

# Implementation Guide for Small- and Medium-Sized Enterprises

CIS Controls Implementation Group 1

Version 2.0

September 2023

V8

# Acknowledgments

The Center for Internet Security, Inc.® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls® and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

## **Editors**

Joshua M. Franklin, CIS

## **Contributors**

Dave Tchozewski  
Ginger Anderson, CIS  
Robin Regnier, CIS  
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (<https://www.cisecurity.org/controls/>) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS).

# Contents

|                                                                                   |           |
|-----------------------------------------------------------------------------------|-----------|
| Introduction                                                                      | 1         |
| Next Steps                                                                        | 3         |
| Overview                                                                          | 4         |
| <b>Phase 1 Complete the Five Inventory Worksheets</b>                             | <b>5</b>  |
| Know What's Connected to Your Office Network                                      | 6         |
| Know What Software Is on Your Systems                                             | 7         |
| Know the Data You're Trying to Protect                                            | 8         |
| Know Which Service Providers You're Using                                         | 9         |
| Know Which Accounts You're Using                                                  | 10        |
| <b>Phase 2 Complete Your Asset Protection Worksheets</b>                          | <b>11</b> |
| Configure and Protect Your Computers                                              | 12        |
| <b>Phase 3 Complete Your Account Security Worksheets</b>                          | <b>13</b> |
| Protect Your Accounts                                                             | 14        |
| <b>Phase 4 Complete Your Backup and Recovery Worksheet</b>                        | <b>15</b> |
| Create and Manage Your Data Backups                                               | 16        |
| <b>Phase 5 Complete Your Incident Response</b>                                    | <b>17</b> |
| Have an Incident Response Plan in Place Prior to an Attack                        | 18        |
| <b>Phase 6 Complete Your Cyber Education Worksheet</b>                            | <b>19</b> |
| Ensure All Employees Are Trained to Recognize and Prevent Cybersecurity Incidents | 20        |
| <b>Appendix A Cybersecurity Worksheets Summary</b>                                | <b>A1</b> |
| Enterprise Asset Inventory Worksheet                                              | A2        |
| Software Asset Inventory Worksheet                                                | A3        |
| Data Inventory Worksheet                                                          | A4        |
| Service Provider Inventory Worksheet                                              | A5        |
| Account Inventory Worksheet                                                       | A6        |
| Asset Protection Worksheet                                                        | A7        |
| Account Security Worksheet                                                        | A8        |
| Backup and Recovery Worksheet                                                     | A9        |
| Incident Response Worksheet                                                       | A10       |
| Cyber Education Worksheet                                                         | A11       |
| <b>Appendix B Mapping the CIS Controls to This Guide</b>                          | <b>B1</b> |
| <b>Appendix C Helpful Resources</b>                                               | <b>C1</b> |

## Additional Resources

A spreadsheet can be downloaded [here](#) for users to use in lieu of provided worksheets.

# Introduction

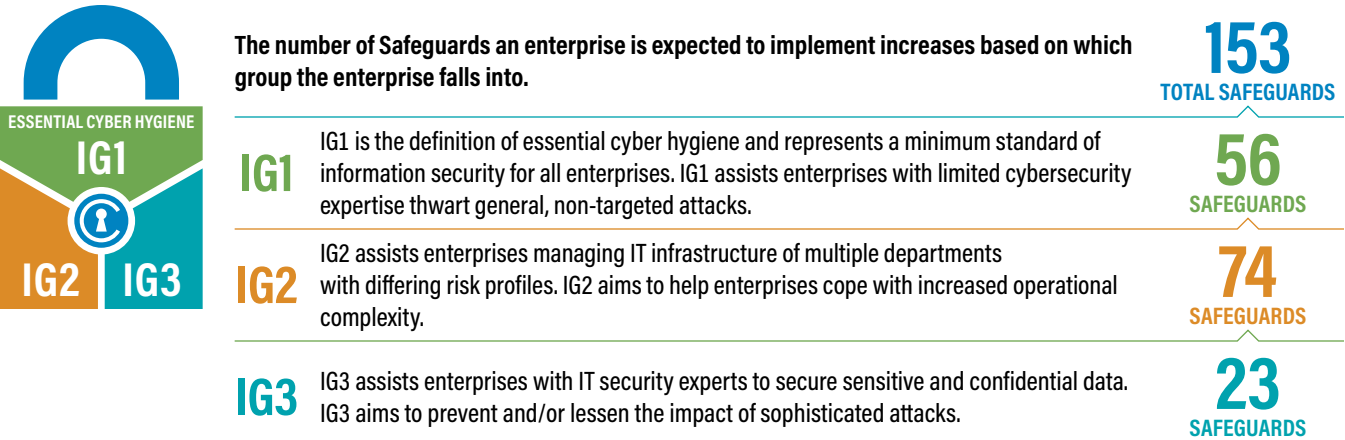
Credit card breaches, identity theft, ransomware, stolen passwords, theft of intellectual property, loss of privacy, denial of service — these cyber incidents have become everyday news. Victims include some of the largest, best-funded, and most security-savvy enterprises: government agencies, major retailers, financial services companies, even security solution vendors. Many of the victims have millions of dollars to allocate for cybersecurity, yet still fall short in their efforts to defend against common attacks. What’s even more disturbing is that many of the attacks could have been prevented by well-known security practices such as regular patching and secure configurations.

