10-Minute Security Assessment for Small Businesses

Check your organization's security posture with this practical, jargon-free assessment.

How to use this assessment: Work through each section and check the boxes for controls you have in place. Be honest—this is for your benefit, not a compliance audit. At the end, you'll see where you stand and what to prioritize next.

1. Access Control & Authentication

- [ ] **Multi-factor authentication (MFA) is enabled for all email accounts** HIGH RISK
  Email compromise is the #1 entry point for attackers. MFA blocks most attacks even if passwords are stolen.

- [ ] **MFA is enabled for all cloud services and financial systems** HIGH RISK
  Banking, payroll, accounting software, and cloud storage all need MFA protection.

- [ ] **We have a password policy and employees use strong, unique passwords** MEDIUM RISK
  Password managers help teams create and store strong passwords without the frustration.

- [ ] **Admin accounts are limited to only people who need them**
  Not everyone needs admin rights on their computer or cloud systems. Limit privileges to reduce risk.

2. Data Backup & Recovery

- [ ] **We have automatic backups running daily** HIGH RISK
  Ransomware can't hold you hostage if you can restore from backups. Manual backups don't happen consistently.

- [ ] **Backups are stored offsite or in the cloud (not just local)** HIGH RISK
  If ransomware hits your office, local-only backups get encrypted too. Cloud or offsite storage is critical.

- [ ] **We test our backups at least quarterly** MEDIUM RISK
  Untested backups fail when you need them most. Restore a random file once a quarter to verify they work.

TSG The Stasulli Group

3. Software Updates & Patch Management

- [ ] **Automatic updates are enabled for operating systems** HIGH RISK
  Most breaches exploit known vulnerabilities that already have patches. Auto-updates close these gaps.

- [ ] **We patch business software and applications regularly**
  Office suites, browsers, Adobe products, and business apps all need regular updates.

- [ ] **Our network equipment (router, firewall) gets updated at least quarterly**
  Network devices are often forgotten but are critical entry points for attackers.

4. Email Security & Phishing Defense

- [ ] **We have email filtering/spam protection in place** MEDIUM RISK
  Email security blocks known phishing attempts and malicious links before they reach employees.

- [ ] **Employees receive security awareness training at least annually**
  Your team is your first line of defense. Regular training helps them recognize and report threats.

- [ ] **We have a process for employees to report suspicious emails**
  Make it easy for staff to flag potential phishing. A quick report can stop an attack before it spreads.

5. Incident Response & Business Continuity

- [ ] **We have an incident response plan documenting what to do if attacked** MEDIUM RISK
  Who do you call? What systems get shut down? What's the communication plan? Document it before you need it.

- [ ] **We know how long we could operate without our primary systems**
  If email/cloud/network goes down for 24 hours, can you function? Knowing this helps prioritize recovery.

- [ ] **Key employees know their role in a security incident**
  IT, management, and key staff should know their responsibilities during an incident.

6. Mobile Devices & Remote Work

- [ ] **Work devices require screen locks/passwords**
  Lost or stolen devices are a common breach source. Screen locks are your first defense.

- [ ] **Remote employees use VPN or secure connections for work**
  Public WiFi is unsafe for business data. VPNs encrypt traffic even on untrusted networks.

- [ ] **We can remotely wipe company data from lost/stolen devices**
  Mobile device management (MDM) lets you erase company data if a device goes missing.

Your Security Score

Count your checked boxes to see where you stand:

15-18 boxes checked:	**Strong foundation ✓**
10-14 boxes checked:	**Moderate risk - prioritize gaps**
5-9 boxes checked:	**High risk - immediate action needed**
0-4 boxes checked:	**Critical - you're vulnerable**

Your score: _____ / 18

Need help closing the gaps?

The Stasulli Group helps small and mid-size businesses in Central Texas and nationwide build practical, sustainable security programs—without the jargon or stress.

We can help you prioritize fixes, implement controls, and prepare for compliance requirements like HIPAA, NIST 800-171, or SOC 2.

info@stasulligroup.com • stasulligroup.com