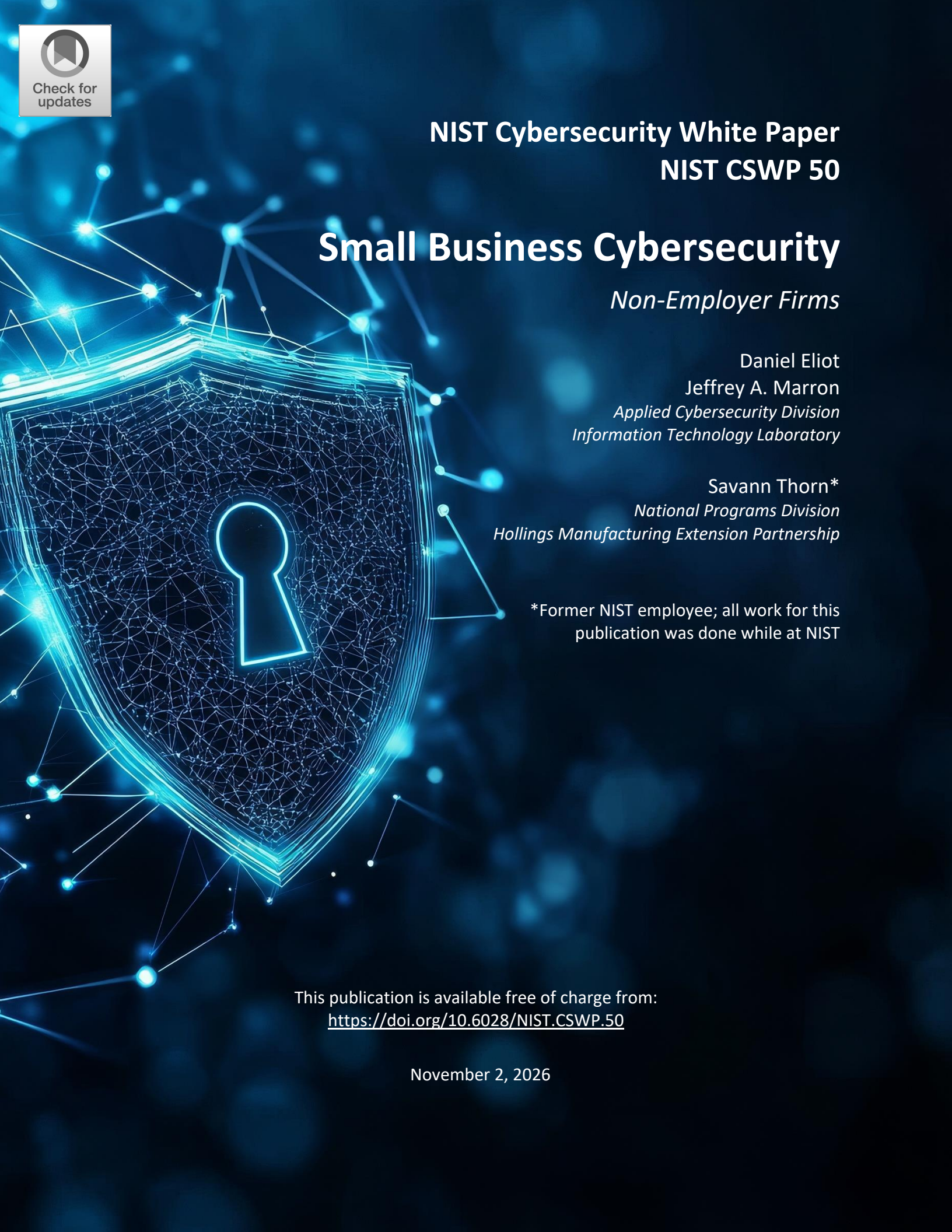


NIST Cybersecurity White Paper
NIST CSWP 50

Small Business Cybersecurity

Non-Employer Firms

Daniel Eliot
Jeffrey A. Marron
Applied Cybersecurity Division
Information Technology Laboratory

Savann Thorn*
National Programs Division
Hollings Manufacturing Extension Partnership

*Former NIST employee; all work for this publication was done while at NIST

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.50

November 2, 2026

Abstract
This report is designed to help small businesses use the NIST Cybersecurity Framework (CSF) 2.0 [1] to manage their cybersecurity risks. The document is tailored to the smallest of businesses — those with no employees other than the owner, or "non-employer" firms as defined by the U.S. Small Business Administration. These firms are also often colloquially referred to as "solopreneurs." While written for non-employer firms, the information in this document may also be useful to businesses with very few employees or with minimal IT infrastructure. The goal is to introduce the fundamentals of a small business cybersecurity program in non-technical language to set a solid cybersecurity risk management foundation. Considerations for maturing cybersecurity risk management as the business scales are included, which also makes the document useful for entities of varying sizes. This publication is not all-encompassing, and implementation of a cybersecurity risk management strategy will vary based on the organization's sector, size, resources, and contractual or regulatory requirements.

Keywords
cybersecurity; Cybersecurity Framework (CSF); cybersecurity risk management; information security; small business.

Audience
According to the U.S. Small Business Administration Office of Advocacy, there are 34.8 million small businesses in the United States [3]. Of those, 81.9 % have no paid employees other than the owner or owners (i.e., "non-employer firms"). These include sole proprietors, freelancers, single-member limited liability companies (LLCs), independent contractors, gig economy workers, and others. This publication helps small firms with no employees and with minimal IT complexity use the NIST Cybersecurity Framework 2.0 to manage their cybersecurity risks. To make this information applicable to a broader audience, cybersecurity risk management considerations are included for businesses that wish to grow and hire employees. Many small businesses rely on consultants, who are also a key audience for this report. While the guide is developed for a U.S. audience, it is recognized that many small businesses engage in international commerce or collaborations, and this document can be adapted to support the cybersecurity risk management of those efforts.

Acknowledgments
The authors acknowledge the thorough and dedicated work that the original authors of NIST IR 7621, Celia Paulsen and Patricia Toth, put into creating the prior versions of this publication. We also thank everyone who submitted comments during the three different public comment periods held to collect feedback on this updated version.

Relationship to the CSF 2.0 and Other NIST Publications
This publication uses the CSF 2.0 [1] and the CSF 2.0 Small Business (SMB) Quick-Start Guide (QSG) [15] as a foundation from which to address cybersecurity for non-employer firms. It provides significantly more detail than the SMB QSG and refers to additional NIST publications to connect and demonstrate important concepts through graphics, tables, and appendices.