So, what are the rest of us supposed to do? **How do enterprises with small budgets and limited staff respond to the continuing cyber problem?** This guide seeks to empower small enterprise owners to help them protect their enterprises with a limited number of high-priority actions based on the Center for Internet Security’s Critical Security Controls (CIS Controls). The CIS Controls are a prioritized set of defensive actions aimed to protect enterprises from the most common attacks. They are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. Each CIS Control includes smaller actions, known as CIS Safeguards, which focus on measurable actions so that you can more easily track your progress in applying effective protection against common attacks.

 **CIS Controls** In an effort to simplify and prioritize the process of effectively implementing the CIS Controls, CIS created three Implementation Groups (IGs) — IG1, IG2, and IG3, as shown below. IGs are based on the risk profile and resources that an enterprise has available to them to implement the CIS Controls. Each IG identifies a set of Safeguards that they need to implement. IG1, defined as “essential cyber hygiene,” provides effective security value with technology and processes that are generally already available while providing a basis for more tailored and sophisticated action, if warranted. By defining IG1, we can specify tools that can be put in place to implement the actions, measurements to track progress or maturity, and reporting that can be used to manage an enterprise improvement program. Building upon IG1 is an additional set of Safeguards (IG2) for enterprises with more resources and expertise, but also greater risk exposure. Finally, the rest of the Safeguards make up IG3, for enterprises with the greatest risk exposure. CIS recommends IG1 for users of this guide.

**This guide works as a ladder to help smaller enterprises rapidly adopt IG1, or essential cyber hygiene.** IG1 is not just another list of good things to do; it is an essential set of steps that help all enterprises deal with the most common types of attacks we see in real life. The methodology provided in this guide is meant to fast-track a large majority of the recommended actions within IG1. Once an enterprise has taken all of the steps recommended within this guide, enterprises should identify the IG1 Safeguards they have yet to complete and ensure they are putting all of the IG1 Safeguards into place within their IT infrastructure.

Figure 1. Understanding IG1



**So, what specific threats does this guide help with?** This guide is meant to help small enterprises defend against some of the most common threats, including:

---



### Theft of Information

Hackers and dissatisfied employees try to obtain personally identifiable information (PII), or steal credit card information, customer lists, intellectual property, and other sensitive information.

---



### Password Theft

Attackers steal passwords to access company systems.

---



### Phishing Attacks

Email designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system.

---



### Ransomware

Malicious software blocks access to a computer so that criminals can hold your data for ransom.

---



### Natural Disasters

Data loss occurs due to natural events and accidents like fires and floods.

---



### Defacement and Downtime

Attackers force your website or other technology to no longer look or function properly. This could be as a joke, for political reasons, or to damage your reputation

---

# Next Steps

Whether you use the CIS Controls, and/or another way to guide your security improvement program, you should recognize that “it’s not about the list.” You can get a credible list of security recommendations from many sources—it is best to think of the list as a starting point. It is important to look for the ecosystem that grows up around the list. Where can I get training, complementary information, explanations; how have others implemented and used these recommendations; is there a marketplace of vendor tools and services to choose from; how will I measure progress or maturity; how does this align with the many regulatory and compliance frameworks that apply to me? The true power of the CIS Controls is not about creating the best list, it is about harnessing the experience of a community of individuals and enterprises to actually make security improvements through the sharing of ideas, tools, lessons, and collective action.

To support this, CIS acts as a catalyst and clearinghouse to help us all learn from each other. Since Version 6, there has been an explosion of complementary information, products, and services available from CIS, and from the industry-at-large. Please contact CIS for the following kinds of working aids and other support materials, such as:

- Mappings from the CIS Controls to a very wide variety of frameworks
- Use cases of enterprise adoption
- A list of ongoing references to the CIS Controls in national and international standards, state and national legislation and regulation, trade and professional associations, etc.
- Information tailored for small and medium enterprises
- Measurement and metrics for the CIS Controls
- Pointers to vendor white papers and other materials that support the CIS Controls

If you have additional questions, reach out to the CIS Controls team at [controlsinfo@cisecurity.org](mailto:controlsinfo@cisecurity.org).

