NIST Cybersecurity White Paper
NIST CSWP 50 ipd

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

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

April 14, 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 will also be useful to businesses with very few employees or with minimal IT infrastructure. The goal is to introduce 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, also making 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—termed "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 as they grow and hire employees—acknowledging that some non-employer firms may never hire additional employees. Many small businesses rely upon 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.

Supplemental Content

NIST will continue to create additional resources to help small businesses protect their businesses from cybersecurity risks. All resources are made publicly available on the NIST Small Business Cybersecurity Corner website at https://www.nist.gov/itl/smallbusinesscyber. Suggestions for additional resources to reference on the NIST Small Business Cybersecurity Corner website can always be shared with NIST at smallbizsecurity@nist.gov.

Acknowledgments

The authors acknowledge the thorough and dedicated work 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.

Table of Contents

List of Tables

List of Figures

Executive Summary

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 and include sole proprietors, freelancers, single-member Limited Liability Companies (LLCs), independent contractors, gig economy workers, and others.

As many small businesses have become more reliant upon data and technology to operate and scale a modern business, 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 be devastating to a small business and can negatively impact 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 the business' development creates a foundation from which to build a resilient business in the face of ever-increasing cybersecurity risks. No business - of any size - can prevent every cybersecurity incident from occurring. But it can take steps to implement a cybersecurity plan that will enhance security while achieving business objectives.

"No business - of any size - can prevent every cybersecurity incident from occurring. But it can take steps to implement a cybersecurity plan that will enhance security while delivering business objectives."

Publication Background and Updates

Cybersecurity White Paper (CSWP) 50 was initially published in 2009 as NIST IR 7621, *Small Business Information Security*: *The Fundamentals*. The publication underwent an initial revision in 2016 (NIST IR 7621, Rev.1). A pre-draft call for comments was issued in 2024, followed by an initial public draft and comment period on NIST IR 7621, Rev. 2. During the revision process, the publication was converted to CSWP 50, *Small Business Cybersecurity: Non-Employer Firms.* One of the most significant changes to this revision is its narrowed scope. The previous versions of this publication discussed the broader topic of information security. To simplify and focus the content, this revised publication is now focused specifically on cybersecurity, which is a subset of information security. Based on community input, the audience has also been narrowed. Prior versions focused on "small business," which is a very broad and diverse population. This revision is tailored to a more specific population—non-employer firms [2] with minimal information technology (IT) complexity. Subsequent publications within this series may address other business populations. This version also reflects changes in technology and recent updates to NIST publications, including the Cybersecurity Framework (CSF) 2.0. The information is also now presented in tabular format to enhance readability.

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) as a foundation from which to address cybersecurity for a specific audience—non-employer firms. It provides significantly more detail than the SMB QSG and brings in additional NIST publications as reference material to connect and demonstrate important concepts through graphics, tables, and appendices.

1. Introduction

This publication specifically addresses cybersecurity basics for non-employer firms (no paid employees other than the owners of the business) with minimal IT complexity, helping them to use the NIST Cybersecurity Framework 2.0 [1] to begin managing their cybersecurity risks. Small businesses can implement many of these actions on their own with limited technical knowledge or with minimal financial investment. To make this information applicable to a broader audience, cybersecurity risk management considerations are included for businesses as they grow. This publication 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.

Foundational Goals of Cybersecurity

Businesses of all sizes are increasing their reliance on technology and digitally created, stored, processed, and communicated information. At the same time, criminals are increasing their capabilities to attack these technologies and information. Consequently, cybersecurity risk must be addressed alongside other business risks (e.g., environmental, legal, financial, reputational), even for the smallest of businesses.

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

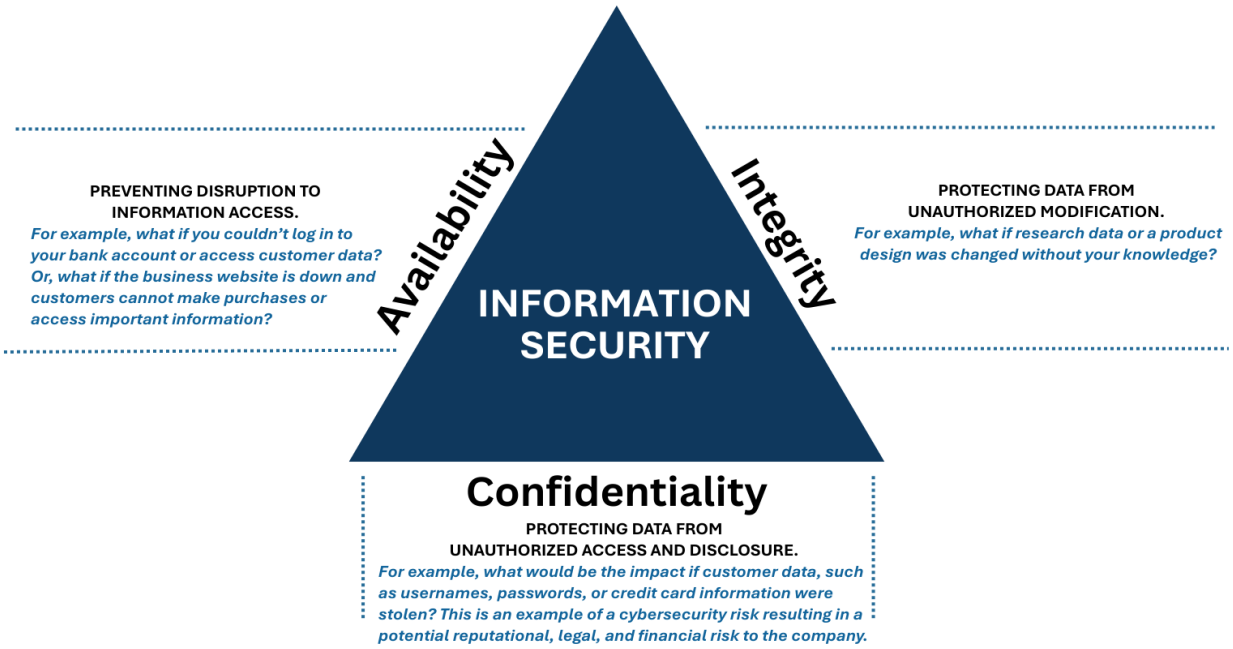


Figure 1: CIA Triad

[1] It is recognized that in some industries "safety" is also added to the "confidentiality, integrity, and availability" triad—especially those in industrial control systems or operational technology environments.

So where can you get started? Begin by understanding the business' context and high value assets.

Understanding Business Context: A good first step for business owners to begin managing cybersecurity risks is to understand the internal and external environment in which the business operates:

1. **External context** involves the expectations of outside stakeholders that affect and are affected by the non-employer firms, such as clients, suppliers, regulators, legislators, and third-party providers (such as e-commerce or payment processors). These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored.

2. **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 the adopted security practices (e.g., password management, data backups, or use of secure platforms and software).

Understanding High Value 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 document high-value assets that the business is dependent upon, evaluate how important they are to the business, identify potential risks to those assets, and take steps to protect them. In addition to the business' own assets, it will also likely handle digital assets of customers or partners and might sign contracts dictating specific data handling requirements and auditing processes (see business context section above). This is why 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, is such an important preliminary step. It is also important, whenever possible, to minimize the commingling of personal and business assets to keep a clear division between personal devices and business-related devices. At this stage, consider using a simple inventory like in Table 1 to get started (see Appendix G):

Table 1: Getting Started with a Basic Asset Inventory

Software or hardware name, serial number, service ID, or other identifying asset information	Asset Owner	High-value data received, processed, stored, or transmitted by this asset	Location (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)

To accompany the asset inventory, a simple network diagram helps to illustrate critical assets and how (and what) data flows between them. Figure 2 shows a graphic depicting a sample architecture for a fictional small, non-employer firm.

