Cybersecurity Risk Assessment Framework for Small Organisations

By following this basic risk assessment framework, small (and micro) organisations in the UK can enhance their cybersecurity posture and better protect themselves against cyber threats.

This framework is composed of two parts, **Primary** and **Enhanced**, to provide the greatest resilience.

THE PRIMARY FRAMEWORK

1. Identification of Assets:

- Identify all digital assets including hardware, software, data, and networks.
- Determine the criticality of each asset to business operations.

2. Threat Identification:

- Research and understand common cyber threats targeting micro and small organisations.
- Consider threats such as phishing attacks, ransomware, malware, and insider threats.

3. Vulnerability Assessment:

- Assess the vulnerabilities present in the organisation's systems and networks.
- Identify weaknesses in software, configurations, and access controls.

4. Risk Analysis:

- Analyse the likelihood of cyber threats exploiting identified vulnerabilities.
- Evaluate the potential impact of each threat on business operations, finances, and reputation.

5. Risk Prioritization:

- Prioritize identified risks based on their likelihood and potential impact.
- Focus on addressing risks with the highest likelihood and impact first.

6. Control Implementation:

- Implement appropriate cybersecurity controls to mitigate identified risks.
- Examples include firewalls, antivirus software, encryption, regular software updates, and employee training.

7. Monitoring and Detection:

- Establish systems for monitoring network traffic, system logs, and user activity.
- Implement intrusion detection systems and security incident response procedures.

AJN SOLUTIONS GROUP

Risk Management Solutions
Corporate Governance Solutions

www.antonyjnewman.com

tony@antonyjnewman.com

8. Response and Recovery Planning:

- Develop a cybersecurity incident response plan outlining procedures to follow in case of a security breach.
- Define roles and responsibilities for responding to incidents and recovering from cyberattacks.

9. Regular Review and Update:

- Regularly review and update the cybersecurity risk assessment to reflect changes in the organisation's technology, operations, and threat landscape.
- Adapt cybersecurity controls and strategies as needed to address emerging threats and vulnerabilities.

10. Compliance and Regulations:

- Ensure compliance with relevant cybersecurity regulations and standards, such as the UK's Cyber Essentials scheme or the General Data Protection Regulation (GDPR).
- Stay informed about regulatory requirements and update cybersecurity practices accordingly.

11. Staff Awareness and Training:

- Provide cybersecurity awareness training to all employees to educate them about common cyber threats and best practices for protecting sensitive information.
- Encourage a culture of cybersecurity awareness and vigilance throughout the organisation.

12. External Support:

- Consider seeking external support from cybersecurity experts or Managed Security Service Providers (MSSPs) to augment the organisation's cybersecurity capabilities, especially for smaller organisations with limited resources.

By incorporating the following 8 additional elements into their cybersecurity risk management approach, micro and small organisations in the UK can further strengthen their defences against cyber threats and mitigate the potential impact of security breaches on their operations and stakeholders.

www.antonyjnewman.com
tony@antonyjnewman.com

THE ENHANCED FRAMEWORK

13. Data Protection and Privacy:

- Ensure that appropriate measures are in place to protect sensitive data, including customer information, employee records, and financial data.
- Implement encryption, access controls, and data loss prevention mechanisms to safeguard against unauthorised access and data breaches.

14. Secure Remote Work Practices:

- With the increasing trend of remote work, establish secure remote access policies and procedures.
- Implement secure VPN connections, multi-factor authentication (MFA), and endpoint security solutions to protect devices used for remote work.

15. Third-Party Risk Management:

- Assess the cybersecurity posture of third-party vendors and service providers that have access to the organisation's systems or data.
- Ensure that contracts with third parties include provisions for cybersecurity requirements and responsibilities.

16. Business Continuity and Disaster Recovery:

- Develop and maintain a business continuity plan that outlines procedures for maintaining essential business functions during and after a cybersecurity incident.
- Implement backup and recovery processes to ensure timely restoration of data and systems in the event of a cyberattack or data loss.

17. Incident Reporting and Collaboration:

- Establish clear procedures for reporting cybersecurity incidents internally and externally, including to regulatory authorities and law enforcement agencies if required.
- Foster collaboration with industry peers, government agencies, and cybersecurity organisations to share threat intelligence and best practices for cyber defence.

18. Regular Security Audits and Assessments:

- Conduct regular security audits and assessments to identify gaps in cybersecurity controls and practices.
- Engage independent third-party auditors or cybersecurity professionals to perform comprehensive assessments and provide recommendations for improvement.

19. Budget Allocation for Cybersecurity:

- Allocate sufficient budget and resources for cybersecurity initiatives, considering the potential impact of cyber threats on the organisation's operations and reputation.
- Ensure that cybersecurity investments are aligned with business objectives and risk tolerance levels.

20. Executive Leadership and Board Oversight:

- Ensure that cybersecurity receives adequate attention and oversight from executive leadership and the board of directors.
- Establish clear lines of communication for reporting cybersecurity risks and incidents to senior management and the board.

www.antonyjnewman.com
tony@antonyjnewman.com