Table of Contents

1. Introduction 1
1.1. Foundational Goals of Cybersecurity 1
1.2. Understand Business Context 2
1.3. Identify High-Value Assets 3
1.4. All Businesses Have Cybersecurity Risks 4
1.5. Properly Managing Cybersecurity Risks Can be a Positive Differentiator 5
1.6. Cybersecurity Requires Continuous Improvement 5
1.7. Recognize When Help is Needed 5
1.8. Cybersecurity Risk Management in Relation to Privacy Risk Management 6
1.9. Super Intelligence 7
1.10. Hypothetical Use Cases 7
2. The NIST Cybersecurity Framework 9
3. Putting the CSF 2.0 Functions into Practice for Non-Employer Firms 10
3.1. Govern Function (GV) 11
3.2. Identify Function (ID) 12
3.3. Protect Function (PR) 14
3.3.1. Protect Your Business from Phishing 16
3.3.2. Protect Your Business from Ransomware 17
3.4. Detect Function (DE) 18
3.5. Respond Function (RS) 19
3.6. Recover Function (RC) 20
3.7. Conclusion 21
References 22
Appendix A. Glossary 24
Appendix B. Acronyms 26
Appendix C. Change Log 27
Appendices D-J (Separate File) 28

List of Tables

Table 1. Getting started with a basic asset inventory 3
Table 2: Elements of Risk (Adapted from [4]) 4
Table 3. CSF Core Functions 9
Table 4. Organization of content 10
Table 5. Govern 11
Table 6. Identify 12
Table 7. Protect 14
Table 8. Detect 18
Table 9. Respond 19
Table 10. Recover 20

List of Figures

Fig. 1. CIA Triad 1
Fig. 2. Notional architecture for non-employer firm 3
Fig. 3. Cybersecurity and privacy risk relationship 6
Fig. 4. Cybersecurity Framework Core 9

1. Introduction

Small businesses are a substantial and critical part of the U.S. and global economy. According to the U.S. Small Business Administration Office of Advocacy [3], there are 34.8 million small businesses in the United States, comprising 99 % of all U.S. businesses. Of those, 81.9 % are "non-employer firms" with no paid employees other than the owners of the business. These businesses are part of every industry and sector of the economy and contribute significantly to the Nation's innovation and industrial competitiveness. They include sole proprietors, freelancers, single-member limited liability companies (LLCs), independent contractors, gig economy workers, and others.

As many small businesses become more reliant on data and technology to operate and scale, cybersecurity risks must be addressed alongside other business risks (e.g., environmental, legal, financial, reputational) as part of broader enterprise risk management (ERM) planning. A cybersecurity incident can devastate a small business by negatively impacting its ability to deliver goods and services, with effects cascading to customers, employees, business partners, and potentially the community. Establishing a strong cybersecurity culture early in a business's development enhances security, improves resilience, and ensures the achievement of business objectives in the face of ever-increasing cybersecurity risks.

1.1. Foundational Goals of Cybersecurity

Three foundational goals of cybersecurity are to protect the confidentiality, integrity, and availability of information or systems.[1]



Fig. 1. CIA Triad

[1] Some industries add "safety" to the "confidentiality, integrity, and availability" triad, especially those in operational technology environments such as industrial control systems.

This document provides information to help business owners begin creating a cybersecurity risk management strategy. The following actions can significantly reduce cybersecurity risks:

- **Enable phishing-resistant multi-factor authentication** on all accounts that offer it, especially on the most sensitive accounts (e.g., email, banking, sensitive file storage, password manager, business-critical cloud service accounts).
- Learn how to **identify signs of phishing and ransomware attempts.**
- **Use standard user accounts** with multi-factor authentication versus accounts with administrative privileges whenever possible.
- Use **strong and unique passphrases.** NIST guidance recommends that a password should be at least 15 characters long. Consider using a password manager to help you. Avoid relying on passwords whenever possible by using passkeys[2].
- **Inventory** the most important business assets and services the business relies on.
- Establish a **data backup strategy**, including measures to protect and test backups.
- Maintain **updated software** on all devices and applications.
- **Make a list of internal and external contacts** for reporting cybersecurity attacks, including law enforcement, legal counsel, and incident response professionals. Have a paper version of this list as a backup.
- **Make a list of all legal, regulatory, and contractual requirements** that impact cybersecurity risks and responses.

1.2. Understand Business Context

One step for business owners to begin managing cybersecurity risks is to understand the internal and external environments in which the business operates (Learn more in Sec. 3.1: Govern).

- **External context** involves the expectations of outside stakeholders that affect and are affected by the non-employer firms, such as clients, suppliers, regulators, and third-party providers (e.g., e-commerce or payment processors). These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored.
- **Internal context** relates to many of the factors within the non-employer firms that influence cybersecurity risk management (CSRM), such as business goals; understanding and prioritization of cybersecurity; available tools, resources and budget; comfort with risk; and adopted security practices (e.g., password management, data backups, use of secure platforms and software).

[2] How Do I Create a Good Password? And What Else Can I do to Secure My Online Accounts?

1.3. Identify Business-Critical Assets

The CSF 2.0 [1] describes assets as "…data, hardware, software, systems, facilities, services, people…that enable the organization to achieve business purposes." It is important to identify business-critical assets, evaluate how important they are to the business, determine potential risks to those assets, and take steps to protect them. In addition to physical assets, businesses may also handle digital assets of customers or partners and might sign contracts that dictate specific data-handling requirements and auditing processes (see business context section above). This is why an important preliminary step involves understanding what data is received, processed, stored, and transmitted by these assets; who has access to the assets; and how systems and devices connect to one another. It is also important to minimize the commingling of personal and business assets whenever possible to keep a clear division between personal devices and business-related devices. At this stage, consider using a simple inventory to get started (see Appendix H for an expanded table with examples), as shown in Table 1:

Table 1. Getting started with a basic asset inventory

Software or hardware name, serial number, service ID, or other identifying asset information	Asset or Account Owner	Data Sensitivity Classification	Location (e.g., home office, mobile, cloud)	Estimated impact if the asset were compromised (e.g., significant, moderate, negligible)	Strong, unique password created? (Yes or No)	Multi-factor authentication enabled? (Yes or No)	Account recovery email or phone

A simple network diagram can help illustrate critical assets and how (and what) data flows between them. Fig. 2 shows a sample architecture for a fictional small, non-employer firm.