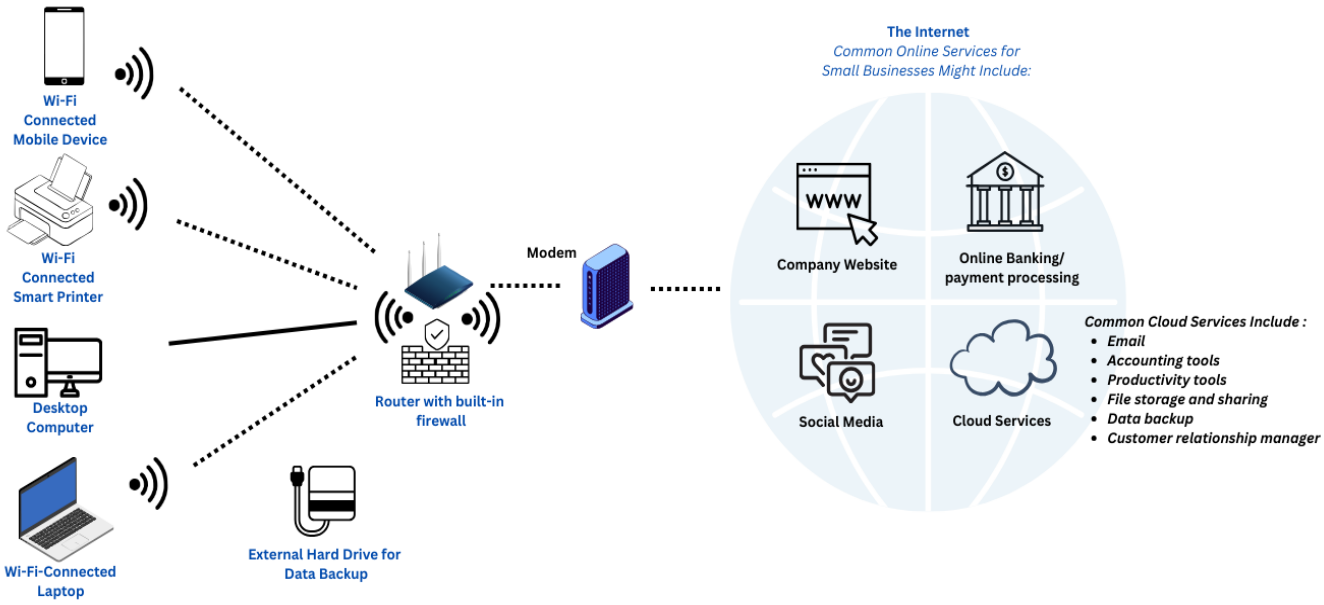


Figure 2: Notional Architecture for Non-Employer Firm

The firm might have a stationary desktop computer in the office (whether that is at home or somewhere else), a Wi-Fi enabled printer, and a laptop and phone that serve as mobile devices for connecting to the internet to access the business' necessary data and systems—whether that's the company website, online banking, social media, or cloud services that the business depends upon to extend their capabilities and operate more efficiently. The firm might also have an external hard drive that is used as one of their methods of backing up data. Though the number of assets in this diagram is limited, and will vary depending upon 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.

All businesses have cybersecurity risk. The overall impact of a cybersecurity incident could include:

- Inability to operate
- Regulatory fines and penalties or legal fees
- Decreased productivity
- Loss of business-critical information

- Adverse impact to reputation, including loss of trust from customers, employees, or business partners
- Damage to credit and inability to get loans from banks
- Loss of business income

Managing cybersecurity risks well 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' 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—demonstrated by taking their cybersecurity seriously

- 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 possible—and necessary—to implement a program that balances security with the broader needs and capabilities of the business.

Cybersecurity requires continuous improvement.

Many business leaders strive for continuous improvement in the business—growing revenues, gaining more market share, expanding the product offering, operating more efficiently, etc. Cybersecurity risk management also requires continuous improvement. As the business grows or changes, as technologies and threats change, as the business adopts new or emerging

Below are a few best practices that significantly reduce cybersecurity risks:

- ✓ Enable phishing-resistant **multi-factor authentication** on all accounts that offer it.
- ✓ Use **strong and unique passphrases.** A passphrase is similar to a password but is generally longer—in the form of a sequence of words or other text. Length has been found to be a primary factor in password strength [11].
- ✓ Learn how to **recognize phishing attempts.**
- ✓ Regularly **back up data**.
- ✓ Maintain **updated software** on all devices and applications.

These practices are expanded upon later in the document.

technologies (such as artificial intelligence), as employees or service providers change, and as legal and regulatory requirements change, leaders must revisit and update the business' cybersecurity risk management strategy to evaluate cybersecurity risks and how they might impact the ultimate mission and goals of the business.

Recognize when help is needed.

No one is an expert in every business and technical area. Many small businesses outsource tax, intellectual property, or contractual work to accountants or lawyers. These are complex topics that require specialized training. Cybersecurity is much the same. It is common for businesses of all sizes to outsource their cybersecurity needs to companies that specialize in these services. Here are a few considerations to be mindful of:

- It is important to start with a clear list of cybersecurity outcomes to achieve with the service—such as meeting specific cybersecurity requirements or goals.
- Read online reviews to see what the experience of other customers has been and to make sure that the provider can support the business needs. Once options are narrowed, request quotes from multiple vendors. Make sure to not only focus on the cost—the quotes should help you learn about their experience working within the industry and supporting small businesses, as well as provide information about how they can help meet any specific legal, regulatory, or contractual requirements.
- 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.
- **Related Resource:** Building Your Small Business' Cybersecurity Team: From In-House to Outsourcing

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. 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 without that data having been breached or compromised through a security

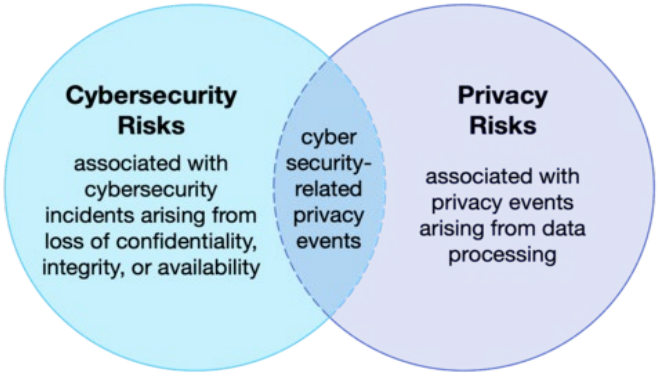


Figure 3: Cybersecurity and Privacy Risk Relationship

incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods, beyond the need for which the information was initially collected [6].