The Center for Internet Security (CIS®) is a 501(c)(3) nonprofit organization whose mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

For additional information, go to <https://www.cisecurity.org>.

# Overview

Security and good IT management go hand-in-hand, since a well-managed network is more difficult to successfully attack than a poorly managed one. To begin understanding how well your enterprise is managing its cybersecurity, start by asking yourself these questions:

- Do you know what computers, phones, and other IT assets are being used in your office?
- Are you using unique, secure passwords and multi-factor authentication wherever possible?
- Do you set up your computers with security in mind?
- Do you manage who has access to sensitive information or who has extra privileges?
- Is your staff clear about their role in protecting your enterprise from cyber incidents?

To address these types of questions, this guide lists a variety of free or low-cost tools, as well as procedures you can implement to improve your security. The list is not meant to be exhaustive, but it is representative of the wide variety of resources available at low or no cost that any small business can leverage to improve its cybersecurity. To help you prioritize your efforts, this guide recommends using a phased approach to improve your cybersecurity:

**CIS Implementation Group 1 is not just another list of good things to do. IG1 represents an essential set of steps that all enterprises should implement ASAP to defend their networks. This guide will help quickly put your enterprise onto a secure path.**

|                |                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Phase 1</b> | Complete the five inventory worksheets: <ul style="list-style-type: none"><li>• Enterprise Asset Inventory Worksheet</li><li>• Software Asset Inventory Worksheet</li><li>• Data Inventory Worksheet</li><li>• Service Provider Inventory Worksheet</li><li>• Account Inventory Worksheet</li></ul> |
| <b>Phase 2</b> | Complete the Asset Protection Worksheet for each asset in the inventory.                                                                                                                                                                                                                            |
| <b>Phase 3</b> | Complete the Account Security Worksheet for each account in the account inventory.                                                                                                                                                                                                                  |
| <b>Phase 4</b> | Complete the Backup and Recovery Worksheet for each asset.                                                                                                                                                                                                                                          |
| <b>Phase 5</b> | Complete the Incident Response Worksheet.                                                                                                                                                                                                                                                           |
| <b>Phase 6</b> | Ensure that all employees review the training options listed in the Cyber Education Worksheet.                                                                                                                                                                                                      |

Each step in Phase 1 is accompanied by worksheets or spreadsheets to help you along the way. This phase involves knowing what's connected to your network, the software you use, what data is being protected, your service providers, and your accounts. Phase 2 focuses on protecting your technology, and Phase 3 ensures that each account your enterprise uses is appropriately locked down. Phase 4 helps you to back up and store enterprise data elsewhere. And Phases 5 and 6 help your enterprise to prepare in advance for disruptive events through planning and education.

You may want to assign one person in your enterprise to be the cybersecurity leader to report regularly on security activities. **Once any worksheets are completed, you can print them out and put them into a binder for safekeeping and organization, slowly creating a physical record of your cybersecurity posture. Alternatively, these worksheets can be stored digitally in a spreadsheet.** It doesn't matter if you keep a physical or digital copy of the worksheets, but if not adequately protected, the information stored within can be used to make cyber attacks against your enterprise much easier. Physical worksheets and binders should be locked up in a safe location, and digital files should be stored on a password-protected computer in line with cyber hygiene best practices.

# Phase 1

## Complete the Five Inventory Worksheets

The first step in this phase is to know your network, including your connected devices, critical data, and software. Without a clear understanding of the computers and other technology you must protect, you'll have a hard time protecting your property and data.

Here are a few key questions worth considering:

- Do you know which devices are connected to your network and what software is installed?
- Do you know which software platforms are being used by your employees (e.g., email, chat tools)?
- Do you know which devices contain your most important data?

Remember, if your enterprise's data is lost, stolen, or corrupted, you could be put out of business. Accidents and natural disasters can also destroy the data you rely on. A company's data can be quite valuable. Parties internal and external to your enterprise may want to steal customer lists, credit card information, or intellectual property. Your network and the connected devices are the primary means to steal that data. Connected devices are the "front door." It doesn't matter if your enterprise is large or small; anyone can be a target.

### PROGRESS METER

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| ► Phase 1 | Complete the five inventory worksheets:                                           |
|           | Enterprise Asset Inventory Worksheet                                              |
|           | Software Asset Inventory Worksheet                                                |
|           | Data Inventory Worksheet                                                          |
|           | Service Provider Inventory Worksheet                                              |
|           | Account Inventory Worksheet                                                       |
| Phase 2   | Complete the Asset Protection Worksheet.                                          |
| Phase 3   | Complete the Account Security Worksheet.                                          |
| Phase 4   | Complete the Backup and Recovery Worksheet.                                       |
| Phase 5   | Complete the Incident Response Worksheet.                                         |
| Phase 6   | Ensure all employees review training options listed in Cyber Education Worksheet. |

# Know What's Connected to Your Office Network

Multiple benefits result from having a good understanding of which devices are on your network. Your environment becomes easier to manage and you know what devices need to be protected. Below are some actions you can take to learn about the devices on your network.