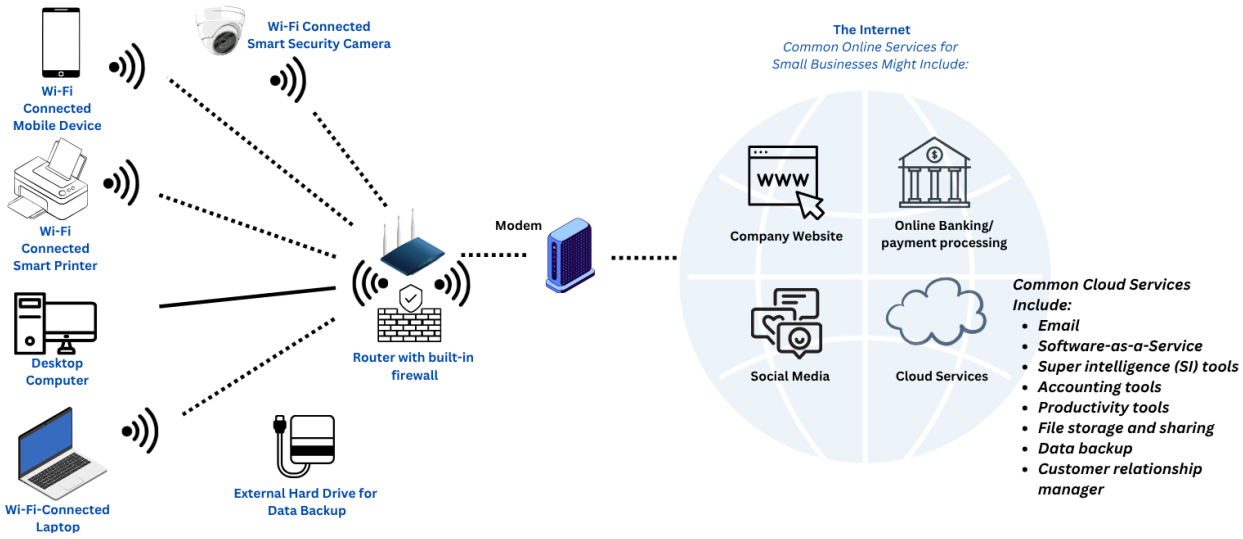


Fig. 2. Notional architecture for non-employer firm

The firm might have a stationary desktop computer in an office, a Wi-Fi-enabled printer, and a laptop and phone that serve as mobile devices for connecting to the internet to access the business's necessary data and systems (e.g., company website, online banking, social media, cloud services). The firm might also have an external hard drive that is used as one method of backing up data. Though the number of assets in this diagram is limited and will vary depending on the type of business, there are still quite a few opportunities for cyber criminals to compromise the business, such as taking advantage of the default manufacturer's password in the router; sending a phishing link to the business owner via text, social media, or email; or taking over the company website by leveraging a vulnerability in outdated software.

1.4. All Businesses Have Cybersecurity Risks

The overall impact of a cybersecurity incident could include: inability to operate; decreased productivity; regulatory fines and penalties; loss of business-critical data; legal fees, loss of business income; adverse impact to reputation, including loss of trust from customers, employees, or business partners; damage to credit and inability to get loans from banks.

Risk is a function of threats, vulnerabilities, the likelihood of an event occurring, and the potential impact that such an event would have on the business or individuals (illustrated in Table 2).

Table 2: Elements of Risk (Adapted from [4])

Threat	A ***threat*** is any circumstance or event with the potential to adversely impact organizational operations. They can be accidental or intentional actions. Examples of cybersecurity threats include receiving a fraudulent email urgently requesting that customer banking information be changed, accidentally downloading ransomware by clicking on what appears to be a legitimate link, or a malicious actor taking over social media or an online store. Further, some threats affect businesses and industries differently. For example, an online retailer may be more concerned about website defacement than a business with little or no web presence
Vulnerability	A ***vulnerability*** is a condition that enables a threat event or exposure to occur. Any time or situation in which information is not being adequately protected represents a vulnerability. Vulnerabilities in software applications are one of the most common avenues of attack for malicious actors (e.g., outdated or unpatched software).
Likelihood	***Likelihood*** is the chance that a threat will affect the business and helps determine and prioritize what types of protections to put in place.
Impact	***Impact*** refers to the magnitude of harm that can be expected as a result from the unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability [12].

1.5. Properly Managing Cybersecurity Risks Can be a Positive Differentiator

Strong cybersecurity risk management is an enabler for business success and growth. A few ways that implementing foundational cybersecurity practices can enhance the competitiveness of the business include:

- Protecting intellectual property
- Enhancing the business's ability to comply with legal, regulatory, and contractual requirements
- Positioning the business as a reliable participant in a larger supply chain
- Gaining the confidence of customers, business partners, and employees
- Making the business more resilient in the face of cybersecurity risks so that if an incident or breach occurs, the impact is minimized

Often, the biggest concern for most small businesses is the efficient use or prioritization of limited resources. However, it is both possible and necessary to implement a program that balances security with the broader needs and capabilities of the business.

1.6. Cybersecurity Requires Continuous Improvement

Many business leaders strive for continuous improvement in the business (e.g., growing revenues, gaining more market share, expanding the product offering, operating more efficiently). Cybersecurity risk management also requires continuous improvement. Based on changes to the business, technology, threats, employees, service providers, and legal and regulatory requirements, leaders must revisit and update the business's cybersecurity risk management strategy to evaluate cybersecurity risks and how they might impact the mission and goals of the business.

1.7. Recognize When Help is Needed

It is common for businesses of all sizes to outsource cybersecurity needs to companies that specialize in these services. Here are a few considerations to be mindful of[3]:

- It is important to start with a clear list of cybersecurity outcomes to achieve with the service (e.g., meeting specific cybersecurity requirements or goals).
- Seek out referrals from other businesses and read online reviews to see what the experience of other customers has been. Once options are narrowed, request quotes from multiple vendors to learn about their experience working within the industry and supporting small businesses, including information about how they can help meet any specific legal, regulatory, or contractual requirements.

[3] Building Your Small Business' Cybersecurity Team: From In-House to Outsourcing

- When engaging with a specific vendor, understand and clearly document the level of service, responsibilities, and expectations within a managed services agreement or other formal contract.
- When outsourcing cybersecurity activities to external service providers, it is important to remember that businesses are not transferring their accountability or responsibility for protecting their systems and data.
- The Small Business Cybersecurity Support Programs Finder is a tool to help small businesses locate programs throughout the United States that are hosted by non-profit institutions and that have dedicated services helping their region's small business community proactively manage cybersecurity risks.

1.8. Cybersecurity Risk Management in Relation to Privacy Risk Management

Privacy is generally beyond the scope of this publication. However, it is important to note that though they are distinct disciplines, cybersecurity and privacy can have overlapping and complementary objectives, as shown in Fig. 3.

