FREE DOWNLOAD

Cyber Security Essentials for Small Business: A Complete Guide



Security Readiness Checklist

A Comprehensive Self-Assessment for Small Business Cybersecurity

72	9	3
Security Controls	Critical Domains	Priority Levels

Assess your security posture · Identify critical gaps · Build your action plan

Benchmark against industry best practices · Optimize your cyber insurance positioning

FIRST UNDERWRITERS

Insurance Brokers · Established 1992 · Pacific Northwest

How to Use This Checklist

This Security Readiness Checklist is designed to help small business owners and managers assess their current cybersecurity posture across nine critical domains.

Whether you're applying for cyber liability insurance, preparing for a compliance audit, or simply want to understand where your business stands, this checklist provides a structured, prioritized framework for evaluation and action planning.

1 Assess Each Item

Work through each of the 9 sections with your IT team or managed service provider. For each control, check the box if the item is fully implemented. Be honest — this assessment is most valuable when it reflects your actual security state.

2 Note Priority Levels

Each item includes a priority rating: High, Medium, or Low. High-priority items represent the most critical controls and should be addressed first. These ratings align with industry best practices and common cyber insurance requirements.

3 Calculate Your Score

Count the total number of items checked across all sections (out of 72 total).
Divide your checked items by 72 and multiply by 100 to get your percentage.
Use the Scoring Guide on the final page to interpret your results.

4 Build Your Action Plan

Identify all unchecked High-priority items — these are your immediate action items.
Create a 30/60/90-day implementation plan with assigned owners and deadlines.
Schedule a follow-up assessment in 90 days to measure your progress.

5 Review with Your Broker

Share your completed checklist with your First Underwriters broker to discuss how your security posture impacts your cyber insurance coverage and premiums. Identify risk transfer opportunities for gaps that cannot be immediately remediated.

Pro Tip

Many cyber insurance carriers offer premium discounts for businesses that can demonstrate strong security controls. A completed checklist can help you qualify for better rates and broader coverage.

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

1 Access Controls & Authentication

8 items

☐	Multi-factor authentication (MFA) enabled on all business-critical accounts	HIGH
☐	Strong password policy enforced (minimum 12 characters, complexity requirements)	HIGH
☐	Password manager deployed for all employees	HIGH
☐	User access rights reviewed and updated quarterly	MEDIUM
☐	Former employee accounts deactivated within 24 hours of departure	HIGH
☐	Administrative/privileged accounts limited to essential personnel only	HIGH
☐	Separate admin and standard user accounts for IT staff	MEDIUM
☐	Role-based access control (RBAC) implemented across all systems	MEDIUM

Section 1 Score: _____ / 8

5 High-priority items

2 Network Security

8 items

☐	Business-grade firewall installed, configured, and actively monitored	HIGH
☐	Wi-Fi networks secured with WPA3 encryption and unique passwords	HIGH
☐	Guest Wi-Fi network separated from internal business network	MEDIUM
☐	Virtual Private Network (VPN) required for all remote access	HIGH
☐	Network segmentation implemented to isolate sensitive data	MEDIUM
☐	Intrusion detection/prevention system (IDS/IPS) deployed	MEDIUM
☐	DNS filtering enabled to block access to known malicious sites	MEDIUM
☐	All unused network ports and services disabled	LOW

Section 2 Score: _____ / 8

3 High-priority items

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

3 Endpoint Protection & Device Management

8 items

- [ ] Antivirus/anti-malware software installed on all endpoints — HIGH
- [ ] Endpoint Detection and Response (EDR) solution deployed — MEDIUM
- [ ] Automatic operating system updates and patching enabled — HIGH
- [ ] All software applications kept current with latest security patches — HIGH
- [ ] Full-disk encryption enabled on all laptops and portable devices — HIGH
- [ ] Mobile Device Management (MDM) policy for company and BYOD devices — MEDIUM
- [ ] USB and removable media usage policy enforced — LOW
- [ ] Screen lock enforced after 5 minutes of inactivity — LOW

Section 3 Score: _____ / 8

4 High-priority items

4 Data Protection & Backup

8 items

- [ ] Critical business data identified, classified, and inventoried — HIGH
- [ ] Automated daily backups of all critical data and systems — HIGH
- [ ] Backups stored offsite or in a secure cloud environment — HIGH
- [ ] Backup restoration tested at least quarterly — HIGH
- [ ] 3-2-1 backup rule followed (3 copies, 2 media types, 1 offsite) — MEDIUM
- [ ] Sensitive data encrypted at rest and in transit — HIGH
- [ ] Data retention and disposal policies documented and followed — MEDIUM
- [ ] Secure data destruction procedures for decommissioned hardware — MEDIUM