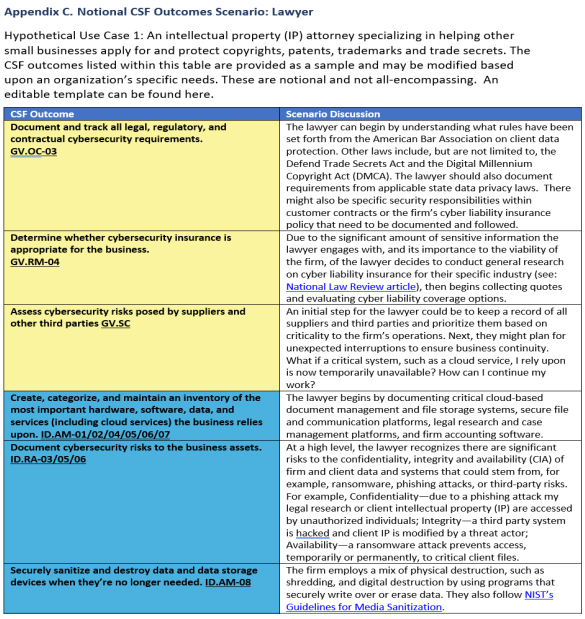
Related Resources:

- Getting Started with the NIST Privacy Framework: A Guide for Small and Medium-Sized Businesses.
- International Association of Privacy Professionals (IAPP) U.S. State Privacy Legislation Tracker.
- United Nations Trade and Development Data Protection and Privacy Legislation Worldwide.

Hypothetical Use Cases

Three hypothetical use cases are provided within the appendices to provide a contextualized discussion. The hypothetical use cases are not intended to be comprehensive for the chosen industry or cover every CSF 2.0 category or subcategory that an organization may select as they build out their cybersecurity risk management strategy. As shown in Fig. 4, they attempt to illustrate an example of how the outcomes within each scenario can be achieved. It is important to note that there are many other ways the outcomes can be achieved beyond these notional examples.

- Hypothetical Use Case 1: An intellectual property (IP) attorney specializing in 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 at their home workshop.
- Hypothetical Use Case 3: A marketing and sales consultant who works with clients large and small around the world, helping them with branding and product go-to-market strategies.



Appendix C. Notional CSF Outcomes Scenario: Lawyer

Hypothetical Use Case 1: An intellectual property (IP) attorney specializing in helping other small businesses apply for and protect copyrights, patents, trademarks and trade secrets. The CSF outcomes listed within this table are provided as a sample and may be modified based upon an organization's specific needs. These are notional and not all-encompassing. An editable template can be found here.

CSF Outcome	Scenario Discussion
Document and track all legal, regulatory, and contractual cybersecurity requirements. GV.OC-03	The lawyer can begin by understanding what rules have been set forth from the American Bar Association on client data protection. Other laws include, but are not limited to, the Defend Trade Secrets Act and the Digital Millennium Copyright Act (DMCA). The lawyer should also document requirements from applicable state data privacy laws. There might also be specific security responsibilities within customer contracts or the firm's cyber liability insurance policy that need to be documented and followed.
Determine whether cybersecurity insurance is appropriate for the business. GV.RM-04	Due to the significant amount of sensitive information the lawyer engages with, and its importance to the viability of the firm, of the lawyer decides to conduct general research on cyber liability insurance for their specific industry (see: National Law Review article), then begins collecting quotes and evaluating cyber liability coverage options.
Assess cybersecurity risks posed by suppliers and other third parties GV.SC	An initial step for the lawyer could be to keep a record of all suppliers and third parties and prioritize them based on criticality to the firm's operations. Next, they might plan for unexpected interruptions to ensure business continuity. What if a critical system, such as a cloud service, I rely upon is now temporarily unavailable? How can I continue my work?
Create, categorize, and maintain an inventory of the most important hardware, software, data, and services (including cloud services) the business relies upon. ID.AM-01/02/04/05/06/07	The lawyer begins by documenting critical cloud-based document management and file storage systems, secure file and communication platforms, legal research and case management platforms, and firm accounting software.
Document cybersecurity risks to the business assets. ID.RA-03/05/06	At a high level, the lawyer recognizes there are significant risks to the confidentiality, integrity and availability (CIA) of firm and client data and systems that could stem from, for example, ransomware, phishing attacks, or third-party risks. For example, Confidentiality—due to a phishing attack my legal research or client intellectual property (IP) are accessed by unauthorized individuals; Integrity—a third party system is hacked and client IP is modified by a threat actor; Availability—a ransomware attack prevents access, temporarily or permanently, to critical client files.
Securely sanitize and destroy data and data storage devices when they're no longer needed. ID.AM-08	The firm employs a mix of physical destruction, such as shredding, and digital destruction by using programs that securely write over or erase data. They also follow NIST's Guidelines for Media Sanitization.

Figure 4: Notional CSF Outcomes Scenario

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

2. The NIST Cybersecurity Framework

The NIST Cybersecurity Framework 2.0 (CSF 2.0) [1] is a flexible, technology-neutral framework that helps organizations—regardless of size, sector, or maturity—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.

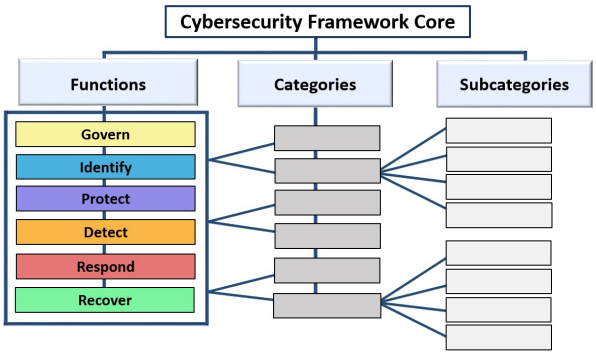


Figure 5: Cybersecurity Framework Core

The CSF Core (Fig. 5) provides high-level cybersecurity outcomes (i.e., a result from taking action) organized into Functions (Table 2), Categories, and Subcategories, that can help any organization manage its cybersecurity risks. These can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise.

The CSF Core can be viewed in its entirety online with the **CSF 2.0 Reference Tool**. This tool enables users to view, sort, and export the full CSF 2.0 into human and machine-readable formats, such as JSON and Excel, to engage with it more dynamically.

A **CSF Organizational Profile** is a strategic exercise to help organizations understand where they currently are (Current Profile) in terms of the CSF outcomes and where they want to be or need to be (Target Profile). Analyzing the differences between the current and target enables an organization to find gaps and develop a prioritized action plan for addressing those gaps. Using Profiles in this manner helps an organization make better-informed decisions about how to improve cybersecurity risk management in a prioritized and cost-effective manner.

Table 2: The Six Functions of the CSF Core

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

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

Learn more about the NIST Cybersecurity Framework: nist.gov/cyberframework.

3. Organization of this document

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 business 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 tables on the following pages are organized into the column headings as shown in Table 3:

Table 3: Organization of Content

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
This column explains **what** action a business might consider taking to reduce cybersecurity risks. The activities are not all encompassing. They are considerations to help establish a cybersecurity risk management strategy and create a strong foundation upon which to build. Citations included 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 to take to reduce or manage cybersecurity risks.	This column provides tips for **how** a business can get started with the action.	This column highlights options for **what's next** as a business adds employees or grows in other ways.

Appendices are 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.

3.1. Govern Function (GV)

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

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[2] depending on which sector it operates in. There may also be contractual requirements (e.g., with customers, business partners) for cybersecurity or privacy risk management.	Create a spreadsheet to document and track all requirements. Appendix F 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	Cyber 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.	Speak to others in the industry and to a trusted insurance agent to understand if cybersecurity insurance is appropriate. Understand if business contracts or agreements require cybersecurity insurance. Understand what potential situations are covered and *not* covered, and what types of data are covered.	Account for any increased complexity (e.g., expanded mission, new business processes, or 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 cybersecurity risks posed by suppliers and other third parties GV.SC	External service providers (cloud platforms, managed IT services, etc.) 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.	Contracts, including purchase orders, can be a primary vehicle a small business has for addressing risk with third parties. 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 these relationships may introduce to the business.

Learn More

- 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

[2] Examples of sources of regulatory requirements include Health Insurance Portability and Accountability Act (HIPAA) and 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.

Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Create, categorize, and maintain an inventory of the most important hardware, software, data, and services (including cloud services) the business relies upon. ID.AM-01/02/04/05/06/07	Inventorying and categorizing data and systems enables business leaders to make informed decisions on what protective measures to take to reduce cybersecurity risks.	Use Appendix G to get started by inventorying the most important hardware, software, data, and services the business relies upon. 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 actually occurs.	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 H.	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're no longer needed. ID.AM-08	Not doing so means potentially handing over sensitive information, like passwords or 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. Using a shredder is also an effective method for destroying data.	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 of 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 evaluations, such as a penetration test. Take insights from these exercises 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.
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 such an event would have to the business.	Use Appendix G to begin documenting cybersecurity risks to the business' most important assets.	Growing businesses can find success in documenting, categorizing and prioritizing cybersecurity risks using a risk register [4].

Elements of Risk (Adapted from [4])

Threat	A ***threat*** is any circumstance or event with the potential to adversely impact organizational operations. These threats might come in the form of personnel or natural events; they can be accidents or intentional. An example of a threat is an employee accidentally submitting login credentials through a phishing scam. Another is an employee accidentally downloading ransomware by clicking on what appeared to be a legitimate link, rendering critical business assets inaccessible.
Vulnerability	A ***vulnerability*** is a condition that enables a threat event to occur. Any time or situation where information is not being adequately protected represents a vulnerability. A common vulnerability is outdated or unpatched software. Vulnerabilities found in software applications are one of the most common avenues of attack for criminals, which is why it is so important to update software when new versions are available.
Likelihood	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. ***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	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability [12].

Learn More

- Guide to Conducting Risk Assessments
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

Resources for Threat Intelligence

Publicly available sources of system security alerts and advisories include:

- The Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- InfraGard
- Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) also often provide security alerts and advisories.

3.3. Protect Function (PR)

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

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 not only to business owners and employees, but also to 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 they have their own unique accounts and cannot access sensitive business data. Limit account access, such as to cloud services, to only those who require access for a specified time, to accomplish specific tasks.	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 job. Remove access to sensitive assets when an employee transitions into another role where access is no longer needed. Remove access to all the business' information, systems, and devices when an employee leaves the company or when a third-party relationship is ended.
Change default manufacturer passwords. PR.AA-01	Many devices, such as Wi-Fi routers, come with default administrative passwords. Default passwords are easily found or known by criminals and can be used to access the device.	Review the security settings on all devices, new and old, to ensure unique, strong passwords are created. Document within an asset inventory which devices have had their manufacturer passwords updated. See Appendix I.	Establish and regularly review policies and procedures for onboarding and managing devices to ensure default passwords are changed and managed securely.
Regularly update and patch software and operating systems. PR.PS-02	Un-patched or outdated software can introduce vulnerabilities that attackers can exploit.	Install updates and patches for all assets in your inventory. Enabling automatic updates will help manage updates. Make a habit of routinely checking for available updates at least monthly.	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, such as Small Business Development Centers. There are also many free online courses. One of the most common attacks is phishing. Learn more about phishing below.	As employees are hired, a critical factor in minimizing cybersecurity risks will be creating a culture of cybersecurity. Part of that is regular, effective employee training on information security policies, cyber hygiene practices, and how to recognize and report suspicious activity.

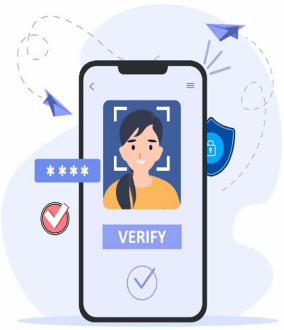
Actions to Consider	Rationale	Getting Started	Considerations as the Business Grows
Regularly back up data. Establish measures to protect and test backups. PR.DS-11	Backups enable restoration of data in case a computer breaks, or a malicious program infects the system.	Configure devices and systems to regularly back up information. Consider having multiple data backups, with at least one on media that is not connected to the computer (such as an external hard drive). Periodic testing can provide confidence that the backups will restore data when needed. View CISA's recommendations.	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, for example, 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 (like a password or PIN)
- ✓ something you have (like a smart card or security key)
- ✓ something you are (like your fingerprint or face)

Enabling MFA on all accounts that offer it **is one of the most important steps one will 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** 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, such as a fingerprint or 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 (explained on the next page) is delivered to organizations and is one of the biggest threats to a business. These messages are often disguised as a trusted source, such as a bank, credit card company, a customer, or trusted advisor.

How to spot a phish

- A request to download an attachment or click on a link—treat all attachments and links with caution.
- A sense of urgency. 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 contact information or information from a public company website, not from the message itself. Or, if it is an urgent message from a known individual or entity, contact them directly through trusted, known contact information to verify the message.
- A suspicious-looking source email address (is the bank emailing you from a "gmail.com" account instead of a legitimate company email account)?
- A request for individuals to divulge or change sensitive information, like bank account numbers, customer information, or Social Security number.

Training on how to identify and report phishing, coupled with enabling phishing-resistant multi-factor authentication (MFA), are steps that will significantly reduce the chances of a business falling victim to this common threat.

Learn More

- NIST Small Business Cybersecurity Corner
- 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 (Cybersecurity and Infrastructure Security Agency)

3.3.2. Protect Your Business from Ransomware

Ransomware is a type of malicious attack where criminals encrypt an organization's data and demand payment to restore access. Imagine trying to log into a particular system or trying to access data and not having access to it anymore. That could be tremendously disruptive to a small business. How long could the business operate without access to critical data or systems? Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public.

Ransomware is typically delivered via email, but it can also be delivered in other ways, such as through social media messages, malicious ads, or text messages. A successful ransomware attack can stop a business in its tracks. **Basic preventive steps to protect against and recover from ransomware threats include, but are not limited to:**

- Don't open files or click on links from unknown sources unless first running an antivirus scan or inspect links carefully.
- Run scheduled checks to identify available patches and install these as soon as feasible.
- Configure operating systems and/or third-party software to run only authorized applications.
- Inform technology vendors of expectations (e.g., in contract language) that they will need to apply measures that discourage ransomware attacks.
- Use malware detection software, such as antivirus software, at all times. Set it to automatically scan emails and flash drives.
- Block access to untrusted web resources. Use products or services that block access to server names, IP addresses, or 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).
- Use standard user accounts with multi-factor authentication versus accounts with administrative privileges whenever possible.
- Back up data, secure backups, and test restoration.
- Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

Bullets adapted from 13.

Learn More

- NIST IR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile
- NIST's Small Business Ransomware Resources
- CISA's Stop Ransomware Guide

3.4. Detect Function (DE)

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

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. These often have the capability of keeping a log to identify suspicious activity. Ensure this functionality is enabled (check the operating instructions for how to do this). Logs can be a helpful tool during an incident investigation.	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 confined to the internet. There is a physical component as well. Imagine if someone broke into a home, office, or vehicle and stole 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., locks on filing cabinets, securely storing devices, and 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).	There are advanced physical access control mechanisms, such as biometric authentication or access cards, to better control and monitor access. Surveillance equipment can also be installed, or one can choose an office that has a security guard who screens guests.

Learn More

- Detecting a Potential Intrusion
- Data Integrity Detecting and Responding to Ransomware and Other Destructive Events

3.5. Respond Function (RS)

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

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 to minimize the impact of the incident.	When an incident is detected, thoroughly document it to share with the incident responder. This includes a description of the incident, when it was first detected, and what actions have been taken, if any. Reach out to those experts who are listed in the cybersecurity incident response plan to seek assistance. See Appendix H, Respond and Recover Worksheet.	When the business grows to the point where there are multiple internal functional areas (e.g., human resources, cybersecurity, communications), include individuals from across the business to execute the response plan alongside any external stakeholders. 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 are situations where there will be a legal, regulatory, or contractual responsibility to communicate certain details of a confirmed incident with relevant stakeholders.	Refer to the incident response plan to identify what the responsibilities are for communicating a confirmed cybersecurity incident with business stakeholders as required by laws, regulations, contracts, or policies. See Appendix H, Respond and Recover Worksheet.	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.