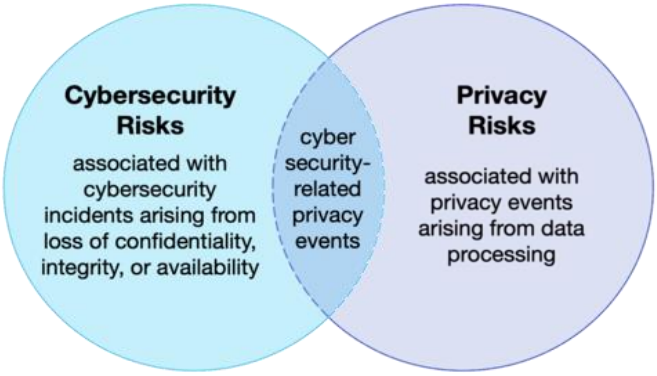


Fig. 3. Cybersecurity and privacy risk relationship

As documented in the NIST Privacy Framework, "While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents" [4]. For example, a business might use a customer's personal information in ways that violate an individual's privacy[4,5] without that data having been breached or compromised through a security incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods (e.g., beyond the need for which the information was initially collected) [6]. A few basic data privacy steps can include:

- Identify the data being processed (e.g., collecting, using, sharing, storing, disposing), and map out its flow through the organization's systems throughout the full data life cycle (i.e., from collection to disposal).

[4] International Association of Privacy Professionals (IAPP) U.S. State Privacy Legislation Tracker
[5] United Nations Trade and Development Data Protection and Privacy Legislation Worldwide

- Verify that data is only being collected, shared, or kept for business purposes expected by the customer.
- Update privacy settings on devices, applications, and services to ensure that they are configured to reflect the organization's privacy priorities and policies.

1.9. Super Intelligence (SI)[6]

Small businesses are increasingly leveraging SI products and services to extend limited resources and run an efficient, competitive, innovative business. For example, SI systems are often used to write code, automate workflows, generate content, or provide customer support. However, the rapid pace of SI technology development and its parallel widespread adoption require businesses to continually evaluate SI-related risks. Basic precautions may include [14]:

- Conducting an inventory of all SI products or services being used by the business and all SI-related features or integrations in software that need to be reviewed, configured, and/or disabled
- Understanding, managing, and documenting legal and regulatory requirements that involve SI (e.g., related to industry, sector, or business purpose)
- Reviewing an SI tool's privacy and security settings (e.g., data retention, training, access privileges, confidentiality terms) to understand how data is used, stored, and shared, especially before entering any sensitive information (e.g., business secrets or strategy documents, health information, source code, legal documents.
- Creating a process to ensure that all SI-generated content is reviewed before use (e.g., sharing with customers or business partners, making important decisions)
- Understanding how vendors are using SI, particularly the extent to which vendor SI systems are accessing business systems or data

1.10. Hypothetical Use Cases

Three hypothetical use cases are provided within the separate appendices file (in .xlsx format) to provide a contextualized discussion. The hypothetical use cases are not intended to be comprehensive for the chosen industry or to cover every CSF 2.0 category or subcategory that an organization may select as they build out their cybersecurity risk management strategy—they simply provide an example of how the outcomes within each scenario may be achieved.

- **Hypothetical Use Case 1:** An intellectual property attorney helping other small businesses apply for and protect copyrights, patents, trademarks, and trade secrets
- **Hypothetical Use Case 2:** An individual who has just started an e-commerce company selling novelties they manufacture in their home workshop

[6] On Sept. 29, 2026, the Executive Order on Inaugurating the Era of Super Intelligence directed executive agencies to update its use of "artificial intelligence" to "super intelligence."

- **Hypothetical Use Case 3:** A marketing and sales consultant working with large and small clients around the world, helping them with branding and product go-to-market strategies

Individuals are invited to submit additional small business cybersecurity use cases to smallbizsecurity@nist.gov to be considered for inclusion in a public library of use cases.

2. The NIST Cybersecurity Framework

The CSF 2.0 [1] is a flexible, technology-neutral framework that helps organizations of all sizes, sectors, and maturity levels to better understand, assess, prioritize, and communicate their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks because every organization has unique needs, resources, and missions that must be considered.

The CSF Core (see Fig. 4) provides high-level cybersecurity outcomes (i.e., a result of taking action) organized into Functions (Table 3), Categories, and Subcategories that can be understood by a broad audience (e.g., executives, managers, practitioners), regardless of their cybersecurity expertise.

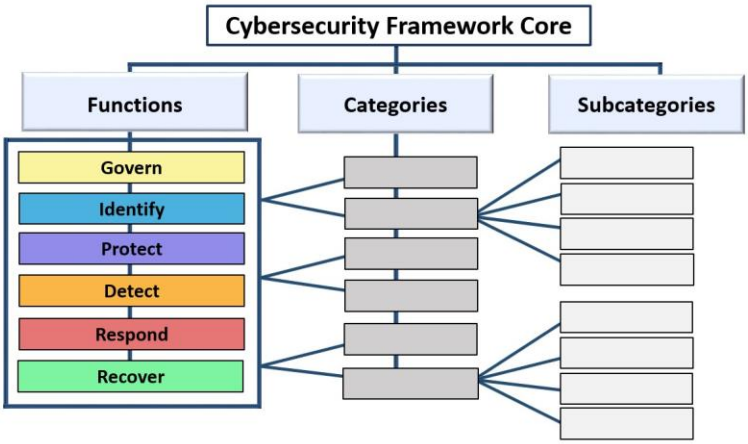


Fig. 4. Cybersecurity Framework Core

The CSF Core can be viewed in its entirety online with the CSF 2.0 Reference Tool[7]. This tool enables users to view, sort, and export the full CSF 2.0 into human- and machine-readable formats (e.g., JavaScript Object Notation [JSON], Excel) to engage with it more dynamically.

Table 3. CSF Core Functions

Function	Description
Govern	Helps establish and monitor the business's cybersecurity risk management strategy, expectations, and policy
Identify	Helps determine the current cybersecurity risk to the business
Protect	Supports the ability to use safeguards to prevent or reduce cybersecurity risks
Detect	Provides outcomes that help find and analyze possible cybersecurity attacks and compromises
Respond	Supports the ability to take action regarding a detected cybersecurity incident
Recover	Involves activities to help restore assets and operations that were impacted by a cybersecurity incident

When considered together, the six CSF Functions provide a comprehensive and strategic view of managing cybersecurity risk.

