

ARE YOU CYBER READY?

Use this checklist to evaluate your organization's current cybersecurity posture. Each item represents a critical component of a robust, multi-layered security strategy.



ACCESS CONTROL & AUTHENTICATION

- ☐ Implement Multi-Factor Authentication (MFA) for all critical systems)
- ☐ Enforce strong password policies, including complexity requirements and regular updates.
- ☐ Restrict user access based on roles and responsibilities (least privilege principle).

EMAIL & WEB PROTECTION

- ☐ Implement email filtering to detect and block phishing attempts.
- ☐ Use web content filtering to prevent access to malicious websites.
- ☐ Educate employees on recognizing and reporting suspicious emails and links.

ENDPOINT & NETWORK SECURITY

- ☐ Deploy antivirus and anti-malware solutions across all devices.
- ☐ Utilize firewalls to monitor and control incoming and outgoing network traffic.
- ☐ Regularly update and patch operating systems and software to address vulnerabilities.

SECURITY AWARENESS & TRAINING

- ☐ Conduct regular cybersecurity training sessions for all staff members.
- ☐ Simulate phishing attacks to test and reinforce employee awareness.
- ☐ Establish clear policies on acceptable use of company resources and data handling.

DATA BACKUP & RECOVERY

- ☐ Maintain regular, automated backups of critical data and systems.
- ☐ Store backups in secure, off-site or cloud-based locations.
- ☐ Test backup restoration processes periodically to ensure data integrity.

INCIDENT RESPONSE PLANNING

- ☐ Develop a formal incident response plan outlining roles, responsibilities, and procedures.
- ☐ Establish communication protocols for internal and external stakeholders during incidents.
- ☐ Review and update the incident response plan regularly to reflect emerging threats.

MONITORING & DESIGN

- ☐ Implement continuous monitoring tools to detect unusual activities and potential breaches.
- ☐ Set up alerts for unauthorized access attempts and other security incidents.
- ☐ Regularly review logs and reports to identify and address anomalies.

COMPLIANCE & RISK MANAGEMENT

- ☐ Identify and understand applicable regulatory requirements (e.g., HIPAA, PCI DSS, GDPR).
- ☐ Conduct regular risk assessments to evaluate potential threats and vulnerabilities.
- ☐ Document and implement policies to ensure compliance and mitigate identified risks.

SCORING YOUR CYBER READINESS:

0–10 items checked:

High Risk – Immediate action required to address critical vulnerabilities.

11–20 items checked:

Moderate Risk – Some measures in place, but significant improvements needed.

21–24 items checked:

Low Risk – Strong cybersecurity posture; continue to monitor and update practices

NEED HELP?

If you're unsure about any of these items or need help enhancing your cybersecurity measures, MapleTronics is here to support you. Our GuardE.N. solution offers comprehensive protection tailored to your business needs.