Learn More

- NIST Incident Response Preparation Resources Page
- 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
- Best Practices for Victim Response and Reporting of Cyber Incidents

3.6. Recover Function (RC)

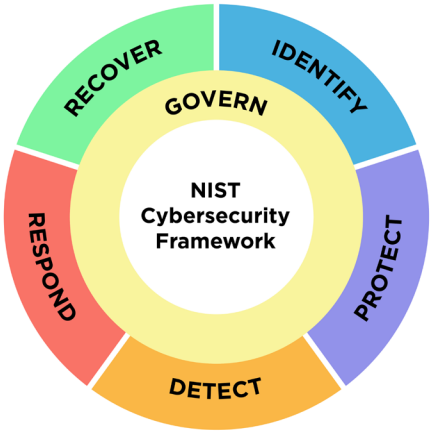
The Recover Function involves activities to help restore assets and operations that were impacted by a cybersecurity incident.

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 getting the business back operational.	Verify the integrity of any backups and other assets before putting them back into use so that chances of re-infecting the system are minimized.	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 an effective recovery. In some instances, there might be legal responsibilities to communicate with the public or designated stakeholders.	Seeking input from legal counsel prior to distributing communications about an incident is encouraged.	Like with response, 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 happening in the future.	Prepare an after-action report that documents the incident, the response and recovery actions taken, and 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.

Learn More

- Guide for Cybersecurity Event Recovery
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

3.7. Conclusion



The six CSF Functions from above (Govern, Identify, Protect, Detect, Respond, and Recover), when considered together, provide a comprehensive and strategic view of managing cybersecurity risk. 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. The activities are not all encompassing. They are considerations to help establish a cybersecurity risk management strategy and create a strong foundation upon which to build. As the business grows and adds employees and additional 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) 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) 800-60, Vol. 1, Rev. 1. 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) 800-61, Rev. 3. 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) 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) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[13] Barker WC, Fisher W, Scarfone KA, Souppaya MP (2022) Ransomware Risk Management: A Cybersecurity Framework Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8374. https://doi.org/10.6028/NIST.IR.8374

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., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or 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.
[NIST SP 800-160 Vol. 2 Rev. 1]

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, if necessary.

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. [NIST 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. (Definition based on ISO Guide 73 [6] and NIST SP 800-60 Vol. 1 Rev. 1 [7])

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. [NIST SP 800-171Ar3 from OMB Circular A-130 (2016)]

Threat
Any circumstance or event with the potential to adversely impact organizational operations (a negative risk). [NIST 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. Notional CSF Outcomes Scenario: Lawyer

Hypothetical Use Case 1: An intellectual property (IP) attorney specializing in helping other small businesses apply for and protect copyrights, patents, trademarks, and trade secrets. The CSF outcomes listed within this table are provided as a sample and may be modified based upon an organization's specific needs. These are notional and not all-encompassing.

CSF Outcome	Scenario Discussion
Document and track all legal, regulatory, and contractual cybersecurity requirements. GV.OC-03	The lawyer begins by understanding what rules have been set forth from the American Bar Association on client data protection. Other laws include, but are not limited to, the Defend Trade Secrets Act and the Digital Millennium Copyright Act (DMCA). The lawyer also documents requirements from applicable state data privacy laws. There might also be specific security responsibilities within customer contracts or the firm's cyber liability insurance policy that need to be documented and followed.
Determine whether cybersecurity insurance is appropriate for the business. GV.RM-04	Due to the significant amount of sensitive information the lawyer engages with, and its importance to the viability of the firm, the lawyer decides to conduct general research on cyber liability insurance for their specific industry (see: National Law Review article), then begins collecting quotes and evaluating cyber liability coverage options.
Assess cybersecurity risks posed by suppliers and other third parties GV.SC	The lawyer keeps a record of all suppliers and third parties and prioritizes them based on criticality to the firm's operations. Next, they plan for unexpected interruptions to ensure business continuity.
Create, categorize, and maintain an inventory of the most important hardware, software, data, and services (including cloud services) the business relies upon. ID.AM-01/02/04/05/06/07	The lawyer begins by documenting critical cloud-based document management and file storage systems, secure file and communication platforms, legal research and case management platforms, and firm accounting software.
Document cybersecurity risks to the business assets. ID.RA-03/05/06	At a high level, the lawyer recognizes there are significant risks to the confidentiality, integrity and availability (CIA) of firm and client data and systems that could stem from, for example, ransomware, phishing attacks, or third-party risks. For example, Confidentiality—due to a phishing attack the legal research or client intellectual property (IP) are accessed by unauthorized individuals; Integrity—a third party system is hacked and client IP is modified by a threat actor; Availability—a ransomware attack prevents access, temporarily or permanently, to critical client files.
Securely sanitize and destroy data and data storage devices when they're no longer needed. ID.AM-08	The firm employs a mix of physical destruction, such as shredding, and digital destruction by using programs that securely write over or erase data. They also follow NIST's Guidelines for Media Sanitization.
Strive for continuous improvement (ID.IM)	At least once a year, the lawyer updates their asset inventory and incident response plan. Regularly, they engage with their managed security service provider (MSSP) to identify areas to strengthen the firm's cybersecurity posture.

CSF Outcome	Scenario Discussion
Create a cybersecurity incident response plan ID.IM-04	They identify who their primary contacts are for incident response, recognizing they are not equipped to respond to an incident all by themselves. This involves a local law enforcement cybercrimes contact, regional FBI field office, insurance agent, and their MSSP. A more thorough plan is developed in collaboration with their MSSP.
Limit access to sensitive assets to only those who require it to perform their job responsibilities. PR.AA-05	They ensure that clients are only able to access their own information within file storage or communication systems. The lawyer does not use privileged admin accounts for day-to-day tasks. They also ensure systems are not accessing more information than what they need by configuring access settings.
Change default manufacturer passwords. PR.AA-01	As the lawyer is conducting an inventory of all the firm's software and hardware, it is recognized the firm's router password was never changed from the manufacturer's password. This is immediately changed to one that is unique to the firm.
Regularly update and patch software and operating systems. PR.PS-02	All the firm's browsers, systems, and applications are set to automatically update. This also includes device software updates and router firmware updates.
Recognize common attacks and perform basic cyber hygiene tasks. PR.AT-01/02	The lawyer periodically takes available cybersecurity training from local business and trade groups and participates in webinars to better understand how to identify common cybersecurity risks.
Regularly back up data. Establish measures to protect and test backups. PR.DS-11	The firm regularly backs up critical data in near-real-time, tests backups at least annually, and securely stores some backups offline and offsite to reduce chances that an incident or disaster will damage them.
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	Phishing-resistant MFA is enabled on all accounts that offer it, including privileged administrative accounts. The lawyer has also purchased a password manager to help them manage all their passwords.
Continuously monitor assets to find indicators of attacks or compromises. DE.CM	The lawyer uses antivirus software but has also engaged an MSSP to help with cybersecurity incident detection, including 24/7 network monitoring to identify potential anomalies and alert the firm to any issues.
Assess the physical environment for signs of tampering or suspicious activity. DE.CM-02	The firm is located in a co-working space. The lawyer regularly assesses the physical environment to ensure no locks or devices have been tampered with. They also lock their door when they leave the office to ensure no unauthorized individuals access the space.
Execute the incident response plan in coordination with relevant third parties. RS.MA-01	The firm is hit with a ransomware attack, locking them out of their system. For this firm, their first call is to their MSSP to engage the incident response plan.
Communicate with internal and external stakeholders on response activities as required by laws, regulations, or policies. RS.CO	The lawyer goes back to their incident response plan and to their documented cybersecurity requirements to understand what their reporting requirements are for cybersecurity incidents. They communicate according to what is dictated within those plans.