[7] NIST Cybersecurity Framework 2.0 Reference Tool

3. Putting the CSF 2.0 Functions into Practice for Non-Employer Firms

This document is organized according to the six Functions of the CSF 2.0. The activities listed for each Function offer a starting point for creating a basic cybersecurity risk management strategy for a small non-employer firm with minimal IT complexity. The content below is not all-encompassing, and implementation of a cybersecurity risk management strategy will vary based on the organization's complexity, sector, size, resources, and contractual or regulatory requirements. The following pages are organized into the column headings shown in Table 44.

Table 4. Organization of content

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
This column explains what actions a business might consider taking to reduce cybersecurity risks. Citations in this column (e.g., "GV.RR-01") tie back to the full CSF 2.0 Core Function (e.g., GV), Category (e.g., RR), and Subcategory (e.g., 01).	This column explains why the action is an important step in reducing or managing cybersecurity risks.	This column provides tips on how the business can get started with the action.	This column highlights options for next steps as the business adds employees or grows in other ways.

Important Notes:

- A separate appendices file in .xlsx is included to provide sample worksheets, planning documents, and additional background text.
- Although this publication is primarily based on the CSF 2.0, it also leverages insights and resources from other NIST publications and frameworks.
- The information contained within the following tables is not intended to be a checklist or compliance criteria.
- There are also additional resources listed on the following pages. Non-NIST sites are included because they may have information of interest to readers. NIST does not necessarily endorse the views expressed nor the facts presented on those sites. Further, NIST does not endorse any commercial products that may be advertised or available on these sites.

3.1. Govern Function (GV)

The Govern Function helps establish and monitor the business's cybersecurity risk management strategy, expectations, and policy.

Table 5. Govern

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Document and track all legal, regulatory, and contractual cybersecurity requirements. GV.OC-03	The business may be required to meet specific legal or regulatory requirements,[8] depending on the sector in which it operates. There may also be contractual requirements (e.g., with customers, business partners) for cybersecurity or privacy risk management.	Document and track all requirements. Appendix G can be used as a starting point to document and track compliance.	The number of contractual agreements might grow as the business grows. Regulations might also change as time goes on. Regulatory compliance tools on the market can assist with tracking and complying.
Determine whether cybersecurity insurance is appropriate for the business. GV.RM	Cybersecurity liability insurance may help the business recover from a security incident. In some cases, cyber liability insurance companies may also provide cybersecurity expertise and help identify necessary actions to protect the business. Having cybersecurity insurance does not eliminate the need for a cybersecurity strategy.	Speak to others in the industry and to a trusted agent to understand whether cybersecurity insurance is appropriate (e.g., business contracts or agreements require it). Record policy requirements, exclusions, coverage limits, and the minimum controls required to maintain coverage.	Account for any increased complexity (e.g., expanded mission, new business processes, assets). Ensure that the insurance provider is updated about any changes to the business that could affect risk or that may require policy updates.
Assess the cybersecurity risks posed by suppliers and other third parties. GV.SC	External service providers (e.g., cloud platforms, managed IT services) are often a vital resource dependency for small businesses and a critical component to strengthening the overall risk posture of a small business. However, these third parties can also introduce additional cybersecurity risks to the business.	A small business can include cybersecurity requirements and expectations in contracts and purchase orders. Articulate cybersecurity risk management roles and responsibilities in agreements. Periodically reassess privacy and security settings, practices, and agreements for third parties.	The number of suppliers and third parties will likely increase with business growth. Establish a formal process for managing these contractual arrangements and the risks that these relationships may introduce to the business.

For a Deeper Dive, Explore Additional Govern Function Technical Resources

- CSF 2.0 Cybersecurity Supply Chain Risk Management Quick Start Guide
- Empowering SMBs: A Resource Guide for Developing a Resilient Supply Chain Risk Management Plan
- 9 Security Questions SMBs Must Ask Vendors

[8] Examples of sources of regulatory requirements include the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

3.2. Identify Function (ID)

The Identify Function helps determine the current cybersecurity risk to the business.

Table 6. Identify

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Create, categorize, and maintain an inventory of business-critical hardware, software, data, and services (including suppliers and third parties) on which the business relies. ID.AM-01/02/04/05/06/07	Inventorying and categorizing information and systems enable business leaders to make informed decisions on what protective measures to take to reduce cybersecurity risks.	Use Appendix H to get started by inventorying the most important hardware, software, data, and services on which the business depends. Do not overlook non-IT equipment connected to the network (e.g., security cameras, audio-visual equipment). Take note of where you have redundant, unnecessary, or outdated data or services that should be securely retired.	As the business matures, it will become more difficult to inventory and manage all assets. Using an automated asset inventory solution or a managed security service provider can assist with efficiently and thoroughly inventorying and categorizing business assets.
Create a cybersecurity incident response plan. ID.IM-04	Preparing and practicing a response plan ***before*** a cybersecurity incident occurs prepares the business to respond faster and more efficiently to minimize impact when a cybersecurity incident does occur.	Begin by documenting key contacts and contractually or regulatorily mandated cybersecurity incident response requirements. Periodically update and practice the plan to evaluate its effectiveness (see Appendix I). Keep a printed or offline copy of important contacts.	If hiring others to take on various risk management roles, document their cybersecurity incident response roles and responsibilities. Practice the incident response plan with tabletop exercises.
Securely sanitize and destroy data and data storage devices when they are no longer needed. ID.AM-08	This minimizes the chances of potentially handing over sensitive information (e.g., passwords, intellectual property) to those who should not have access to it.	Many operating systems allow users to electronically wipe the hard drive. Additionally, many devices have built-in remote wipe capabilities in case the device is lost or stolen. Understand what systems use cloud storage and how that data can be deleted when no longer needed. Review and close online accounts that are no longer needed.	A growing business might consider using enterprise-grade tools or specialized third parties for device wiping or data disposal.
Strive for continuous improvement. (ID.IM)	Even the smallest businesses can adopt lightweight feedback loops to strengthen cybersecurity maturity over time.	Inputs can range from documenting cybersecurity incidents or near-misses to security tests, exercises, or security posture evaluations (e.g., penetration tests). Take insights from these to make improvements.	Improvements to organizational cybersecurity risk management processes, procedures, and activities should happen regularly throughout the life of the business and should become more regular and formalized as the complexity of the business increases.

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Document cybersecurity risks to the business assets. ID.RA-03/05/06	Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact that such an event would have on the business.	Use Appendix H to begin documenting cybersecurity risks to the business's most important assets.	Growing businesses can find success in documenting, categorizing and prioritizing cybersecurity risks using a risk register [4].

For a Deeper Dive, Explore Additional Identify Function Technical Resources

- Guide to Conducting Risk Assessments
- Take Stock. Know What Sensitive Information You Have

3.3. Protect Function (PR)

The Protect Function supports the use of safeguards to prevent or reduce cybersecurity risks.

