SMALL BUSINESS CYBERSECURITY CHECKLIST

Practical Cybersecurity Safeguards Every Organization Should Implement

Protect your business from phishing attacks, ransomware, data breaches, and operational disruptions with this practical cybersecurity assessment guide.

Written By Justin Small, US Air Force (Retired)

Prepared By

Justin Small, US Air Force (Retired)

Cybersecurity Consultant

25+ Years of Information Technology & Cybersecurity Experience

20-Year U.S. Air Force Veteran

CompTIA Security+ Certified

Executive VP, IT & Cybersecurity Director for Diamond Self Storage Management, LLC

Creative Web Solutions -

Helping Small Businesses Improve Their Technology and Cybersecurity

---

Inside This Guide

Introduction

Cybersecurity does not have to be complicated or expensive. Most cyberattacks succeed because basic security controls are missing, outdated, or ignored.

This checklist covers practical cybersecurity safeguards that every small business should implement to reduce the risk of ransomware, phishing attacks, data breaches, and business disruptions.

Use this document as a starting point to evaluate your organization's security posture.

Account Security

Multi-Factor Authentication (MFA)

☐ MFA is enabled for email accounts.

☐ MFA is enabled for Microsoft 365 or Google Workspace.

☐ MFA is enabled for banking and financial accounts.

☐ MFA is enabled for remote access tools.

☐ MFA is enabled for cloud storage services.

Why It Matters

Passwords can be stolen. MFA adds a second layer of protection that significantly reduces the likelihood of unauthorized access.

Password Management

☐ Employees use unique passwords for every system.

☐ Passwords are at least 12 characters long.

☐ Password manager software is used.

☐ Shared passwords are eliminated whenever possible.

☐ Former employee passwords have been disabled.

Why It Matters

Weak or reused passwords remain one of the most common causes of security incidents.

Email Security

Phishing Protection

☐ Employees receive phishing awareness training.

☐ Staff know how to identify suspicious links.

☐ Staff verify unexpected requests for money or sensitive information.

☐ Email filtering and spam protection are enabled.

☐ Employees know who to contact if they suspect phishing.

Why It Matters

Phishing remains the most common attack method used against small businesses.

Computer Security

Endpoint Protection

☐ Antivirus or endpoint protection is installed.

☐ Security software updates automatically.

☐ Unauthorized software installation is restricted.

☐ Screens lock automatically after inactivity.

☐ Employee computers are encrypted.

Why It Matters

Endpoints are often the first target during a cyberattack.

Software Updates

☐ Operating systems are updated regularly.

☐ Web browsers are updated.

☐ Office software is updated.

☐ Network devices receive firmware updates.

☐ Unsupported software has been removed.

Why It Matters

Many attacks exploit known vulnerabilities that already have available patches.

Data Protection

Backups

☐ Critical business data is backed up daily.

☐ Backups are stored separately from production systems.

☐ Backup restoration testing is performed.

☐ Cloud backups are enabled where appropriate.

☐ Backup procedures are documented.

Why It Matters

Backups are often the difference between recovery and business interruption after a ransomware attack.

Network Security

Wireless Network

☐ Wi-Fi uses WPA2 or WPA3 encryption.

☐ Default router passwords have been changed.

☐ Guest Wi-Fi is separated from business systems.

☐ Remote management is disabled unless required.

☐ Network equipment firmware is current.

Why It Matters

Poorly secured networks provide easy access for attackers.

Employee Access Control

User Accounts

☐ Every employee has an individual login.

☐ Shared accounts are minimized.

☐ Administrative privileges are limited.

☐ Employee access is reviewed regularly.

☐ Accounts are disabled immediately upon termination.

Why It Matters

Employees should only have access to systems necessary for their job duties.

Physical Security

Office Security

☐ Server and network equipment are secured.

☐ Visitor access is controlled.

☐ Sensitive documents are protected.

☐ Computer screens are not visible to the public.

☐ Mobile devices are protected with passwords or biometrics.

Why It Matters

Cybersecurity includes physical security controls.

Incident Response

Cyber Incident Readiness

☐ Employees know how to report suspicious activity.

☐ Emergency contacts are documented.

☐ Critical vendors are identified.

☐ Cyber insurance information is readily available.

☐ A written incident response plan exists.

Why It Matters

Preparation can significantly reduce the impact of a cybersecurity incident.

Cybersecurity Self-Assessment Score

Count the number of completed items:

☐ 0–15 Completed
High Risk – Significant cybersecurity improvements recommended.

☐ 16–30 Completed
Moderate Risk – Several important controls should be strengthened.

☐ 31–45 Completed
Good Security Posture – Continue improving and reviewing controls.

☐ 46–55 Completed
Strong Security Posture – Maintain and regularly assess security practices.

About the Author

Justin Small has more than 25 years of information technology and cybersecurity experience, including 20 years of service in the United States Air Force. He currently serves as Executive Vice President, IT and Cybersecurity Director for Diamond Self Storage Management and provides cybersecurity consulting services to small businesses and self-storage operators throughout Texas.

For additional cybersecurity resources and consulting services, visit Creative Web Solutions, http://www.texascws.com.