



South Florida Business Cybersecurity Readiness Checklist

A practical checklist for business owners and managers to spot common security gaps before they become downtime, ransomware, or compliance problems.

Use this as a quick readiness review. Check each item that is already in place, then use the scorecard to decide what needs attention next.

What This Checklist Covers

- Microsoft 365 and login security
- Email, phishing, and account takeover protection
- Endpoint protection and patching
- Backups, recovery, and business continuity
- Employee training, access controls, monitoring, and response planning

This is not a replacement for a formal risk assessment, compliance review, or legal advice. It is a practical planning tool to help your team identify priorities.

1. Identity, Access, and Microsoft 365

Status	Readiness Item	Notes
[]	Multi-factor authentication is required for all email, Microsoft 365, VPN, remote access, and administrator accounts.	
[]	Administrator accounts are limited, separate from daily-use accounts, and reviewed at least quarterly.	
[]	Former employee accounts are disabled promptly and shared passwords are not used.	
[]	Conditional access, suspicious-login alerts, or equivalent controls are configured for cloud accounts.	
[]	Password reset and recovery methods are protected from unauthorized changes.	

2. Email Security and Phishing Defense

Status	Readiness Item	Notes
[]	Email filtering is enabled for phishing, malware, impersonation, and suspicious attachments.	
[]	Employees know how to report suspicious email and verify unusual payment, gift card, or credential requests.	
[]	Domain protection is configured where appropriate, including SPF, DKIM, and DMARC.	
[]	Business email compromise response steps are documented for finance, HR, and leadership teams.	
[]	Recurring phishing/security awareness training is provided to staff.	

3. Devices, Patching, and Endpoint Protection

Status	Readiness Item	Notes
☐	Workstations and servers run supported operating systems and receive security updates on a set schedule.	
☐	Endpoint protection is installed, monitored, and centrally managed where possible.	
☐	Local admin rights are limited and reviewed for staff devices.	
☐	Lost or stolen devices can be locked, wiped, or removed from company access.	
☐	Critical business applications are tracked so patches and renewals are not missed.	

4. Backups, Recovery, and Continuity

Status	Readiness Item	Notes
☐	Critical data is backed up automatically and protected from ransomware or accidental deletion.	
☐	Backups are tested regularly, not just assumed to work.	
☐	Recovery time expectations are documented for email, files, line-of-business systems, and phones.	
☐	A business continuity plan exists for outages, storms, ransomware, and internet/provider failures.	
☐	At least one person knows who to call first during an IT emergency.	

5. Network, Wi-Fi, and Vendor Access

Status	Readiness Item	Notes
☐	Firewalls, Wi-Fi, and remote access tools are reviewed and kept current.	
☐	Guest Wi-Fi is separated from business systems.	
☐	Vendor access is limited to what is needed and removed when no longer required.	
☐	Important network equipment is documented and covered by support/warranty where needed.	
☐	Remote management tools are monitored and protected with MFA where available.	

6. Monitoring, Response, and Policy

Status	Readiness Item	Notes
☐	Alerts from email, endpoint, firewall, and cloud systems are reviewed by someone responsible.	
☐	The company has a simple incident response checklist for suspected compromise or ransomware.	
☐	Cyber insurance requirements are reviewed before renewal, not after a claim.	
☐	Acceptable use, password, and device policies are documented in plain language.	
☐	Security and backup posture is reviewed after major staffing, vendor, or system changes.	

Scorecard

Add one point for every checked readiness item. Use the range below as a simple planning guide.

Score Range	What It Usually Means	Suggested Next Step
0-9	High exposure or incomplete basics.	Prioritize MFA, backups, email security, and endpoint coverage first.
10-17	Some controls are present but gaps remain.	Turn the missing items into a 30-day remediation plan.
18-24	Stronger baseline, but needs validation.	Test recovery, review admin access, and document response steps.
25+	Solid starting posture.	Keep reviewing quarterly and after major staff/vendor/system changes.

Priority Notes

Top gap to fix first	
Owner	
Target date	
Systems affected	
Follow-up review date	

How Nextek IT Can Help

If this checklist surfaces gaps you want help prioritizing, Nextek IT can help turn those findings into a practical security roadmap for your business systems, Microsoft 365 environment, backups, endpoint protection, and support operations.

Visit nextekit.com or contact Nextek IT to discuss the next right step for your organization.

Prepared for South Florida businesses by Nextek IT.