VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

Is Your Business at Risk?

A Cybersecurity Checklist for the Office Technology You Use

If your business falls short for even one of the following security issues, the probability of a cyber-attack is high. But if you adhere to the following security measures, you significantly reduce risk, improve resilience, and demonstrate the responsible stewardship of customer and company data.

☑ Do you update software regularly?

Cyber criminals often attack vulnerabilities in unpatched software and other office technologies. For business apps and operating systems as well as copiers, multifunction printers (MFPs), servers, network devices, firewalls, routers, etc., enable automatic patching wherever possible. Also maintain a regular patch management schedule.

☑ Are your endpoints protected?

Beyond standard antivirus tools, implement endpoint detection and response (EDR) to detect threats, with alerts monitored by a Security Operations Center (SOC) for rapid response. For more comprehensive protection, extended detection and response (XDR) and managed detection and response (MDR, via a managed security services provider) build on EDR to unify threat detection across multiple security layers.

☑ Are your network(s) and devices safe?

For users, enforce strong, unique passwords and move toward password managers and passphrases instead of just 90-day changes. Also require multi-factor authentication (MFA) for email, cloud apps, virtual private network (VPNs), and administrative access. On the IT side, deploy next-generation firewalls, secure Wi-Fi, and endpoint protection on all devices; encrypt hard drives and removable media by default; and monitor networks and endpoints continuously for suspicious activity.

☑ If you support remote work and VPN...

Treat access to any VPN as an extension of your internal network. Require device security checks (patched OS, disk encryption, EDR) before allowing VPN connections. Where possible, adopt Zero Trust or secure access service edge (SASE) models that verify users and devices continuously rather than relying solely on VPNs.

☑ Do you know where your data lives?

If your business stores data across cloud apps, laptops, mobile devices, and file shares, maintain a clear inventory of where data resides and who can access it. Use business-grade SaaS platforms with centralized admin controls, data loss prevention (DLP), and audit logging. Additionally eliminate “shadow IT” by standardizing approved tools.

☑ Is all data backed up securely?

When business data is critical, follow the 3-2-1 backup rule: three copies of data, on two different media, with one copy offsite and offline or immutable. Use frequent, automated, incremental backups and regularly test restoration to ensure that backups actually work.

☑ Do you plan for uptime and resilience?

If downtime could easily impact revenue or customer trust, leverage data protection and disaster recovery solutions that support the rapid recovery of systems and applications. Document and test a business continuity and incident response plan at least annually. A managed security services provider is an excellent resource for each of these measures.

☑ How often do you train employees?

For all employees who use email and the internet, provide cybersecurity awareness training at least twice per year, if not more. Training should cover phishing, social engineering, safe remote work, device security, and data handling. Reinforce expectations, run simulated phishing tests, and hold employees accountable in following security policies.

Ready to get started? We can help.

Contact us today for a free consultation. Call (800) 828-4801 or visit us at www.visualedgeit.com/contact