## Create a policy and complete accompanying worksheet

Create a policy for keeping an enterprise asset inventory. Additionally, the [Enterprise Asset Inventory Worksheet](#) (see page A2) should be completed. If printed, multiple copies of the worksheets may be needed to contain all of your devices. List all the computers, smart phones, tablets, and other technology you own. You will likely need to walk around and check for any forgotten computers and talk to employees about the computers they use. Be sure to include the device's name, type (e.g., desktop, phone), model, where it resides in your office, and a serial number or other identifier about the device. Some users may be out of the office or working remotely, and all of those systems should be included as well.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Enterprise Asset Inventory Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Check your wireless router Internet Protocol (IP) address and device names for all devices connected to the network.
- ☐ For larger networks, use network scanning tools (commercial or open source) to identify all the devices on your network. Example tools are listed in the cost-effective solutions section below.
- ☐ If you have the technical expertise, you can use simple network scanning tools such as [Nmap](#) and [Zenmap](#).
- ☐ Leverage the [CIS Enterprise Asset Management Policy Template](#).



## Cost-effective solutions

**Spiceworks:** Free IT inventory and asset management software to identify devices and software on your network (<https://www.spiceworks.com/>)

**Lansweeper:** Cross-platform IT asset discovery tool (<https://www.lansweeper.com/>)

**OpenAudit:** Inventory software on workstations, servers, and network devices (<http://www.open-audit.org/>)

## PROGRESS METER

### Phase 1 Complete the five inventory worksheets:

#### ► Enterprise Asset Inventory Worksheet

Software Asset Inventory Worksheet

Data Inventory Worksheet

Service Provider Inventory Worksheet

Account Inventory Worksheet

### Phase 2 Complete the Asset Protection Worksheet.

### Phase 3 Complete the Account Security Worksheet.

### Phase 4 Complete the Backup and Recovery Worksheet.

### Phase 5 Complete the Incident Response Worksheet.

### Phase 6 Ensure all employees review training options listed in Cyber Education Worksheet.

# Know What Software Is on Your Systems

Managing software is a key component of both good IT and effective cybersecurity. Unknown software within your environment can pose legal liability and security risks. Unpatched software is a common way for malware to infiltrate and attack your systems. Software you don't know about can't be updated or patched. By understanding what software you have installed, and controlling who can install, modify, and delete that software, you'll reduce both the likelihood and impact of being compromised.



## Create a policy and complete accompanying worksheet

Create a policy for keeping a software asset inventory. Additionally, the [Software Asset Inventory Worksheet](#) (see page A3) should be completed. If printed, multiple copies of the worksheets may be needed. List all of the software that you regularly use, especially software that you purchased. Feel free to modify the worksheet as needed. Consider applications for laptops, point of sale (POS) systems, and even mobile apps. Software used by remote users should be included as well. When in doubt, document it.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Software Asset Inventory Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Create an inventory of applications that are running on your computers:
  - ☐ Manually check the installed programs within the Windows operating system to get a list of installed software applications.
  - ☐ Periodically check to see what software applications are running on your devices, using available inventory or auditing tools.
- ☐ Develop an enterprise process for securely downloading software to your network and make sure employees understand it.
- ☐ Leverage the [CIS Software Asset Management Policy Template](#).



## Cost-effective solutions

**Spiceworks:** Free IT inventory and asset management software to identify devices and software on your network (<https://www.spiceworks.com/>)

**PDQ:** Software inventory and patching app (<https://www.pdq.com>)

**OpenAuditIT:** Inventory software on workstations, servers, and network devices (<http://www.open-audit.org/>)

## PROGRESS METER

### Phase 1 Complete the five inventory worksheets:

Enterprise Asset Inventory Worksheet

► Software Asset Inventory Worksheet

Data Inventory Worksheet

Service Provider Inventory Worksheet

Account Inventory Worksheet

### Phase 2 Complete the Asset Protection Worksheet.

### Phase 3 Complete the Account Security Worksheet.

### Phase 4 Complete the Backup and Recovery Worksheet.

### Phase 5 Complete the Incident Response Worksheet.

### Phase 6 Ensure all employees review training options listed in Cyber Education Worksheet.

# Know the Data You're Trying to Protect

To protect your business, you need to understand the value of your data and how it can be used. You may also be required by law to protect certain types of information such as credit card and medical information. Enterprise data may be stored on laptops inside your office, stored in the cloud, or stored on phones and computers used by remote employees. Data is messy and gets everywhere you don't want it.