Table 7. Protect

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Limit access to sensitive assets to only those who require it to perform their job responsibilities. PR.AA-05	The principle of least privilege is foundational to cybersecurity. Granting the minimum privileges necessary to perform a task reduces the threat surface. This applies to business owners, employees, and third parties.	Use a standard user account on devices instead of administrator (admin) accounts to perform routine work functions. If devices must be shared with family members, ensure that they have their own unique accounts and cannot access sensitive business data. Limit account access (e.g., to cloud services) to only those who require access for a specified time, to accomplish specific tasks. Periodically review access permissions for all accounts and adjust accordingly.	As employees are hired or third-party vendors are used, establish policies and procedures to grant access only to systems and information that they need to do their jobs. Remove access to sensitive assets when an employee transitions into another role that no longer requires access. Remove access to all business information, systems, and devices when an employee leaves the company or when a third-party service agreement ends.
Change default manufacturer passwords. PR.AA-01	Many devices (e.g., routers, printers, IoT devices) come with default administrative passwords that are easily found or known by criminals and can be used to access the device.	Review the security settings on all devices to ensure that unique, strong passwords are created. Create an asset inventory to document devices whose manufacturer passwords have been updated (see Appendix J).	Establish and regularly review policies and procedures for onboarding and managing devices to ensure that default passwords are changed and managed securely.
Regularly update and patch software and operating systems. PR.PS-02	Unpatched or outdated software can introduce vulnerabilities that attackers can exploit to gain access to information.	Install updates and patches for all assets in the asset inventory. Enabling automatic updates can help manage updates. Make a habit of routinely checking for available updates at least monthly. Check with vendors or manufacturers to identify end-of-life software and devices; remove unsupported systems and replace devices or services that no longer receive security updates.	Growing businesses can utilize an automated patch management system to help identify, prioritize, acquire, install, and verify the installation of patches, updates, and upgrades to systems and devices.
Recognize common attacks and perform basic cyber hygiene tasks. PR.AT-01/02	Awareness training equips business owners with the knowledge and skills to perform general tasks with cybersecurity risks in mind.	Take security awareness training at least once a year. Many organizations regularly provide free or low-cost cybersecurity training. Find educational resources on the NIST Small Business Cybersecurity Corner.	Create a culture of cybersecurity through regular, effective employee training on information security policies, cyber hygiene practices, and how to recognize and report suspicious activity.

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Regularly back up data. Establish measures to protect and test backups. PR.DS-11	Backups enable the restoration of data in case of hardware or software failures or system compromise.	Regularly back up information. Consider having multiple data backups with at least one on a medium that is not connected to the device (e.g., on an external hard drive or in the cloud). Periodic testing can provide confidence that the backups will restore data when needed. View CISA's recommendations. Research the backup policies or services of your cloud providers.	As more devices and systems are added, consider using centralized solutions to conduct and manage backups and identify who within the organization is responsible for backing up data.
Enable multi-factor authentication (MFA) on all accounts that offer it and consider using password managers to generate and protect strong, unique passwords. PR.AA-03	Passwords alone are not effective for protecting data from most attackers, as passwords have become too easy for threat actors to exploit at scale and with limited effort.	Review all account settings to enable MFA, especially phishing-resistant MFA, on all points of access and for all users (learn more about MFA in the box below). This is especially critical for any sensitive or privileged accounts, including those that access backed-up data. With so many passwords to keep track of, a common and relatively inexpensive approach is using a password manager to create and maintain unique, strong passwords.	If third parties or employees are granted system access, require MFA to be enabled and used on all accounts that offer it. To streamline access, consider implementing Single Sign-On (SSO) technologies. These technologies allow users to access multiple applications, tools, and systems with just one set of credentials.

Multi-Factor Authentication (MFA)

MFA is an important security enhancement that requires a user to verify their identity by providing **more than just a username and password.** If a password is compromised, MFA creates a second barrier that makes it much harder for the threat actor to access business systems and data. It requires a user to provide a combination of two or more of the following:

- Something you know (e.g., password, PIN)
- Something you have (e.g., smart card, security key)
- Something you are (e.g., fingerprint, face)

Enabling MFA on all accounts that offer it **is one of the most important steps one can take to protect their business from cybersecurity risks.** Some forms of MFA are more secure than others, as some forms of MFA can be susceptible to phishing threats. Common **phishing-resistant authenticators** that are widely available today can take the form of something called a passkey, which works on specific websites and allows users to authenticate in combination with another factor (e.g., fingerprint, PIN) without requiring a username and password. Learn more about MFA.

There are many cybersecurity risks facing businesses of all sizes, but two common threats are phishing and ransomware. The next two pages provide an overview of each.

3.3.1. Protect Your Business from Phishing

Phishing is a type of scam that uses convincing emails or other messages (e.g., texts, social media messages) to trick people into opening harmful links or downloading malicious software. This is often how ransomware is delivered to organizations and is one of the biggest threats to a business. Training on how to identify and report phishing coupled with enabling phishing-resistant MFA can significantly reduce the chances of a business falling victim to this common threat. Super Intelligence (SI) can now be used to craft increasingly convincing phishing attacks, so it is more imperative than ever to take a second or third look at any message that asks you to take action (e.g., click a link, download a file, transfer funds, log into an account, submit sensitive information).

Tips for Spotting a Phish

- Treat all attachments and links with caution.
- Criminals want individuals to act quickly. **Stop and take a moment to think about the request, even if it looks legitimate.** Verify the request by using known or public contact information, not the message itself. If it is an urgent message from a known individual or entity, contact them directly through trusted, known contact information to verify the message.
- Look at the source email address to verify legitimacy (e.g., a bank emailing you from a commercially or publicly available mail service account instead of a legitimate company email account).
- Verify that requests to divulge or change sensitive information (e.g., new routing numbers, invoice changes, urgent payment requests, gift card requests, account changes) are legitimate by confirming with a trusted source before acting.

Additional Phishing Resources

- NIST Small Business Cybersecurity Corner Phishing Resources
- NIST Human-Centered Cybersecurity Phishing Resources
- How do I create a good password—and what else can I do to secure my online accounts?
- Recognize and Report Phishing
- Mobile Device Best Practices
- Best Practices for Securing Your Home Network

3.3.2. Protect Your Business from Ransomware

Ransomware is a type of malicious attack in which criminals encrypt an organization's data and demand payment to restore access. A ransomware attack is tremendously disruptive to a small business. The risk extends beyond local files and networks to cloud-based accounts and SaaS.

