable, potentially resulting in financial losses, regulatory penalties and reputational damage. To protect your organisation, consider best practices for the following cyber-hygiene factors:

- **Passwords**—The use of strong passwords—containing at least 12 characters and a mix of upper- and lowercase letters plus symbols and numbers—that are changed regularly is an essential cyber-hygiene practice. Ensure users don't share passwords or repeatedly use them across different accounts.
- **Multifactor authentication**—Limit cyber-criminals' opportunity to steal data by making sure important accounts, including email, social media and banking apps, require multifactor authentication.
- **Data backups**—Back up essential files in a separate location, such as on an external hard drive or in the cloud.
- **Firewalls—**Utilise a network firewall to prevent unauthorised users from accessing company websites, emails and other sources of information accessed through the internet.
- **Security software**—Employ high-quality antivirus software to perform automatic device scans to detect and remove malicious software and provide protection from various online threats and security breaches.
- **Employee education**—Employees are one of your organisation's most significant cyber-security vulnerabilities. Arrange cyber-security training to teach employees to identify phishing attacks, social engineering and other cyber-threats.

Overall, daily routines, good behaviours and occasional checkups can make all the difference in ensuring your organisation's cyber health is in optimal condition.

For additional cyber-security resources, contact us today.