Section 4 Score: _____ / 8

5 High-priority items

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

5 Email & Communication Security

8 items

☐	Email filtering and anti-phishing solution deployed	HIGH
☐	SPF, DKIM, and DMARC records configured for all company domains	HIGH
☐	Employees trained to identify and report phishing attempts	HIGH
☐	Simulated phishing exercises conducted at least twice annually	MEDIUM
☐	Email encryption available for sending sensitive information	MEDIUM
☐	Business Email Compromise (BEC) prevention controls in place	HIGH
☐	Verification protocol for wire transfers and payment changes	HIGH
☐	Auto-forwarding rules monitored and restricted	LOW

Section 5 Score: _____ / 8

5 High-priority items

6 Employee Training & Security Culture

8 items

☐	Cybersecurity awareness training completed by all employees annually	HIGH
☐	New hire security orientation completed within first week	HIGH
☐	Documented acceptable use policy signed by all employees	MEDIUM
☐	Social engineering awareness training conducted regularly	MEDIUM
☐	Clear procedures for reporting suspected security incidents	HIGH
☐	Security champion or point-of-contact designated for each department	LOW
☐	Regular security newsletters or updates shared with staff	LOW
☐	Clean desk and clear screen policy enforced	LOW

Section 6 Score: _____ / 8

3 High-priority items

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

7 Incident Response & Business Continuity

8 items

☐	Written Incident Response Plan (IRP) documented and accessible	HIGH
☐	Incident response team identified with clear roles and responsibilities	HIGH
☐	Incident response plan tested via tabletop exercise at least annually	HIGH
☐	Cyber insurance policy in place with adequate coverage limits	HIGH
☐	Insurance carrier's breach response hotline documented and accessible	HIGH
☐	Business continuity/disaster recovery plan documented and tested	HIGH
☐	Contact list for key vendors, legal counsel, and law enforcement current	MEDIUM
☐	Communication templates prepared for breach notification	MEDIUM

Section 7 Score: _____ / 8

6 High-priority items

8 Vendor & Third-Party Risk Management

8 items

☐	Inventory of all third-party vendors with access to company data	HIGH
☐	Vendor security assessments conducted before onboarding	MEDIUM
☐	Data processing agreements (DPAs) in place with all relevant vendors	MEDIUM
☐	Vendor access limited to minimum necessary permissions	HIGH
☐	Cloud service provider security configurations reviewed	MEDIUM
☐	SaaS application inventory maintained and reviewed quarterly	MEDIUM
☐	Third-party access revoked promptly when relationships end	HIGH
☐	Critical vendor business continuity capabilities verified	LOW

Section 8 Score: _____ / 8

3 High-priority items

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

9 Compliance & Documentation

8 items

☐	Written Information Security Policy (WISP) documented	HIGH
☐	Privacy policy compliant with applicable regulations (state/federal)	HIGH
☐	Industry-specific compliance requirements identified and met	MEDIUM
☐	Security policies reviewed and updated at least annually	MEDIUM
☐	Asset inventory of all hardware, software, and data maintained	MEDIUM
☐	Risk assessment conducted at least annually	HIGH
☐	Security audit logs retained per regulatory requirements	MEDIUM
☐	PCI DSS compliance verified if accepting credit card payments	HIGH

Section 9 Score: _____ / 8

4 High-priority items

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.

Scoring Guide & Next Steps

Your Total Score: _____ / 72 Controls Implemented

Percentage: (Your Score ÷ 72) × 100 = _____ %

Performance Tiers

90 – 100% — **Excellent**

Strong security posture. Focus on continuous improvement and emerging threats.
You're well-positioned for favorable cyber insurance terms.

70 – 89% — **Good**

Solid foundation with room for improvement. Prioritize completing all High-priority items.
Review your cyber insurance coverage to ensure alignment with your risk profile.

50 – 69% — **Needs Improvement**

Significant gaps exist. Develop a 90-day action plan targeting High-priority items first.
Contact your broker to discuss risk mitigation options and coverage adjustments.

Below 50% — **At Risk**

Critical vulnerabilities present. Immediate action required on all High-priority items.
Engage a qualified IT security provider and contact First Underwriters to review coverage needs.

Priority Level Guide

HIGH	Critical controls addressing the most common and impactful cyber threats. Address first.
MEDIUM	Important controls that strengthen your overall security posture. Target in your 60-day plan.
LOW	Best-practice controls that enhance security maturity. Include in your long-term roadmap.

Ready to Strengthen Your Cyber Protection?

First Underwriters specializes in helping small businesses find the right cyber liability coverage to protect against data breaches, ransomware, and business interruption. Contact us for a complimentary cyber risk review and insurance consultation.

www.firstunderwriters.com

This checklist is for informational purposes only and does not constitute professional cybersecurity advice.