10-point Cyber Checklist

Guardian Technology Group

Purpose: Use this list to verify your business is protected against the most common cyber threats today. Work through it with your IT provider or leadership team.

1. Backups You Can Restore

- Daily backup of all critical files.
- Monthly backup stored offline or offsite.
- Restore tested at least quarterly.
- **Ask:** *Can we prove we can restore our data today?*

2. Multi-Factor Authentication (MFA)

- MFA enabled for email, payroll, banking, and any system containing sensitive data.
- Phone-based codes or authentication apps preferred over email verification.
- **Ask:** *Do all critical accounts require a second step to log in?*

3. Endpoint Protection

- Use a modern, monitored antivirus/endpoint detection system—no expired trials.
- Includes ransomware, credential theft, and malware protection.
- **Ask:** *Is someone actively monitoring alerts, or is this "set it and forget it"?*

4. Patch and Update Everything

- Operating systems, software, and devices updated on a fixed monthly schedule.
- Printers, firewalls, routers, and cloud apps included in the update process.
- **Ask:** *When was the last time every device was patched?*

5. Staff Cybersecurity Training

- Quarterly training sessions to identify phishing, BEC scams, and AI/deepfake threats.

- Reporting procedure for suspicious emails and calls.
- **Ask:** *Would every employee know what to do if they received a suspicious request from "me"?*

6. Access Control

- Limit access to only what each role requires.
- Remove access immediately when an employee leaves.
- Admin rights granted only with documented approval.
- **Ask:** *Who has unnecessary access right now?*

7. Incident Response Plan

- Written, tested plan for handling ransomware, phishing, and data breaches.
- Roles assigned for technical response, communication, and decision-making.
- **Ask:** *If we were hit today, who would take charge and what's the first step?*

8. Secure Remote Access

- Remote work secured with MFA, VPN, and business-owned or secured devices.
- Vendor and contractor access monitored and restricted.
- **Ask:** *Can an attacker use a home PC to breach our network?*

9. AI and Deepfake Voice Verification

- Require voice, dual or email verification for financial or sensitive requests.
- Train staff to verify even if the voice sounds like an executive.
- **Ask:** *Do we have a "no exceptions" verification policy?*

10. Cyber Insurance Readiness

- Policy reviewed and confirmed to cover ransomware, BEC, and social engineering attacks.
- Incident response and forensic coverage included.
- **Ask:** *Do we meet all security requirements in our Cyber insurance policy?*

Pro Tip:
Work on one checklist item per week. In 10 weeks, your business will be significantly harder to hack.