Cyber-security Fundamentals

Cyber-security breaches continue to be a problem for all types of organisations. According to a survey by the Department for Digital, Culture, Media & Sport, four in 10 businesses and a quarter of charities reported experiencing cyber-attacks in the past 12 months.

While organisations are always at risk from a cyber attack, there may be a heightened risk at certain times. Broader problems—such as hacktivism and geopolitical tensions—can increase the cyber-risk organisations face.

One such risk is the currently observed pattern of malicious Russian behaviour in cyber-space. Organisations are being urged to boost their defences against potential cyber-attacks linked to tensions between Russia and Ukraine. Regardless of risk, it's always wise to adhere closely to a cyber-strategy. Consider the following cyber-security fundamentals.

Check Your System Patching

System patching is essential to correct errors in software that could lead to vulnerabilities if not fixed. Make sure you patch the following:

- Users' desktops, laptops and mobile devices (If possible, turn on automatic updates.)
- Firmware on your organisation's devices •

Internet-facing services

Additionally, review any unpatched systems. Ideally, all key business systems should be patched. If this isn't practical, put mitigations for any remaining unpatched systems in place.

Check Your Defences

Bolster your defences by ensuring antivirus software is installed correctly and active on all systems.

Review all firewall rules regularly. These determine the network traffic allowed to enter and exit your network. Often temporary firewall rules are set up to enable a contractor or similar to perform a task for a particular timeframe. If such rules are left in place for longer than required, security risk increases.

Additionally, check the security defences of all other devices such as laptops and mobile phones. Consider the National Cyber Security Centre's device security guidance.

Four in 10 businesses have experienced cyber-attacks in the past 12 months.

Access Management

Access management is the process of identifying, tracking and managing users' access to any IT applications or systems. Increase your access management resilience through the following methods:

- **Bolster password security**—Ask staff to ensure passwords are unique to the organisation and not re-used at home. Educate users to create strong and unique passwords with a mixture of letters, numbers and characters.
- **Review accounts**—Carefully review any accounts with privileged or administrative access. The fewer people with access to sensitive information, the better, so manage the number of privileged

accounts and swiftly remove old or unused accounts.

- **Review multi-factor authentication (MFA)**—If you have MFA enabled, check it's properly configured.

Logging and Protective Monitoring

Logging is the practise of managing the log data produced by your applications and infrastructure. Determine what logging you have in place, where logs are stored and how long logs are retained.

Security monitoring is vital for the identification and detection of threats to your IT systems. Review your logs—especially antivirus logs—regularly to search for errors, anomalies or suspicious activity. Where possible, keep your logs for at least one month.

Review Backups

Check that your backups are working to ensure your data is safe and secure in the event of a cyber-attack:

- **Perform test restorations**—Test currently saved data by restoring a small number of files/folders to a machine to confirm that your backups are running as planned.
- **Consider a cold backup**—A backup taking place when the database is offline and not accessible to update is known as a cold backup. This method ensures the backup remains unaffected should any incident impact your live environment.
- **Extend your backup**—Don't just back up data. Ensure machine state and any critical external credentials (such as private keys and access tokens) are backed up too.

Check Your Internet Footprint

Check your external internet-facing footprint is up to date. This includes checking which IP addresses your system uses and which domain names belong to you. Check that your password is secure on any domain registration account.

Additionally, consider performing a vulnerability scan to check that everything you need to patch has been patched. Better still, make this a part of a wider organisational Vulnerability Management Plan.

Check Third-Party Access

If third-party organisations have access to your IT networks, make sure you thoroughly understand what level of privilege they have and take time to review any third-party security practices. Remove any third-party access that's no longer required.

Study Your Incident Response Plan

Check your incident response plan to ensure escalation routes and contact details are up to date. Make sure your policy states who has the authority to make critical decisions and covers the procedure for any out of-hours response. Additionally, consider how your incident response plan will be made available if your business systems are no longer functioning during an attack.

Educate Staff

Educate staff on the different types of cyber-attack. One such attack is phishing. According to Symantec, one in every 3,722 emails in the UK is a phishing attempt. Therefore, it's vital to ensure you have a process in place to deal with any reported phishing emails.

Further, ensure that your staff are made aware of any heightened cyber-risk. Getting buy-in from employees is crucial to help facilitate the adherence to the cyber security strategy. Also, make sure everyone knows how to report suspected security breaches quickly.

Conclusion

Cyber-security is a serious concern for all businesses. Contact us today to learn how our risk management resources and insurance solutions can help protect your organisation from cyber-attack.