cdt360
by Curran Data Technologies

Cyber Resilience Essential Checklist

Use this checklist to ensure you're accounting for privacy concerns, compliance issues, and the policies and procedures critical to maintaining a secure organization and a culture of cybersecurity.

Achieve cyber resilience success with cdt360 by Curran Data Technologies

"Cyber resilience is the concept to help organizations as it looks at a wider scope where it comprises cybersecurity and business resilience. Cyber resilience can be defined as the organizations ability to withstand and/or quickly recover from cyber events that disrupt usual business operations."

Cyber Resilience

Privacy Program:

- **1. Internal Privacy Policy -** Your internal privacy policy should include employee records, email and internal usage, client/customer usage, internal systems and access, mobile devices, laws and regulations, and consequences for violating the policy. Prepare for the need to have a public-facing privacy policy, if you do not already have one.
- **2. Employee training on the privacy policy -** After creating privacy policies, you need to train your staff to ensure they understand the content.
- **3. Internal policy for data retention -** Creating a policy for data retention controls how long your company will retain data. This policy reduces the impact of a data breach and cuts data storage costs.

Security Program:

- **4. Security awareness training of employees and contractors -** Use online security training that is tailored to the needs of the organization. Such courses provide employees and contractors with a basic understanding of the potential physical and cybersecurity threats and how to respond.
- **5. Phishing awareness training -** It is recommended to use a service to randomly test users on their ability to identify phishing emails monthly to determine where additional training is needed.

- **6. Clean desk policy -** The adoption of a clean desk policy is designed to allow for the protection of any information and data that may be found at a user's workstation. With the removal or secure storage of sensitive information when employees or workforce personnel are away from their desks, the organization can ensure that data confidentiality, integrity, and availability may be guaranteed.
- **7. Visitor program -** Having a clearly understood visitor policy and escort program is vital to the security of employees, workforce personnel, clients, physical assets, and important data. The type of visitor policy needed fully depends on your office and workspace's type, size, and location.
- **8. Identify digital assets -** Conduct at a minimum an annual risk assessment that includes a complete digital asset inventory, known vulnerability report, and an assessment of risk and impact to the business.;
- **9. Multi-Factor Authentication (MFA) -** MFA is a preventative method that employs answers to a combination of prompts that involve something you know, something you have, and something you are to authenticate access into a system. These prompts can range from "where did you go to high school" to biometric methods like fingerprints and can combine passwords with technology by using text messages or emails as an additional authentication step. At least two of the three must be used to achieve MFA.

Tools:

- **10. Virtual Private Network (VPN) -** A VPN is an encryption-based communication method that connects a remote office or worker to an organization's private network over a shared or public network. The encryption effectively makes a tunnel within the public network that data can pass through without being read by eavesdroppers.

- **11. Secure Wi-Fi / wireless networking -** Securing Wi-Fi in use at the organization is one vital component that protects data and ensure the security of critical business systems. Ensure these three items are addressed:
  - - Change the default admin password on the Wi-Fi router.
  - - Update the Wi-Fi router firmware
  - - Create a guest Wi-Fi network
- **12. Secure Email Gateway (SEG) -** Email is the primary target hackers use to gain access to private company data. Email is often the least secure means of passing data into and within an organization. Modern methods of attacking email systems have grown in sophistication and the targeting of individuals.
- **13. System auditing -** On the firewall solution, ensure that logging is enabled and that the logs are periodically reviewed by assigned staff to identify potential patterns that may indicate a compromise or ongoing attack. many vendors provide or include a built-in reporting utility for the detailed analysis of information related to the network traffic with their firewall solutions.
- **14. Configure backup solution -** One of the most known and least implemented security controls is data recovery, or specifically data backups. An organization may have many processes and utilities for backing up critical information. Implement a 3-2-1 backup solution.
- **15. Test backup solution -** Regularly test backup restoration procedures. This process involves regularly testing backup media for reliability and testing the recovery procedure to ensure that the process has been verified during a disaster and can be replicated quickly and with minimal errors.
- **16. Domain Name Systems (DNS) and content filtering -** Use the Domain Name System (DNS) layer to filter content based on IP addresses to control web use and reduce infections by blocking sites known to pose a high risk of containing malware. While most firewalls have this included, once the user leaves the office (remote workforce) they need an agent installed on their laptop or wireless device.

- **17. Endpoint Detection and Response (EDR) -** Endpoint Detection and Response (EDR) is a cybersecurity technology that addresses the need for continuous monitoring and response to advanced threats. It is a subset of endpoint security technology and a critical piece of an optimal security posture. Attackers do not work 8 am to 5 pm, so you need 24x365 for effective detection and response.
- **18. Security Incident and Event Management -**Typically include the collection of security-related logs across network devices, the ability to correlate activity across multiple devices, and aids the ability for security analysts to search for and identify potential malicious activity.

System Hardening:

- **19. Clean up all unused programs on all systems -** Every program installed on a host endpoint or server operating system is another avenue of potential entrance for a hacker. Removing unnecessary or unneeded programs helps to limit the number of ways into a system. Close unused ports.
- **20. Use group policies and active directory -** It is recommended to clearly define what groups can access and maintain Microsoft Active Directory groups and rules. Occasionally, issues may arise due to simple user error that can open the gateway for a successful cyber-attack.
- **21. Secure Endpoint configurations -** This includes reducing the attack surface, strengthening user account controls, enforcing device firewalls, and implementing secure policies while maintaining reasonable user efficiency.
- **22. Implement perimeter security -** Properly configure and implement firewalls, routers, VPNs, and Intrusion Detection and Prevention systems (IDS/IPS).

- **23. Patch management plan -** A regular part of the security routine should involve the planning, testing, implementing, and auditing patches through an automated patch management software.
- **24. Monitor and track behavior in cloud apps -** Detect abnormal user behavior like impossible travel, unfamiliar sign-in properties, or suspicious inbox manipulation rules within cloud-based apps like Microsoft 265 and Azure AD to prevent attacks like business email compromise and ransomware.

Vulnerability Management and Assessment:

- **25. Define a vulnerability analysis and resolution strategy -** Vulnerability management is a crucial component in understanding your organization's overall risk. Organizations need to understand how vulnerabilities impact the overall weaknesses within your environment.
- **26. vulnerability management program -** At the core of any vulnerability management program lies the fundamental process of software management. Most vulnerabilities are software "bugs" that can be exploited and possibly compromise confidentiality, information, or availability. As such, an organization should take the time to understand all the software used within their environment.

Response:

- **27. Incident response policy -** Policies set the standard of behavior for activities; such examples include:
- - Statement of Management Commitment
- - Purpose and Objectives of the Policy
- - Scope of the Policy
- - Organizational Structure and Definition of Roles, Responsibilities, and Levels of Authority
- - Severity Ratings of Incidents
- - Performance Measures
- - Reporting and Contact Forms
- **28. Incident response procedures -** Procedures are the specific step-by-step instructions to execute individual processes as part of a plan specific to incident response, which is not the same as business continuity or disaster recovery.
- **29. Incident response roles and responsibilities -** Know the key stakeholders and critical roles within the organization who should care and be involved in a security incident. The responsible stakeholders and roles may change depending on the type of incident and the targeted resources of the organization .

CURRAN DATA TECHNOLOGIES

If you have questions or feel overwhelm - Call us for an easy simple conversation.
800-628-9085 - robert@currandata.com - currandata.com