Ransomware Attacks
Basic Checklist

1. **Employee Training and Awareness:**

- Conduct regular training sessions to educate employees about the risks of ransomware and how to identify phishing emails, suspicious links, and attachments.
- Emphasise the importance of not clicking on unknown links or downloading attachments from unfamiliar sources.

2. **Implement Security Best Practices:**

- Ensure all systems and software are up-to-date with the latest security patches and updates.
- Install reputable antivirus and anti-malware software on all devices and keep them updated.
- Enable firewalls on network devices to monitor and control incoming and outgoing traffic.

3. **Data Backup and Recovery:**

- Regularly backup all critical data and ensure backups are stored securely offline or in a separate network location not accessible from the primary network.
- Test backups regularly to verify their integrity and ensure they can be successfully restored in case of a ransomware attack.

4. **Access Control and Least Privilege:**

- Limit user access to only the systems and data necessary for their job roles (principle of least privilege).
- Implement strong password policies, including regular password changes and the use of multi-factor authentication (MFA) where possible.

5. **Email Security Measures:**

- Deploy email filtering solutions to block known malicious attachments and links.
- Enable email authentication protocols such as SPF, DKIM, and DMARC to prevent email spoofing and domain impersonation.

6. **Network Segmentation:**

- Segment your network into separate zones to contain the spread of ransomware in case of an infection.
- Restrict network access based on user roles and responsibilities, and limit lateral movement within the network.

7. **Incident Response Plan:**

- Develop a comprehensive incident response plan outlining procedures to follow in the event of a ransomware attack.

AJN SOLUTIONS GROUP

Risk Management Solutions
Corporate Governance Solutions

www.antonyjnewman.com

tony@antonyjnewman.com

Ransomware Attacks
Basic Checklist

- Define roles and responsibilities for responding to and mitigating the impact of an attack, including communication protocols with stakeholders and law enforcement if necessary.

8. Regular Security Audits and Assessments:

- Conduct regular cybersecurity assessments and penetration testing to identify vulnerabilities in your systems and network.
- Address any identified weaknesses promptly to reduce the risk of exploitation by ransomware attackers.

9. Vendor and Third-Party Risk Management:

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

10. Stay Informed and Engage with the Community:

- Stay updated on the latest ransomware threats and trends through industry news, alerts, and information sharing platforms.
- Participate in cybersecurity forums and communities to learn from peers and share best practices for ransomware prevention and response.

By following this checklist, micro and small businesses can significantly reduce their risk of falling victim to ransomware attacks and mitigate the potential impact on their operations and data.

AJN SOLUTIONS GROUP

Risk Management Solutions
Corporate Governance Solutions

www.antonyjnewman.com

tony@antonyjnewman.com