Small Business

Cybersecurity Checklist

ACRISURE® CYBER SERVICES

For small businesses, understanding and implementing key cybersecurity measures can seem daunting. This checklist is designed to help simplify the process.

How to use this

1. Score every control 0-3 (see key).

2. Add up your total score and see criteria.

3. Close your red gaps first. (0 or 1) is a near-term action item.

4. Re-score quarterly. Consult with expert advice to help ensure maximum security.

Score	Classification
0	**Not Started:** No policy, tool, or process in place.
1	**In Progress:** Something exists (a draft policy, trial tool) but not rolled out.
2	**Mostly Done**: The control is in place for most systems but has some gaps.
3	**Fully in Place**: Fully implemented, monitored, and reviewed.

Essential Basics | These are your highest-priority security measures.

- ☐ **Passphrase & Password Manager**
  All employees use unique, strong passphrases or password manager tool.
- ☐ **Multi-Factor Authentication (MFA)**
  MFA is enabled on email, banking, and other important business accounts.
- ☐ **Automatic Software Updates**
  All computers, phones, and software update automatically.
- ☐ **Regular Data Backups**
  Critical data is backed up regularly to a separate location (e.g, cloud) and tested.
- ☐ **Endpoint Protection**
  Modern antivirus or EDR software is installed on all devices.
- ☐ **Employee Cybersecurity Training**
  Staff know how to spot phishing emails and report suspicious activity.
- ☐ **Dual Authorization Policy**
  Dual-approval for payments & critical changes.
- ☐ **Secure Offboarding/Onboarding**
  Secure procedures for employees, especially payroll and account access.

Protection Measures | Important measures to secure your operations.

- ☐ **Secure Business Email**
  Emails have authentication protocols, spam filtering, and malware scanning.
- ☐ **Access Controls**
  Employees only have access to files and systems they need for their job.

- [ ] **Secure Wi-Fi Network**
  Business Wi-Fi uses strong encryption (WPA3) and guest network is separate.
- [ ] **Data Protection**
  Sensitive data is encrypted and properly secured at rest and in and transit.
- [ ] **Web Filtering and Monitoring**
  Blocks unsafe websites or downloads, and monitor web traffic.
- [ ] **Device Security**
  Devices are physically secured from theft and automatically locks when idle.
- [ ] **Managed Detection and Response**
  Tools or services that actively monitor, detect, and respond to threats.
- [ ] **Vendor Security**
  You've reviewed the security of key vendors who handle your data.

Thinking Ahead | Getting organized and planning ahead.

- [ ] **Basic Security Policies**
  Clear rules about acceptable use of technology and reporting.
- [ ] **Cyber Liability Insurance**
  Cyber insurance coverage to help avoid financial losses from incidents.
- [ ] **Phishing Simulation Program**
  Regularly test employees' ability to detect phishing threats and scams.
- [ ] **Hardware and Software Inventory**
  Complete and maintained list of all physical devices and applications.
- [ ] **Incident Response Plan (IRP)**
  Written plan for what to do if something goes wrong.
- [ ] **Vulnerability Assessment**
  Professional scans of external/internal systems to detect vulnerabilities.

Understanding Your Score

Add up your score and reference the criteria below.

Your Total Score: _____

0-33: Foundational Stage

Major cybersecurity gaps. Your systems are exposed to ransomware, data loss, and insider threats.

34-44: Developing Stage

You've started implementing protections, but gaps and inconsistency remain.

45-55: Established Stage

Solid baseline. Controls are mostly in place, but you're still vulnerable to more sophisticated threats.

56-66: Mature Stage

You've achieved a proactive and layered defense. You're resilient, not reactive.

Next Steps: Building Your Cyber Resilience

Cybersecurity is an ongoing journey, not a one-time fix. This checklist is a starting point.

1. Prioritize	Focus on the items where you scored lowest, especially foundational controls like MFA, email security, data backups, and employee training.
2. Leverage Frameworks	For more detailed guidance, consider the NIST Cybersecurity Framework (CSF) or CIS Controls.
3. Consider Expert Help	If you lack in-house expertise or need guidance, don't hesitate to consult with a cybersecurity professionals or a Managed IT & Security Services Provider (MSSP) like Acrisure Cyber Services.

Get The Right Cybersecurity *Solutions* that Fit Your Needs & Budget All in One Place.

Acrisure Cyber Services can provide the right-sized solutions to fit your specific needs and budget. Learn more by scanning here:

IMPORTANT NOTE:

The information contained herein is provided for informational purposes only and should not be viewed as a substitute for any legal or other professional advice on any particular issue, for any particular reason, or on any particular subject matter. A meaningful review of an organization's security posture requires an individualized assessment. While the information contained herein has been compiled from sources reasonably believed to be reliable, no warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any representation contained herein.