Here are some examples of data you will want to identify and inventory:

- Credit card, banking, tax, and other financial information
- PII to include Social Security numbers, health information, usernames and passwords, home addresses, birthdates, etc.
- Customer lists, product lists, pricing information, etc.
- Trade secrets, patented technologies, and other forms of intellectual property
- Any other data that may be covered by data protection laws in your country (e.g., medical, privacy, national security)



## Create a policy and complete accompanying worksheet

Create a policy for protecting your data and managing your log files. Additionally, the [Data Inventory Worksheet](#) (see page A4) should be completed. If printed, multiple copies of the worksheets may be needed. List the sensitive information within your enterprise such as personally identifiable information (PII) and financial records. Consider all the data stored on the devices within your enterprise, software, and service provider inventories. Include the filename, the type of media, where it is stored, why this information is valuable, and any individuals with access. Feel free to modify the worksheet as needed. Some remote users may use software that should be included as well. When in doubt, document it.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Data Inventory Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Create an inventory of the data your enterprise stores.
- ☐ Consider any laws that govern the data that your enterprise stores, such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR).
  - ☐ Ensure any data covered by a regulatory framework is appropriately protected according to that framework.
- ☐ Leverage the [CIS Data Management Policy Template](#).
- ☐ Leverage the [CIS Audit Log Management Policy Template](#).



## Cost-effective solutions

N/A: Only you know what data is most valuable in your enterprise.

## PROGRESS METER

### Phase 1 Complete the five inventory worksheets:

Enterprise Asset Inventory Worksheet

Software Asset Inventory Worksheet

#### ► Data Inventory Worksheet

Service Provider Inventory Worksheet

Account Inventory Worksheet

### Phase 2 Complete the Asset Protection Worksheet.

### Phase 3 Complete the Account Security Worksheet.

### Phase 4 Complete the Backup and Recovery Worksheet.

### Phase 5 Complete the Incident Response Worksheet.

### Phase 6 Ensure all employees review training options listed in Cyber Education Worksheet.

# Know Which Service Providers You're Using

Modern enterprises rely on service providers to help manage data and to provide important workplace functions like email, contacts, and calendar. Common service providers include Google®, Microsoft®, and Apple®. Other common service providers may offer human resource, tax, or point of sale (POS) technology. Yet service providers are susceptible to data breaches and lapses in security the same as any other company. Additionally, some service providers may have security settings that need to be enabled by you. Therefore, a service provider's cybersecurity posture affects their ability to secure your data. Understanding which service providers your company uses will help you manage cybersecurity risk.



## Create a policy and complete accompanying worksheet

Create a policy for managing service providers at your company. Additionally, the [Service Provider Inventory Worksheet](#) (see page A5) should be completed. List all of the service providers you regularly use and describe what each provider is used for. Consider service providers for web applications (e.g., Gmail, Yahoo, M365), POS systems, and even service providers that are primarily accessed through mobile. Include a primary user for the service provider. Essentially, who owns the relationship? Feel free to modify the worksheet as needed. When in doubt, document it.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Service Provider Inventory Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Create an inventory of web services or cloud solutions your enterprise uses:
  - ☐ Check with your employees to identify which online services, such as file sharing and online collaboration platforms, they are using as part of their job. Their answers may surprise you!
- ☐ Develop an enterprise strategy for allowing employees to begin using new and approved web services that they require.
- ☐ Leverage the [CIS Service Provider Management Policy Template](#).



## Cost-effective solutions

**N/A:** There is no easy solution, other than talking to your employees, to understand which web services are in use.

## PROGRESS METER

### Phase 1 Complete the five inventory worksheets:

Enterprise Asset Inventory Worksheet

Software Asset Inventory Worksheet

Data Inventory Worksheet

► **Service Provider Inventory Worksheet**

Account Inventory Worksheet

Phase 2 Complete the Asset Protection Worksheet.

Phase 3 Complete the Account Security Worksheet.

Phase 4 Complete the Backup and Recovery Worksheet.

Phase 5 Complete the Incident Response Worksheet.

Phase 6 Ensure all employees review training options listed in Cyber Education Worksheet.

