Cyber 365

The Cyber Resilience Checklist: 20 Essential Steps to Prepare for Cyber Threats

In an era where digital threats are ever-evolving, a proactive approach to cybersecurity is vital for any organisation. Developed in partnership with insights from Cyber 365, this comprehensive Cyber Resilience Checklist serves as a practical guide to strengthen your organisation's cyber defences. Covering essential steps from policy creation to incident response, this checklist empowers your team to secure valuable assets, protect sensitive data, and stay prepared for cyber incidents.

The Cyber Resilience Checklist

- [ ] **1. Develop a Cybersecurity Policy**
  - Draft clear cybersecurity policies that outline acceptable use, incident reporting, and compliance. Make sure all employees understand and follow these guidelines.
- [ ] **2. Identify Critical Assets**
  - Identify your organisation's most valuable data and systems, then implement enhanced protection for these high-priority assets.
- [ ] **3. Establish a Dedicated Incident Response Team (CSIRT)**
  - Form a trained Cyber Security Incident Response Team to respond quickly and effectively to any security incident. Define roles clearly within the team.
- [ ] **4. Conduct Regular Vulnerability Assessments**
  - Schedule vulnerability scans and penetration tests to uncover weaknesses in your systems before they're exploited.
- [ ] **5. Implement Multi-Factor Authentication (MFA)**
  - Secure sensitive systems by enabling MFA, requiring users to verify their identity beyond just a password.
- [ ] **6. Enforce Strong Password Policies**
  - Create complex, frequently updated passwords. Avoid passwords that are easy to guess or related to personal details.
- [ ] **7. Regularly Update Software and Systems**
  - Keep software, operating systems, and security tools up-to-date to close off security gaps in legacy systems.
- [ ] **8. Develop a Cybersecurity Training Program**
  - Train all employees in cybersecurity fundamentals. Prioritise topics like phishing detection and safe browsing practices.
- [ ] **9. Enable Logging and Monitoring**
  - Log activities on critical systems and set up alerts for suspicious behaviour. Regularly review logs to detect potential threats early.
- [ ] **10. Secure Network Perimeters**
  - Use firewalls and intrusion detection systems to secure network boundaries. Ensure configurations are current and robust.

The Cyber Resilience Checklist

- [ ] **11. Implement Data Encryption**
  - Encrypt all sensitive data both at rest and in transit to protect against data theft and leaks.
- [ ] **12. Create a Data Backup and Recovery Plan**
  - Regularly back up critical data, and test your recovery plan frequently to minimise data loss in case of a breach.
- [ ] **13. Conduct Tabletop Exercises for Incident Response**
  - Simulate cyber incidents to train your response team, identify weak spots, and optimise your incident response plan.
- [ ] **14. Regularly Review Access Controls**
  - Restrict access to essential personnel only. Review and adjust permissions periodically to maintain data security.
- [ ] **15. Establish Secure Remote Access Protocols**
  - Use secure remote access tools, such as VPNs, with MFA to prevent unauthorised access to the network.
- [ ] **16. Secure Mobile Devices and BYOD Policies**
  - Implement policies for mobile device security, including MFA on all devices that access company data. Educate employees on securing personal devices.
- [ ] **17. Develop a Communications Plan for Cyber Incidents**
  - Establish a plan that outlines communication protocols with stakeholders, clients, and regulatory bodies in the event of a cyber incident.
- [ ] **18. Use Network Segmentation**
  - Segment your network to restrict lateral movement in case of a breach. Isolate departments or functions as needed.
- [ ] **19. Establish a Disaster Recovery Plan (DRP)**
  - Develop a comprehensive plan for quickly restoring operations after a cyber incident, minimising downtime.
- [ ] **20. Align Cyber Resilience with Business Objectives**
  - Integrate cybersecurity initiatives with broader business goals, ensuring support from leadership and alignment with organisational objectives.

How to Use This Checklist

1. **Self-Assessment:** Start by assessing your current cyber resilience levels for each item on the list.
2. **Create an Action Plan:** Identify areas needing attention, assign priority, and set a timeline for implementation.
3. **Ongoing Updates:** Use this checklist at regular intervals to ensure your security measures evolve with emerging threats.