CYBER SECURITY
ADVICE REPORT FOR SMES

LoughTec
IT • CYBER SECURITY

CONTENTS

BEGINNER LEVEL

For SMEs just starting their cyber security journey, the focus should be on establishing a strong foundation with simple yet effective measures.

Staff Cyber Security Awareness and Continuous Training

What It Is: Educate your employees about the basics of cyber security. This includes recognizing phishing emails, using strong passwords, and understanding the importance of regular software updates.

Why It Matters: Human error is one of the leading causes of security breaches. Cyber Security awareness training helps employees identify and avoid common threats and attacks.

Action: Organize continuous cyber security awareness training for your staff, it helps them to protect your business but also helps protect themselves in their personal lives, it's also very cost effective.

Antivirus and Firewall Protection

What It Is: Install antivirus software and enable firewalls on all devices connected to the company's network.

Why It Matters: These tools are your first line of defence against malicious software and unauthorized access.

Action: Ensure that all systems have up-to-date antivirus software and that firewalls are properly configured and regularly monitored.

Regular Data Backups

What It Is: Implement a routine for backing up critical or all business data.

Why It Matters: In the event of a cyber attack, having backups ensures that you can quickly recover lost or corrupted data.

Action: Use cloud-based services to automate backups, ideally have dual back up's and also critically, test the restoration process periodically.

INTERMEDIATE LEVEL

For SMEs with a basic cyber security foundation, it’s time to move towards more robust and proactive measures.

Multi-Factor Authentication (MFA)

What It Is: Implement MFA across all accounts, requiring users to verify their identity using two or more methods (e.g., password and a mobile app code or biometrics).

Why It Matters: MFA adds an extra layer of security, making it significantly harder for attackers to gain unauthorized access.

Action: Start with critical systems (email, financial software) and expand MFA to other platforms over time.

Regular Security Audits

What It Is: Conduct regular vulnerability audits to identify vulnerabilities in your systems and processes.

Why It Matters: Audits help uncover weaknesses that could be exploited by cyber criminals, allowing you to address them proactively

Action: Schedule quarterly security reviews with IT professionals.

Encryption of Sensitive Data

What It Is: Encrypt sensitive data both at rest and in transit to prevent unauthorized access.

Why It Matters: Encryption ensures that even if data is intercepted or accessed, it remains unreadable to unauthorized users.

Action: Start by encrypting critically important databases containing customer and staff information along with financial records.

ADVANCED LEVEL

For SMEs with a strong cybersecurity posture, focus on continuous improvement and advanced threat detection.

Advanced Threat Detection Systems

What It Is: Deploy advanced threat detection solutions like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Why It Matters: These systems monitor network traffic for suspicious activity and can prevent attacks in real-time, especially out of hours.

Action: Integrate IDS/IPS with your existing security framework and regularly update them to detect new threats.

Incident Response Planning

What It Is: Develop and regularly update an incident response plan that outlines the steps to take in the event of a cyber attack.

Why It Matters: A well-prepared response can minimize damage and downtime which heavily affect's cost and the overall financial impact of a potential cyber attack.

Action: Conduct regular recovery simulations (e.g. Disaster Recovery) to ensure your team is ready to act swiftly and effectively.

Threat Intelligence Sharing

What It Is: Participate in threat intelligence sharing communities to stay informed about the latest cyber threats and trends.

Why It Matters: Sharing intelligence helps SMEs stay ahead of emerging threats by learning from the experiences of others.

Action: Join industry-specific cybersecurity groups and contribute to discussions. Utilize threat intelligence platforms that aggregate data from multiple sources.

CYBER SECURITY

Cyber security is an ongoing process that evolves with your business and although above is a staggered halo of advice, all levels are recommended and there is also much more that can be done. Whether you're just starting out or have an established cyber security framework, there's always room to improve. By following these tailored recommendations, your business can better protect its assets, maintain customer trust and industry reputation whilst being able to thrive knowing you are in a secure digital environment. The key to effective cyber security is staying informed, being proactive and continuously refining and improving your approach as new challenges arise.

Check out our cyber attack impact calculator to see the potential financial impact a cyber attack could have on your business!

Reach out to LoughTec for your confidential, personalised and independent cyber security review!

For more information:

www.loughtec.com