# Know Which Accounts You're Using

Accounts and credentials such as passwords are how we access our phones, tablets, workstations, and web applications. Each of these accounts can be used to break into your enterprise's walled garden to steal your data and hurt your business. There are many ways to covertly obtain access to accounts such as weak and reused passwords, old accounts from a fired employee, or passwords involved in a data breach for a separate company that are also used on your systems. The first step to securing these accounts is knowing which accounts are being used in your enterprise.

|                                                                                     |                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Create a policy and complete accompanying worksheet</b> | Create a policy for inventorying and protecting your accounts. This will go hand in hand with <a href="#">Phase 3: Account Security</a> . Additionally, the <a href="#">Account Inventory Worksheet</a> (see <a href="#">page A6</a> ) should be completed. Use the Enterprise Asset, Software Asset, and Service Provider Asset inventories as your guide. Include the account owner, username, what the account is for, and if this account is used by multiple individuals. If printed, multiple copies of the worksheets may be needed. Feel free to modify the worksheet as needed.     |
|    | <b>Update every three months</b>                           | <p>The first time through will take the longest. It will be easier the second time.</p> <p>The <a href="#">Account Inventory Worksheet</a> is included in this guide. It is also <a href="#">downloadable</a> as a Microsoft Word document or <a href="#">Microsoft Excel spreadsheet</a>.</p>                                                                                                                                                                                                                                                                                               |
|  | <b>Other actions to take</b>                               | <ul style="list-style-type: none"><li><input type="checkbox"/> Create an inventory of accounts for all the devices and services your enterprise uses.<ul style="list-style-type: none"><li><input type="checkbox"/> Check with your employees to identify the websites and services they use for company business.</li></ul></li><li><input type="checkbox"/> Develop an enterprise strategy for creating and documenting new accounts for company resources.</li><li><input type="checkbox"/> Leverage the <a href="#">CIS Account and Credential Management Policy Template</a>.</li></ul> |
|  | <b>Cost-effective solutions</b>                            | <b>N/A:</b> There is no easy solution to finding out what accounts are used throughout a company. Talk to your employees to understand which accounts and services are in use, and encourage them to check in with new information often.                                                                                                                                                                                                                                                                                                                                                    |

## PROGRESS METER

|         |                                                                                   |
|---------|-----------------------------------------------------------------------------------|
| Phase 1 | Complete the five inventory worksheets:                                           |
|         | Enterprise Asset Inventory Worksheet                                              |
|         | Software Asset Inventory Worksheet                                                |
|         | Data Inventory Worksheet                                                          |
|         | Service Provider Inventory Worksheet                                              |
|         | ▶ Account Inventory Worksheet                                                     |
| Phase 2 | Complete the Asset Protection Worksheet.                                          |
| Phase 3 | Complete the Account Security Worksheet.                                          |
| Phase 4 | Complete the Backup and Recovery Worksheet.                                       |
| Phase 5 | Complete the Incident Response Worksheet.                                         |
| Phase 6 | Ensure all employees review training options listed in Cyber Education Worksheet. |

## Phase 2

# Complete Your Asset Protection Worksheets

Now that you know what you have, let’s talk about protecting it. The second phase in this security process is to securely configure each device in your asset inventory. You’ll need to print out and complete a copy of the [Asset Protection Worksheet](#) (see page A7) for *each* of the computers in your inventory. Some systems such as printers or phones won’t have all the same settings listed, and that’s OK. Simply mark them as not applicable (N/A) and finish completing the worksheet. At the end of this phase, if you have 15 devices in your asset inventory, then you should have 15 copies of this [Asset Protection Worksheet](#) completed and signed.

### PROGRESS METER

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Phase 1   | Complete the five inventory worksheets:                                           |
|           | Enterprise Asset Inventory Worksheet                                              |
|           | Software Asset Inventory Worksheet                                                |
|           | Data Inventory Worksheet                                                          |
|           | Service Provider Inventory Worksheet                                              |
|           | Account Inventory Worksheet                                                       |
| ► Phase 2 | Complete the Asset Protection Worksheet.                                          |
| Phase 3   | Complete the Account Security Worksheet.                                          |
| Phase 4   | Complete the Backup and Recovery Worksheet.                                       |
| Phase 5   | Complete the Incident Response Worksheet.                                         |
| Phase 6   | Ensure all employees review training options listed in Cyber Education Worksheet. |

# Configure and Protect Your Computers

Malware and attackers can take advantage of insecure ways that your computer is set up. To protect your enterprise, you need to ensure that your operating system and applications (especially web browsers) are up-to-date and securely configured. In addition, you should identify and leverage the anti-virus (and anti-malware) protections that are already built in to your operating system such as Microsoft Defender Antivirus on Windows.