CSF Outcome	Scenario Discussion
Execute the recovery portion of the incident response plan. **RC.RP-01**	The response team reviews the incident response plan and begins carrying out recovery actions.
Coordinate restoration activities with internal and external parties. **RC.CO**	The firm and the MSSP, and any other stakeholders included in the incident response, meet regularly to understand roles and authorizations for recovery activities and what their progress is and communicate internally and externally as dictated by policy or statute.
Document lessons learned from the incident. **RC.RP-06**	The firm convenes with the MSSP to discuss the after-action report to understand how to reduce the chance of a similar event happening in the future.

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

Hypothetical Use Case 2: An entrepreneur that sells made-to-order hats on a popular internet storefront. The CSF outcomes listed within this table are provided as a sample and may be modified based upon an organization's specific needs. These are notional and not all-encompassing.

CSF Outcome	Scenario Discussion
Document and track all legal, regulatory, and contractual cybersecurity requirements. GV.OC-03	The entrepreneur keeps all signed documents between stakeholders in an administrative binder. Within the binder is a table of contents with names of the agreement and the dates they were signed. The binder includes all business agreements, which include cybersecurity requirements.
Determine whether cybersecurity insurance is appropriate for the business. GV.RM-04	The entrepreneur considers getting a cyber insurance rider on an existing business insurance plan. They consult with their insurance broker and select an appropriate plan.
Assess cybersecurity risks posed by suppliers and other third parties GV.SC	The entrepreneur documents who their critical suppliers and third parties are and what access they have to the business' systems and data. They also identify critical dependencies and any backup processes if the supplier or third party experiences a cyber attack and is temporarily unavailable.
Create, categorize, and maintain an inventory of the most important hardware, software, data, and services (including cloud services) the business relies upon. ID.AM-01/02/04/05/06/07	The entrepreneur uses the asset inventory worksheet found in Appendix G to document all the most critical assets. This is reviewed once every six months.
Document cybersecurity risks to the business assets. ID.RA-03/05/06	The entrepreneur uses Appendix G to begin documenting key assets and risks to those assets. For instance, a key asset is the online store. Unauthorized access or modification to the store, or the unavailability of the store, could have significant negative impact to the business.
Securely sanitize and destroy data and data storage devices when they're no longer needed. ID.AM-08	The entrepreneur works from various co-working locations and uses USB data storage. They keep a log of the memory devices used, when each is put into service, and when it is decommissioned. They are intentional about completely wiping, destroying the device, and recording when this is completed.
Strive for continuous improvement (ID.IM)	They schedule an hour at least once a month to identify areas where they can strengthen their cybersecurity posture. This includes double-checking security settings, ensuring all software is updated, updating or reviewing contractual agreements, etc.
Create a cybersecurity incident response plan ID.IM-04	Part of the entrepreneur's insurance plan includes templates for an incident response plan. These have to be completed and submitted to the insurance company.
Limit access to sensitive assets to only those who require it to perform their job responsibilities. PR.AA-05	The entrepreneur just got a new laptop that is dedicated to the business and no one else is authorized to use it. Access to the online store's management interface is limited to the entrepreneur.

CSF Outcome	Scenario Discussion
Change default manufacturer passwords. **PR.AA-01**	They document all critical assets in an asset inventory and whether default manufacturer passwords were changed (if that applies to the asset).
Regularly update and patch software and operating systems. **PR.PS-02**	Even though the entrepreneur has configured software to update automatically, they also make it a point to do a regular check to see if critical systems or devices need updates.
Recognize common attacks and perform basic cyber hygiene tasks. **PR.AT-01/02**	As a part of growing the business, the entrepreneur regularly attends conferences. They make it a point to attend the cybersecurity sessions. They also take advantage of cybersecurity tips and modules offered by the vendor of the online marketplace used by the business.
Regularly back up data. Establish measures to protect and test backups. **PR.DS-11**	The entrepreneur decides to use an encrypted backup service. The entrepreneur routinely tests the backup platform to make sure it is working as planned.
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	The entrepreneur selects a password manager to manage all the passwords used for the business. They use the authentication worksheet (Appendix I) to track where they have enabled MFA.
Continuously monitor assets to find indicators of attacks or compromises. **DE.CM**	The entrepreneur does not yet have a managed service provider to help with continuous monitoring. They found a low-cost automated tool that helps with endpoint detection and response.
Assess the physical environment for signs of tampering or suspicious activity. **DE.CM-02**	The business operator keeps all assets under lock and key and is careful about not leaving the laptop unattended when using a co-working space.
Execute the incident response plan in coordination with relevant third parties. **RS.MA-01**	The entrepreneur's online marketplace vendor has been the victim of a denial-of-service attack, making the entrepreneur's online storefront unavailable. They implement the incident response plan they worked on with their insurance representative.
Communicate with internal and external stakeholders on response activities as required by laws, regulations, or policies. **RS.CO**	The entrepreneur contacts customer support of the online marketplace and discusses the incident with the insurance representative. Information is shared between the parties. It is determined that the entrepreneur's storefront was not accessed, and no customer data was exposed.
Execute the recovery portion of the incident response plan. **RC.RP.01**	Once the online marketplace is back online, the entrepreneur does not notice any other signs of storefront compromise. However, they still change all passwords, end all active sessions, and log back into all applications.
Coordinate restoration activities with internal and external parties. **RC.CO**	The marketplace vendor helps ensure the online store is back operational and secure.
Document lessons learned from the incident. **RC.RP-06**	The entrepreneur learns that they had not sufficiently considered how their business would be affected by unavailability of the online marketplace. They have revised their plan to consider alternative means to advertise and sell products if the online marketplace is offline.

Appendix E. Notional CSF Outcomes Scenario: Business Consultant

Hypothetical Use Case 3: A marketing and sales consultant who works with clients large and small around the world, helping them with branding campaigns and product go-to-market strategies. The CSF outcomes listed within this table are provided as a sample and may be modified based upon an organization's specific needs. These are notional and not all-encompassing.