Basic preventive steps to protect against and recover from ransomware threats include (adapted from [13]):

- Do not open files or click on links from unknown sources before first running an antivirus scan or inspecting the link carefully.
- Use standard user accounts with MFA versus accounts with administrative privileges whenever possible.
- Run scheduled checks to identify available software updates and install them as soon as feasible.
- Configure operating systems and/or third-party software to only run authorized applications.
- Use malware detection software (e.g., antivirus software) at all times. Set it to frequently update its definitions and automatically scan email attachments and removable drives.
- Introduce authentication delays or configure automatic account lockout as a defense against automated attempts to guess passwords.
- Use products or services that block access to server names, IP addresses, ports, and protocols that are known to be malicious or suspected to be indicators of malicious system activity. This includes using products and services that provide integrity protection for the domain component of addresses (e.g., hacker@poser.com).
- Carefully plan, implement, and test a data backup and restoration strategy. Secure and isolate backups of important data.
- Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.
- Cyber insurance, especially for small and medium-sized businesses, may help alleviate the financial pressure of a ransomware event, helping to keep organizations operational during response and recovery.

Additional Ransomware Resources

- NIST's Small Business Cybersecurity Corner Ransomware Resources
- CISA's Ransomware Response Checklist

3.4. Detect Function (DE)

The Detect Function provides outcomes that help find and analyze possible cybersecurity attacks and compromises.

Table 8. Detect

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Continuously monitor assets to find indicators of attacks or compromises. DE.CM	The ability to identify common indicators of a cybersecurity incident enables individuals to quickly take action to minimize disruption to the business.	Installing and maintaining security software (e.g., antivirus) is a good first step in detecting incidents. Enable logging to identify suspicious activity if the capability is available. Logs can be a helpful tool during an incident investigation. Other examples include enabling new login attempt notifications for accounts, banking and payment transaction alerts, tracking modifications to domain records, and password reset notifications.	Detection capabilities can be enhanced and automated. Depending on the specific operating systems and resources, one might consider using intrusion detection and prevention systems, configuring technology to audit and alert on certain events, engaging a service provider to monitor computers and networks, or using an all-in-one endpoint security product.
Assess the physical environment for signs of tampering or suspicious activity. DE.CM-02	Cybersecurity is not only confined to the internet, but has a physical component as well (e.g., someone breaks into a home, office, or vehicle and steals a device that has sensitive information on it).	Assess physical office space and implement tactics that will reduce the chances of unauthorized individuals having physical access to assets (e.g., locking filing cabinets, securely storing devices, enabling automatic screen locks). Understand the unique physical threats that might come with each location where work is done (e.g., home, café, co-workspace). Device tracking and remote wipe capabilities should be enabled on devices.	Advanced physical access control mechanisms (e.g., biometric authentication, access cards) can improve control and monitor access. Surveillance equipment can also be installed, or one can choose an office that has a security guard who screens guests.

For a Deeper Dive, Explore Additional Detect Function Technical Resources

- Detecting a Potential Intrusion

3.5. Respond Function (RS)

The Respond Function supports the ability to take action regarding a detected cybersecurity incident.

Table 9. Respond

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Execute the incident response plan in coordination with relevant third parties. **RS.MA-01**	Implementing a prepared cybersecurity incident response plan will help minimize the impact of an incident (see Appendix I).	Thoroughly document the incident. This includes a description of the incident (including when it was first detected), security logs, any relevant screenshots, and what actions have been taken, if any. Reach out to the experts listed in the cybersecurity incident response plan (see Appendix I). Identify business continuity options during an incident (e.g., manual workarounds, temporary service delivery methods, backup communication channels).	If the business grows to have multiple internal functional areas (e.g., human resources, IT, communications), include individuals from across the business as well as external stakeholders when executing the response plan. Conduct tabletop exercises to test the incident response plan.
Communicate with internal and external stakeholders on response activities, as required by laws, regulations, or policies. **RS.CO**	There may be a legal, regulatory, or contractual responsibility to communicate certain details of a confirmed incident with relevant stakeholders. There may also be specific time frames that, if not followed, could introduce additional business risks.	Refer to the incident response plan to identify the responsibilities for communicating a confirmed cybersecurity incident with business stakeholders, as required by laws, regulations, contracts, or policies (see Appendix I).	Effective response communications can become more complicated as the business grows. Organizations with more resources will often consult crisis communications professionals to help craft appropriate internal and external messaging.
Contain incidents. **RS.MI-01**	Taking steps to prevent expansion of a cybersecurity event can help to reduce its overall impact.	Basic steps could include disconnecting devices from the network, isolating affected devices or systems, avoiding using suspected or compromised devices and accounts for recovery actions, and revoking sessions. Antivirus software can also be configured to automatically perform containment actions. Allowing a third party (e.g., internet service provider, managed security service provider) to perform containment actions on behalf of the business can help prevent the expansion of an event and mitigate its effects on the business.	As more devices and accounts are used in the business and as employees and third-party vendors are added, incident containment can become more complicated. The business may consider exploring endpoint detection and response technologies or other automated containment capabilities.

3.6. Recover Function (RC)

The Recover Function involves activities to help restore assets and operations that were impacted by a cybersecurity incident.

Table 10. Recover

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Execute the recovery portion of the incident response plan. RC.RP.01	Recovery activities are focused on returning the business to normal operations.	Verify the integrity of any backups and other assets before putting them back into use so that the chances of reinfecting the system are minimized. Review account details (e.g., MFA settings, user accounts, file sharing settings, active sessions, forwarding rules) before putting them back into use.	When there are multiple functional areas (e.g., human resources, cybersecurity, communications), include individuals from across the business to execute the recovery plan alongside any external stakeholders.
Coordinate restoration activities with internal and external parties. RC.CO	Regular communication with internal and external parties is critical for effective recovery. There might also be legal or contractual responsibilities to communicate with the public or designated stakeholders.	This might involve formal customer or business partner notifications. Consider seeking input from legal counsel prior to distributing communications.	Recovery communications can become more complicated as the business grows. Consider seeking assistance from a crisis communications resource.
Document lessons learned from the incident. RC.RP-06	Documenting lessons learned can provide business leaders with insights on how to minimize the chances of a cybersecurity incident in the future.	Prepare an after-action report that documents the incident, the response and recovery actions taken, and any lessons learned.	As recovery concludes, impacts will be felt across the business. Clear and respectful conversations should continue across all parts of the organization after the event to capture insights and lessons learned.

