

The 10-Minute SMB Cybersecurity & IT Maturity Check

A quick, business-friendly scorecard to understand your risk,
strengthen your security, and make confident decisions.

Cybersecurity and IT maturity aren't just technical topics.
They're business essentials.

Most small and mid-sized organizations believe they're "pretty
secure," but once they look closer, they uncover blind spots:

- Unmonitored devices
- Gaps in onboarding/offboarding
- Human error vulnerabilities
- Tools that aren't configured correctly
- Outdated systems and inconsistent networks
- Missing documentation for audits or cyber insurance

This simple 10-minute self-assessment helps you quickly assess
your current situation and identify what to prioritize next.

No jargon. No technical deep dives.
Just a clear, honest picture of your cybersecurity maturity.

Instructions:

- Read each statement and check "Yes", "No", or "Unsure".
- Each section has only 5 questions.
- You'll add up your score at the end.

Let's begin!

Section 1: Foundational Security (Baselines)

These are the essential controls every modern business needs.

Question	Yes	No	Unsure
All staff use Multi-Factor Authentication (MFA) for email and critical apps.	☐	☐	☐
All company devices automatically install updates and patches.	☐	☐	☐
Endpoint protection (antivirus/EDR) is installed on every device.	☐	☐	☐
We have a documented onboarding/offboarding process.	☐	☐	☐
Administrator access is restricted to only necessary individuals.	☐	☐	☐

☐ /5 points available

Section 2: Human Risk & Employee Awareness

Your people are your biggest risk – and your biggest strength.

Question	Yes	No	Unsure
Staff receive cybersecurity awareness training at least once per year.	☐	☐	☐
We run phishing simulations to reduce human error.	☐	☐	☐
We have clear, written policies for passwords, devices, and remote work.	☐	☐	☐
Employees know how to report suspicious emails or activity.	☐	☐	☐
We can remotely wipe lost or stolen devices.	☐	☐	☐

☐ /5 points available

Section 3: Threat Monitoring & Protection

Advanced threats require proactive detection — not reactive cleanup.

Question	Yes	No	Unsure
We have 24/7 security monitoring (SOC/MDR).	☐	☐	☐
Our email system blocks phishing, spam, and impersonation attempts.	☐	☐	☐
Our firewall is modern, updated, and properly configured.	☐	☐	☐
We monitor the dark web for breached passwords and credentials.	☐	☐	☐
We receive alerts for unusual logins or suspicious activity.	☐	☐	☐

☐ /5 points available

Section 4: Backups & Business Continuity

Recovery is just as important as prevention.

Question	Yes	No	Unsure
Cloud apps (Microsoft 365/Google Workspace) are backed up.	☐	☐	☐
All important data, files, and servers are backed up regularly.	☐	☐	☐
Backups are tested at least once per year.	☐	☐	☐
We have a written incident response plan.	☐	☐	☐
We know our recovery time (RTO) and recovery point (RPO) expectations.	☐	☐	☐

☐ /5 points available

Section 5: Compliance & Cyber Insurance Readiness

Requirements are rising — and ensuring compliance reduces risk and cost.

Question	Yes	No	Unsure
We meet the technical controls required by our cyber insurance policy.	☐	☐	☐
We maintain an up-to-date inventory of systems, users, and devices.	☐	☐	☐
We store activity logs needed for audits or investigations.	☐	☐	☐
Vendor access and permissions are reviewed annually.	☐	☐	☐
We follow a recognized framework (HIPAA, CMMC, FINRA, ISO, etc.).	☐	☐	☐

☐ /5 points available

Section 6: IT Strategy & Leadership Alignment

This is what separates reactive IT from proactive, strategic IT.

Question	Yes	No	Unsure
Our IT strategy is aligned with business goals, not just break/fix support.	☐	☐	☐
We receive quarterly or annual IT/cybersecurity reviews.	☐	☐	☐
We maintain a lifecycle plan for replacing outdated technology.	☐	☐	☐
Our environment is standardized across devices and users.	☐	☐	☐
Someone (internal or external) owns IT strategy and accountability.	☐	☐	☐

☐ /5 points available

Your Total Score

Add your totals from each section:

- Foundation Security: / 5
- Human Risk: / 5
- Threat Monitoring: / 5
- Backups & Continuity: / 5
- Compliance: / 5
- Strategic IT Alignment: / 5
- **TOTAL SCORE:** / 30

Results & What Your Score Means

0–11: AT RISK — Immediate attention recommended

You likely have gaps in core security controls, monitoring, or processes. A focused plan can drastically reduce risk and improve insurance readiness.

12–19: DEVELOPING — Making progress, but inconsistent

You have some protections in place, but key areas are missing or untested. This is where cyber incidents happen most often.

20–24: MATURING — Strong foundation

You're moving toward a proactive, well-managed environment. A formal roadmap will help close remaining gaps and prepare for compliance.

25–30: OPTIMIZED — Well-protected and aligned

Your cybersecurity posture is strong, and your IT is supporting your business goals. Continue reviewing quarterly to stay ahead of evolving risks.

Recommended Next Step (Based on your score)

No matter where you land, the next best move is a clear, business-friendly roadmap.

Schedule a call with us and bring your score. We'll help you interpret it, identify key risks, and outline priority steps to strengthen your cybersecurity and IT maturity.

This isn't a sales pitch. It's guidance that is grounded in 30+ years of helping SMBs reduce risk and gain peace of mind.

Get your complimentary 20-minute
Cyber Maturity Review Call

About Preferred

Preferred helps SMBs and nonprofits protect their business, secure their data, and build long-term IT maturity.

- 98% client satisfaction across 70–90 weekly reviews
- Cybersecurity-first managed IT services
- Strategic Business Cybersecurity & Technology Reviews (BCTR)
- Expertise across Mac + Windows environments
- Deep experience in compliance-heavy industries
- Human-centered, responsive, proactive partnership

18521 Spring Creek Dr
Tinley Park, IL 60477
708-781-7110

1624 W Grand Ave.
Chicago, IL 60622

601 3-Mile Rd NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