CSF Outcome	Scenario Discussion
Document and track all legal, regulatory, and contractual cybersecurity requirements. **GV.OC-03**	The consultant will have contractual obligations for each client. These contracts will typically specify data-handling requirements, including confidentiality and integrity of client data, as well as non-disclosure agreements. The consultant's clients are from a variety of industry sectors, so they consider relevant industry and sector-specific regulatory requirements.
Determine whether cybersecurity insurance is appropriate for the business. **GV.RM-04**	Because the consultant's business relies on utilizing client marketing and sales data, the consultant acquires insurance to protect the company. The insurance company provides cybersecurity guidance to assist the consultant. Some clients require the consultant to have a cybersecurity insurance policy in place.
Assess cybersecurity risks posed by suppliers and other third parties **GV.SC**	The consultant has a minimal local IT presence in their office and has contracted out IT services to 3rd parties. This includes storing client data primarily in servers owned by a cloud service provider (CSP), although client data may also be stored on the consultant's primary laptop. The consultant utilizes a small office presence with a printer, mobile phone, laptop and router which connects all the consultant's devices to the internet service provider (ISP) which is another third party. The consultant also stores laptop and phone backups to cloud providers.
Create, categorize, and maintain an inventory of the most important hardware, software, data, and services (including cloud services) the business relies upon. **ID.AM-01/02/04/05/06/07**	The consultant creates an inventory of hardware (i.e., laptop, printer, mobile phone, router); software (i.e., client management software on laptop, financial management software, and general word processing and marketing software); data (i.e., client product details and plans, client product financial data; client marketing strategies) which can be stored both locally on the consultant's devices as well as on servers owned and maintained by the contracted CSP; and services (i.e., ISP for internet access, and CSP for data storage, some analytics, and data backup).
Document cybersecurity risks to the business assets. **ID.RA-03/05/06**	Risks that the consultant considers and documents include: • Malware and/or ransomware on personally-owned devices with can render client data unavailable or untrustworthy • Vulnerabilities in software used by the consultant that could compromise their personally-owned devices • Loss of confidentiality of client data which damages customer reputation and/or result in loss of trust in the consultant • Loss of availability of critical services (i.e., internet access and/or cloud data access) which results in the consultant being unable to complete services for customers

CSF Outcome	Scenario Discussion
Securely sanitize and destroy data and data storage devices when they're no longer needed. ID.AM-08	The consultant must carefully outline with each client what their expectations are regarding the consultant's data handling requirements (e.g., how long data should be maintained by the consultant, which data should not be stored on consultant-owned devices or with a CSP, when data should be destroyed, etc.). The consultant accordingly tracks when data should be deleted for each customer and carefully sanitizes laptops and mobile devices when they are no longer used for work.
Strive for continuous improvement (ID.IM)	The consultant takes notes of data handling processes that work or that need improvement and ensures that identified areas of improvement are acted upon. Additionally, they maintain communication with clients to acquire feedback on processes that work, as well as those that may need improvement.
Create a cybersecurity incident response plan ID.IM-04	For each of the identified risks above, the consultant creates plans for how to respond if each risk is realized. This includes considering possible backup service providers (i.e., ISP and CSP) as well as how they would respond to loss of confidentiality, integrity, or availability of client data. These plans include communication plans with clients, technical recovery plans, as well as ways to continue serving client needs while response and recovery efforts are ongoing. The consultant has already reached out to a cybersecurity service provider to establish a relationship in case response and recovery services are needed.
Limit access to sensitive assets to only those who require it to perform their job responsibilities. PR.AA-05	On their end, the consultant is the only person who has access to confidential client data. However, their work is highly collaborative. During client intake meetings and within contract paperwork, it is documented who is authorized to access confidential client work, their level of access, duration of access, and the processes for onboarding and off-boarding access rights.
Change default manufacturer passwords. PR.AA-01	The consultant changes any default passwords on the router used in their office—particularly any default passwords for accounts used to administer the router. The consultant also sets a unique, strong password or passphrase for the Wi-Fi network. Since the router is personally-owned, the consultant disables remote administrative capabilities on the router so that anyone administering the router must be locally connected via ethernet cable.
Regularly update and patch software and operating systems. PR.PS-02	The consultant ensures that automatic updates are enabled for the operating system and applications on both the laptop and mobile phone used for the business. The consultant also periodically checks for outstanding updates available for the laptop, phone, or the applications they use. Additionally, the consultant sets monthly reminders to check for firmware updates for both the printer and router and ensures that any available updates are applied promptly.

CSF Outcome	Scenario Discussion
Recognize common attacks and perform basic cyber hygiene tasks. PR.AT-01/02	The consultant is not an expert in cybersecurity but tries to stay up-to-date with current risks related to ransomware and to technology used to support clients. They maintain awareness of how to set up automatic updates for business devices and to check for firmware updates for printers and routers. The consultant also ensures that they can change default passwords and uses guidelines/checklists from reputable sources to configure and maintain devices used for business. Anti-virus (AV) software and/or endpoint protection software is also installed on the laptop and mobile phone.
Regularly back up data. Establish measures to protect and test backups. PR.DS-11	They ensure that all applicable devices (e.g., laptop and mobile phone) are configured to back up data to the CSP. However, the consultant has noted that testing the ability to restore data from the backups has not been done and is an area of improvement. The consultant is hesitant to test the backups for fear that the restoration may not be successful and that critical customer data stored on the laptop is lost. The consultant has a note to reach out to the CSP for assistance in testing the restoration of data via backups.
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	The consultant uses a reputable password manager to create and maintain strong, unique passwords/passphrases for all software and websites used for work. Additionally, they ensure that MFA (or the strongest authentication available) is configured for the operating system, all software, and each online site used.
Continuously monitor assets to find indicators of attacks or compromises. DE.CM	The consultant relies primarily on antivirus and endpoint protection software to monitor the laptop and mobile phone used for work. Any alerts are quickly acted upon to remediate any incidents. The consultant also monitors the availability of the office router and critical online services to ensure that they can meet clients' needs.
Assess the physical environment for signs of tampering or suspicious activity. DE.CM-02	The consultant primarily works in a dedicated office environment that is not accessible to the public with many physical security controls in place. However, the consultant has noted that improvements can be made in the placement of the router and the Wi-Fi coverage provided by the antennas to limit network spill over into neighboring office space. The consultant has also considered installing privacy filters for the laptop screen to limit what others can see when they are working in public settings.
Execute the incident response plan in coordination with relevant third parties. RS.MA-01	The consultant is prepared to document any cybersecurity incident that occurs. As noted earlier, a relationship is established with a service provider in case response and recovery services are needed. The contact information for the service provider is stored on paper in the office as well as on a device separate from the devices used for work.
Communicate with internal and external stakeholders on response activities as required by laws, regulations, or policies. RS.CO	The consultant is prepared with contact information for each client in case of a cybersecurity incident that affects that client's data. For each client, relevant industry contact information is prepared in case there are legal, regulatory, or other contractual communication obligations that need to be fulfilled. This contract information is also stored physically on paper in the office as well as on a device separate from the devices used for work.

CSF Outcome	Scenario Discussion
Execute the recovery portion of the incident response plan. **RC.RP.01**	While data is being backed up to the CSP, the consultant has identified testing recovery of the data via backups as an area of improvement. As part of that identified area of improvement, the consultant needs to also verify the integrity of data backups before restoring systems from that data. The consultant has reached out to the cybersecurity service provider to determine if they can assist in testing the restoration of data from backups.
Coordinate restoration activities with internal and external parties. **RC.CO**	The consultant is preparing the coordination of restoration plans and activities with the cybersecurity service provider. Additionally, the consultant has had conversations with each client regarding data protection requirements and communication expectations in the event of a cybersecurity incident. The consultant has considered obtaining legal counsel in preparation for any cybersecurity incident.
Document lessons learned from the incident. **RC.RP-06**	As the consultant is prepared to document the details of any cybersecurity incident that occurs, they are prepared to document and implement lessons learned as part of any cybersecurity incident. This would include documenting response and recovery actions taken, communications actions, and perceived areas for improvement.

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

The following appendices (Appendices F to I) are designed to be customizable to business needs.

Completing the information in Table 4 will assist with documenting and tracking cybersecurity requirements. It will likely need to be modified to meet specific needs, but this provides a starting point.