For a Deeper Dive, Explore Additional Respond and Recover Function Technical Resources

- Cyber Readiness Institute Incident Response Plan Template
- Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile
- FBI's Internet Crime Complaint Center
- Backup and Recover Resources
- NIST Incident Response Preparation Resources Page

3.7. Conclusion

When considered together, the six CSF Functions (i.e., Govern, Identify, Protect, Detect, Respond, and Recover) provide a comprehensive and strategic approach to managing cybersecurity risks. The activities listed for each Function within this guide offer a good starting point for creating a basic cybersecurity risk management strategy for a small non-employer business. As the business grows and adds complexity, the cybersecurity risk management strategy will need to be revised to reflect changes in the risk landscape or environment. To access more NIST small business resources, visit the NIST Small Business Cybersecurity Corner.

References

[1] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[2] U.S. Small Business Administration (2019), A Look at Nonemployer Businesses. (U.S. Small Business Administration Office of Advocacy. https://advocacy.sba.gov/wp-content/uploads/2019/06/A-Look-at-Nonemployer-Businesses.pdf

[3] U.S. Small Business Administration (2024), Frequently Asked Questions About Small Business, July 2024 (U.S. Small Business Administration Office of Advocacy. https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf

[4] Quinn SD, Chua J, Ivy N, Gardner RK, Kent KA, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8286r1. https://doi.org/10.6028/NIST.IR.8286r1

[5] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[6] Fisher W, Craft RE, Ekstrom M, Sexton J, Sweetnam J (2024) Data Confidentiality: Identifying and Protecting Assets Against Data Breaches. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1800-28. https://doi.org/10.6028/NIST.SP.1800-28

[7] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[8] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60v1r1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[9] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 199. https://doi.org/10.6028/NIST.FIPS.199

[10] Nelson A, Rekhi S, Souppaya M, Scarfone KA (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

[11] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[12] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National

Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60v2r1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[13] Souppaya MP, Barker WC, Fisher W, Kent KA (2026) Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8374r1. https://doi.org/10.6028/NIST.IR.8374r1

[14] National Institute of Standards and Technology (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0) (National Institute of Standards and Technology, Gaithersburg, MD), NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

[15] National Institute of Standards and Technology (2024) NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1300. https://doi.org/10.6028/NIST.SP.1300

Appendix A. Glossary

application
A software program hosted by an information system.

assets
An item of value to stakeholders. An asset may be tangible (e.g., hardware, firmware, computing platform, network device) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns. [SP 800-160v2r1]

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [FIPS 200]

availability
Ensuring timely and reliable access to and use of information.

backup
A copy of files and programs made to facilitate recovery.

confidentiality
Protecting information from unauthorized access and disclosure.

cyber resiliency
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. [SP 800-161v2r1]

cybersecurity risk
An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. [6][7, adapted]

integrity
Protecting information from unauthorized modification.

least privilege
The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [CNSSI-4009]

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [SP 800-171Ar3]

threat
Any circumstance or event with the potential to adversely impact organizational operations (a negative risk). [IR 8286]

vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [CNSSI-4009]

vulnerability assessment
Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [CNSSI 4009-2015]

Appendix B. Acronyms

ERM
Enterprise Risk Management

FBI
Federal Bureau of Investigation

CSF
Cybersecurity Framework

CSRM
Cybersecurity Risk Management

CISA
Cybersecurity and Infrastructure Security Agency

HIPAA
Health Insurance Portability and Accountability Act

IAM
Identity and Access Management

ISAC
Information Sharing and Analysis Center

IT
Information Technology

MEP
Manufacturing Extension Partnership

MFA
Multi-Factor Authentication

NIST
National Institute of Standards and Technology

NIST IR
National Institute of Standards and Technology Interagency or Internal Report

PCI DSS
Payment Card Industry Data Security Standard

SBA
U.S. Small Business Administration

SBDC
Small Business Development Center

SMB
Small to Medium-Sized Business

SSO
Single Sign-On

Appendix C. Change Log

Cybersecurity White Paper (CSWP) 50 was initially published in 2009 as NIST IR 7621, *Small Business Information Security*: *The Fundamentals*, and revised in 2016 (NIST IR 7621r1). A pre-draft call for comments was issued in 2024, followed by an initial public draft and comment period on NIST IR 7621r2. During the revision process, the publication was converted to CSWP 50, *Small Business Cybersecurity: Non-Employer Firms.* The previous versions of this publication discussed the broader topic of information security. This version is focused specifically on cybersecurity, which is a subset of information security. Based on community input, the audience was also narrowed. Prior versions focused on "small businesses," which is a very broad and diverse population. This revision is tailored to a specific population — non-employer firms [2] with minimal IT complexity. The information is also now presented in tabular format to enhance readability.

Changes from NIST IR 7621r1 (Revision 1) to CSWP 50 include:

- Changed publication identifier from NIST IR to CSWP
- Updated title
- Specified the audience to focus on single owner and operator businesses with no employees and minimal IT infrastructure
- Narrowed scope from information security to cybersecurity
- Added three new use cases
- Added ransomware, MFA, and phishing explanatory text
- Updated and reduced introductory content
- Simplified language and concepts
- Primary content moved into tables for ease of reading
- Updated content to align with the CSF 2.0
- Eliminated Section 4, "Working Safely and Securely," and moved content into appropriate CSF Function discussions
- Combined Section 1, "Background," and Section 2, "Understanding and Managing Your Risks"
- Moved most appendices into new, separate documents to reduce primary document length

Appendices D-J (Separate File)

All appendices are provided in a separate .XLS document. Each appendix is labeled within the spreadsheet tabs. The document can be accessed under the "Supplemental Material" section of the CSRC publication record.

Appendix D. Notional CSF Outcomes Scenario: Lawyer

Appendix E. Notional CSF Outcomes Scenario: E-Commerce Seller

Appendix F. Notional CSF Outcomes Scenario: Business Consultant

Appendix G. Document and Track All Legal, Regulatory, and Contractual Cybersecurity Requirements

Appendix H. Calculating, Documenting, Categorizing, and Prioritizing Cybersecurity Assets and Risks Worksheet

Appendix I. Respond and Recover Worksheet

Appendix J. Authentication Worksheet

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2026-10-07
Supersedes NIST IR 7621 Revision 1 (November 2016) https://doi.org/10.6028/NIST.IR.7621r1

How to Cite this NIST Technical Series Publication:
Eliot D, Marron JA, Thorn S (2026) Small Business Cybersecurity: Non-Employer Firms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 50 . https://doi.org/10.6028/NIST.CSWP.50

Author ORCID iDs
Daniel Eliot: 0009-0006-3078-555X
Jeffrey A. Marron: 0000-0002-7871-683X
Savann Thorn: 0009-0003-1204-7682

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).