## Create a policy and complete accompanying worksheet

Create separate policies for configuring your systems, defending against malware, and managing vulnerabilities. Additionally, complete the [Asset Protection Worksheet](#) (see page A7) for each device listed in the asset inventory you developed when completing the *Enterprise Asset Inventory Worksheet*. Modify the [Asset Protection Worksheet](#) as needed to accommodate the systems in your office.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Asset Protection Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Ensure that your browsers and all plugins are up-to-date. Only use browsers that automatically update.
- ☐ Run up-to-date anti-malware software to protect devices from malware.
- ☐ Set up free secure domain name system (DNS) services ([Quad9® on Windows](#), [Quad9® on MacOS](#)).
- ☐ Limit the use of removable media (USBs, CDs, DVDs) to those with an approved business need.
- ☐ Use encryption for secure remote management of your devices and to pass sensitive information.
- ☐ Encrypt hard drives, laptops, and mobile devices that contain sensitive information.
- ☐ For systems processing highly sensitive information, implement the recommendations from the CIS Benchmarks ([www.cisecurity.org](http://www.cisecurity.org)) to securely configure devices and applications.
- ☐ Leverage the [CIS Secure Configuration Management Policy Template](#).
- ☐ Leverage the [CIS Malware Defense Policy Template](#).
- ☐ Leverage the [CIS Vulnerability Management Policy Template](#).



## Cost-effective solutions

**Bitlocker®:** Built-in encryption for supported Microsoft® Windows devices ([https://technet.microsoft.com/en-us/library/cc732774\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx))

**FireVault:** Built-in encryption for Mac devices (<https://support.apple.com/en-us/HT204837>)

**Qualys Browser Check:** Tool to check if your browser is up-to-date with all its patches (<https://browsercheck.qualys.com/>)

**OpenVAS:** Tool to scan systems to check security baselines ([www.openvas.org](http://www.openvas.org))

**CIS Benchmarks™:** Free PDFs with consensus-based configuration guidelines for 100+ technologies (<https://www.cisecurity.org/cis-benchmarks/>)

**CIS Guide for Securing Small Offices: Guide for setting up a network for a home office or small business**

(<https://www.cisecurity.org/insights/blog/small-offices-big-security-new-guide-for-securing-telework-environments>)

### Phase 3

# Complete Your Account Security Worksheets

Now that we've secured systems, let's move on to accounts. The third phase involves making sure all your accounts are properly secured. These accounts will all be listed in the *Account Inventory Worksheet* you have already finished. You will need to print out and complete a copy of the [Account Security Worksheet](#) (see page A8) for each of the accounts in your inventory. Some accounts will not support all the settings listed, and that's OK. Do what you can. Simply mark them as N/A and finish completing the worksheet (and consider choosing an alternate service if possible). At the end of this phase, if you have 30 accounts in your account inventory, then you should have 30 copies of this [Account Security Worksheet](#) completed and signed in your binder. If you are using the spreadsheet, simply add additional rows as needed.

#### PROGRESS METER

Phase 1 [Complete the five inventory worksheets:](#)

Enterprise Asset  
Inventory Worksheet

Software Asset  
Inventory Worksheet

Data Inventory Worksheet

Service Provider  
Inventory Worksheet

Account Inventory  
Worksheet

Phase 2 [Complete the Asset Protection Worksheet.](#)

► Phase 3 [Complete the Account Security Worksheet.](#)

Phase 4 [Complete the Backup and Recovery Worksheet.](#)

Phase 5 [Complete the Incident Response Worksheet.](#)

Phase 6 [Ensure all employees review training options listed in Cyber Education Worksheet.](#)

# Protect Your Accounts

The most basic form of protecting your accounts is simply making sure you're using passwords. After that, each password should be 14 characters or more, use at least one special character, and be unique. Reusing passwords from one website on another means that if there's a data breach in one website, it may affect your other devices. For instance, if you reuse the password of your tax software for a dating site, then your financial information may be at risk if the dating site is breached. Finally, make sure you turn on multi-factor authentication (MFA) or two-factor authentication (2FA) for all services. This might involve getting a personal identification number (PIN) or code texted to your phone or using an app on your phone to supply a PIN. It's a hassle but it will save you.



## Create a policy and complete accompanying worksheet

Create a policy for inventorying and protecting your accounts

This will go hand in hand with the inventory activities you performed in Phase 1. Additionally, complete the [Account Security Worksheet](#) (see page A8) for each account listed in the account inventory. Accounts that have not been properly secured are very dangerous to the enterprise. Feel free to modify the worksheet as needed.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Account Security Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Change default passwords for all applications, operating systems, routers, firewalls, wireless access points, printer/scanners, and other devices when adding them to the network.
- ☐ Administrative accounts have extra privileges and can harm a computer if used incorrectly. Use unique and strong passwords for administrative accounts, along with MFA, where possible. Provide instructions for employees on developing strong passwords.
- ☐ Don't browse the internet or read email while logged in as an administrator. Use a separate non-administrative account for reading email, accessing the internet, and composing documents.
- ☐ Require the use of MFA where available, especially for remotely accessing your internal network or email. For example, this could include the use of secure tokens or mobile text options as an extra layer of security beyond only passwords.
- ☐ Consider using a password manager to assist in remembering long, complex, and unique passwords.
- ☐ Leverage the [CIS Account and Credential Management Policy Template](#).