Table 4: Documenting Reporting Requirements

Requirement Body	Individual Requirement to Meet	Status	Deadline	Documentation	Evaluation	Action(s) Needed	Next Review Date
(e.g., HIPAA, PCI DSS)	*(e.g., conducting risk assessments to identify potential vulnerabilities*	*(e.g., in compliance, in progress, out-of-compliance*			*(e.g., self-attest, audit)*		

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

Understanding and Managing Risks

Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the business. Most people make risk-based decisions every day. While driving to work, we assess threats and vulnerabilities such as weather and traffic conditions, the skill of other drivers on the road, and the safety features and reliability of the vehicle we drive.

Elements of Risk (Adapted from [4])

Threat	A ***threat*** is any circumstance or event with the potential to adversely impact organizational operations. These threats might come in the form of personnel or natural events; they can be accidents or intentional. An example of a threat is an employee accidentally submitting login credentials through a phishing scam. Another is an employee accidentally downloading ransomware by clicking on what appeared to be a legitimate link, rendering critical business assets inaccessible.
Vulnerability	A ***vulnerability*** is a condition that enables a threat event to occur. Any time or situation where information is not being adequately protected represents a vulnerability. A common vulnerability is outdated or unpatched software. Vulnerabilities found in software applications are one of the most common avenues of attack for criminals, which is why it is so important to update software when new versions are available.
Likelihood	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. ***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	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability [12].

List the types of information, processes, important people, and technology the business relies upon.

1. In Table 5 (next page), list the assets (e.g., information, people, processes, or technology) that are most important to the business.

Table 5: Getting Started with a Basic Asset Inventory

Software or hardware name, serial number, service ID, or other identifying asset information	Asset Owner	High-value data received, processed, stored, or transmitted by this asset	Location (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)
Cellphone	*Business Owner*	*Date commissioned*	*Mobile*	*Significant*	*Yes*	*Yes*

2. Go through each identified asset type and ask:
    a. What would be the impact to the business if this asset was made public?
    b. What would be the impact to the business if this asset was damaged or inaccurate?
    c. What would be the impact to the business if I or my customers couldn't access this asset?
3. Pick an asset value scale that works best (e.g., low, medium, high, or a numerical range like 1-5).

This sample planning organizer in Table 6 can be used to begin identifying the most important assets, processes, and systems, and then categorize each based on the impact to the business if the confidentiality, availability, or integrity were to become compromised. To learn more, NIST Special Publication 800-60, Vol.1, Rev. 1 [8] provides basic guidelines for mapping types of information and information systems to security categories.

Table 6: Sample Asset Categorization

Asset	Confidentiality Impact (low, moderate, high)	Integrity Impact (low, moderate, high)	Availability Impact (low, moderate, high)	Notes
Intellectual Property	*High*	*High*	*High*	*Critical to business*
E-Commerce Site	*Low*	*Mod*	*High*	*Availability critical*
Customer Relationship Manager	*Med*	*High*	*High*	*Availability critical*
Social Media Account	*Low*	*Mod*	*Low*	*Integrity important*

FIPS Publication 199 [9] defines three levels of potential impact on organizations or individuals should there be a breach of security:

- **Low Impact:** limited adverse effect on organizational operations, assets, or individuals.
- **Moderate Impact:** Serious adverse effect on organizational operations, assets, or individuals.
- **High Impact:** Severe or catastrophic adverse effect on organizational operations, assets or individuals.

Table 7 lists examples of possible threat events and potential risks to the identified assets.

Table 7: Sample Potential Events and Risks to Assets

Asset	Possible Threat Actor/Event	Possible Risks
Intellectual Property	• Ransomware • Malicious insider	• Critical information becomes unavailable • Critical information is stolen or modified
E-Commerce Site	• Denial of service attack on site • Compromise of site due to vulnerability from unpatched software	• E-commerce site is unavailable, impacting sales and revenue generation • E-commerce site is compromised, impacting integrity of business
Customer Relationship Manager	• Third party outage. • Phishing attack	• Customer relationship information becomes unavailable, impacting business • Customer information stolen
Social Media Account	• Malicious attacker	• Social media account is compromised, resulting in loss of integrity and possible damage to business reputation

Appendix H. Respond and Recover Worksheet

Incident response is a critical part of cybersecurity risk management and should be integrated across organizational operations. The six CSF 2.0 Functions play vital roles in incident response [10]:

- Govern, Identify, and Protect help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned from those incidents.
- Detect, Respond, and Recover help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

An adverse cybersecurity incident is "…an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" [7]. Examples include an attacker:

- Using phishing emails to compromise user accounts
- Identifying a vulnerability in network management appliances and exploiting the vulnerability to gain unauthorized access to network communications
- Deploying ransomware to prevent the use of computer systems

Before an incident occurs, be ready with a basic response plan and contact information as shown in Table 8. This will be customized based on the business, but should include:

- ✓ **A business champion**: Someone who is responsible for developing and maintaining the incident response plan.
- ✓ **Who to call:** List all the individuals who are part of the incident response efforts. Include their contact information, responsibilities, and authority.
- ✓ **What/when/how to report:** List the business' communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Table 8: Sample Contact Table

Contact Type	Contact Name	Phone	Email
Business Champion:			
Technical Contact:			
State Police:			
Legal Contact:			
Bank Contact:			

Contact Type	Contact Name	Phone	Email
Insurance Contact:			
Regional FBI Contact *Find an FBI Field Office*			

Coordinate response activities with internal and external stakeholders as required by laws, regulations, or policies.

Incident response reporting and communication activities tend to fall into four categories:

- **Incident coordination** involves communicating current and planned incident response activities for a particular incident among the internal and external parties who have incident response roles and responsibilities.
- **Incident notification** involves formally informing affected customers, employees, partners, regulators, or others about a data breach or other incident.
- **Public communication** involves communicating to the public about the status of a particular incident, such as responding to media inquiries.
- **Incident information sharing** involves sharing cybersecurity threat information with others, usually voluntarily, based on activity observed within the organization's technology assets.

Table 9 can help business owners document their reporting plan and requirements.

Table 9: Sample Reporting Requirements Table

Document the Regulation, Contract, or Law	Document the Reporting Requirement	Document the Reporting Timeframe	Reporting Requirement Contact Information

Appendix I. Authentication Worksheet

Enabling multi-factor authentication (MFA) is one of the best ways to protect data. Start with accounts that can access the most sensitive information. Use the checklists in Table 10 and Table 11 to get started. These lists are not exhaustive and will require you to customize based upon your own environment.

Table 10: Sample MFA Table

Account	MFA Enabled (Yes or No)	Phishing-Resistant MFA Enabled? (Yes or No)
Banking Account(s)		
Accounting and Tax Account(s)		
Merchant Account(s)		
Google, Microsoft, and/or Apple ID Account(s)		
Email Account(s)		
Password Manager(s)		
Website Account(s)		
Customer Relationship Manager Account		
Social Media Sites		

Sample Default Manufacturer Passwords Table

Table 11: Sample Default Manufacturer Passwords Table

Account	Default Password Changed (Yes/No)
Wi-Fi Router	
Smart Device 1	
Smart Device 2	
Security Camera System	
Industrial Control System	
Network-Connected Printer	

Appendix J. Change Log

Changes from NIST IR 7621, Revision 1 to CSWP 50 include:

- Change in publication identifier from NIST IR to CSWP.
- Addition of three new use cases
- Updated title.
- Specified the audience to focus on single owner and operator business with no employees and minimal IT infrastructure.
- Addition of ransomware, MFA, and phishing explanatory text
- Narrowed scope from information security to cybersecurity.
- 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. Addition of three notional use-cases
- Added new appendices.

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 YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication.]

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 ipd (initial public draft). https://doi.org/10.6028/NIST.CSWP.50.ipd

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

Public Comment Period
April 14, 2026 – May 14, 2026

Submit Comments
ir7621-comments@nist.gov

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).