greenhat

Cyberattack Readiness Checklist

Follow us on LinkedIn to receive more powerful IT checklists for your business.

CHECKLIST

Cyberattack Readiness Checklist

Cadence ____________________

Last Review ____________________

Date ____________________

By ____________________

This comprehensive checklist is designed to guide you through essential steps for preparing, detecting, containing, and recovering from a cyberattack. It focuses on minimising impact through proactive data protection, controlled access, rapid response protocols, and efficient restoration processes, ensuring your business can maintain resilience and recover quickly.

Preparation & Prevention

□ Identify & Secure Critical Assets

- □ Classify key assets and data by order of importance, focusing on those essential for business continuity.
- □ Set up impact-reduction priorities directed towards protecting the most critical assets.

□ Develop & Update Incident Response Protocols

- □ Create quick-response procedures for faster containment.
- □ Define escalation paths for timely and effective response.

□ Strengthen Access Controls & Implement Network Segmentation

- □ Apply role-based access control (RBAC) to restrict sensitive data access based on roles.
- □ Segment the network to limit the spread of a potential attack.
- □ Use adaptive security controls such as multi-factor authentication (MFA) and geo-restrictions.

□ Implement Data Backup & Redundancy Measures

- □ Enable automated, encrypted backups to store critical data securely offsite.
- □ Establish system redundancy and auto-failover to ensure continuous operation.

□ Conduct Employee Cybersecurity Awareness

- □ Educate employees on detecting phishing, social engineering, and suspicious links.

□ Prepare Communication & Response Teams

- □ Identify team members responsible for incident coordination, technical response, and communication.
- □ Develop a communication strategy to reduce delays in stakeholder communication during an attack.

□ Install & Update Antivirus & Anti-Malware Software

- □ Install antivirus and anti-malware solutions across all devices keeping them up to date.
- □ Set antivirus software to update automatically, ensuring the latest threat definitions and protections are always in place.

Identification & Rapid Containment

□ Enable Real-Time Threat Detection

- □ Deploy intrusion detection and prevention systems (IDS/IPS) that detect abnormal activities early.
- □ Set up impact-based alerts to prioritise critical threats.

CHECKLIST

Cyberattack Readiness Checklist

- □ Run Vulnerability Scans & Penetration Testing
  - □ Conduct regular vulnerability scans to identify and address system weaknesses.
  - □ Schedule penetration testing and simulate real attacks to uncover and patch any entry points.

Impact Assessment

- □ Analyse the Extent of the Compromise
  - □ Identify compromised data and systems to understand the scope of the attack.
  - □ Evaluate the attack type (e.g., ransomware, malware) to plan the best course of action.
- □ Prioritise Impacted Assets & Operations
  - □ Focus on high-priority systems to reduce immediate impact.
  - □ Document evidence for analysis by capturing logs, system screenshots etc.
- □ Activate Communication Plan
  - □ Notify internal teams about the incident and steps for immediate containment.
  - □ Inform external stakeholders (if needed).

Restoration & Review

- □ Restore Systems from Secure Backups
  - □ Run malware scans to ensure data backups are clean before reinstallation.
  - □ Restore essential systems first, focusing on critical operations to reduce business disruption.
- □ Monitor for Residual Threats
  - □ Monitor network activity post-restoration, checking for signs of recurring issues.
  - □ Address any system vulnerabilities identified during the incident to prevent future incidents.
- □ Conduct a Post-Incident Review
  - □ Analyse the incident, reviewing which response methods were effective and identifying areas needing improvement.
  - □ Update cybersecurity and incident response plans.
- □ Implement Long-Term Security Enhancements
  - □ Run simulations of cyberattacks targeting critical assets to refine containment and response protocols.
  - □ Regularly update cybersecurity tools and training to stay prepared against new and evolving threats.