## Cost-effective solutions

**LastPass®:** Password Manager  
(<https://www.lastpass.com>)

**KeePass:** Open-source password manager  
(<https://keepass.info>)

**Have I Been Pwned:** A site to check if your email addresses have been involved in a data breach  
(<https://haveibeenpwned.com>)

**CIS Password Policy Guide:** For a complete discussion of password strength guidance ([CIS Password Policy Guide](#) ([cisecurity.org](https://cisecurity.org)))

## Phase 4

# Complete Your Backup and Recovery Worksheet

Now that your enterprise has developed a strong cybersecurity foundation, you should begin to build capabilities for response in case you are attacked. This includes the ability to know how to handle a cybersecurity incident and get back to business. Thanks to the handy data inventory you made in Phase 1, you know where your sensitive data is and on which systems it is stored. The first step in this process is to leverage that inventory to make backups of all sensitive data.

Here are key questions for you:

- Do you know which critical files need to be backed up?
- Do you know the last time your critical files were backed up?
- Are you protecting those backups?

### PROGRESS METER

Phase 1 Complete the five inventory worksheets:

Enterprise Asset  
Inventory Worksheet

Software Asset  
Inventory Worksheet

Data Inventory Worksheet

Service Provider  
Inventory Worksheet

Account Inventory  
Worksheet

Phase 2 Complete the Asset  
Protection Worksheet.

Phase 3 Complete the Account  
Security Worksheet.

► Phase 4 Complete the Backup and  
Recovery Worksheet.

Phase 5 Complete the Incident  
Response Worksheet.

Phase 6 Ensure all employees  
review training  
options listed in Cyber  
Education Worksheet.

# Create and Manage Your Data Backups

Making and managing backups can be a tedious task; however, it is one of the best ways to protect yourself, recover after an incident, and get your enterprise back in order. This is especially crucial considering that ransomware can encrypt all your files and hold your data for ransom. A robust response plan, complemented by current and maintained backups, are the best protections when dealing with a cyber incident. Read more about [A Blueprint for Ransomware Defense Using the CIS Controls](#).



## Create a policy and complete accompanying worksheet

Create a policy for managing your backups. Additionally, complete the [Backup and Recovery Worksheet](#) (see [page A9](#)) for each asset in the enterprise. Be sure to reference the Enterprise Asset Inventory you created in Phase 1 so that important data from every device in the enterprise is captured and saved. Each device in your business may have valuable information that is worth storage and protection in case of a cyber incident or natural disaster (e.g., fire, flood). Feel free to modify the worksheet as needed.



## Update every three months

The first time through will take the longest. It will be easier the second time.

The [Backup and Recovery Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## Other actions to take

- ☐ Perform regular backups of all devices that contain important information:
  - ☐ Automated backups are the preferred method. It may be necessary to pay for this service. Consider using secure cloud solutions where feasible.
- ☐ Back up and protect physical paper and other items too.
- ☐ Periodically test your backups by trying to restore a backup as a periodic business practice.
- ☐ Remove sensitive information from computers no longer in use.
- ☐ Ensure that at least one backup destination is not accessible through the network. This will help protect against ransomware attacks since those backup files will not be accessible to the malware.
- ☐ Make sure any backup services are encrypting your data before you choose them for your business.
- ☐ Leverage the [CIS Data Recovery Policy Template](#).



## Cost-effective solutions

**Microsoft "Backup and Restore":** Backup utility tool installed on Microsoft® operating systems (<https://support.microsoft.com/en-us/help/17127/windows-back-up-restore>)

**Apple Time Machine:** Backup tool installed on Apple® operating systems (<https://support.apple.com/en-us/HT201250>)

**Amanda Network Backup:** Free, open-source backup tool (<http://www.amanda.org/>)

**Bacula®:** Open-source network backup and recovery solution (<https://www.bacula.org/>)

## Phase 5

# Complete Your Incident Response

No one wants a cybersecurity incident to happen, but the better prepared you are, the better position you will be in if an attack occurs. Looking at the stats, things aren't always looking good out there. Cyber incidents include a denial-of-service (DoS) attack that shuts down your website, a ransomware attack that locks up your system or your data, a malware attack that results in loss of your customer or employee data, and the theft of a laptop containing unencrypted data. To be prepared, you need to know what resources are available in the event of an incident. You may be able to call on internal IT staff to help, or maybe you rely on a third party to provide incident management services. Either way, you should know the roles and expectations of anyone responsible for incident management before an event occurs.

### PROGRESS METER

Phase 1 **Complete the five inventory worksheets:**

Enterprise Asset  
Inventory Worksheet

Software Asset  
Inventory Worksheet

Data Inventory Worksheet

Service Provider  
Inventory Worksheet

Account Inventory  
Worksheet

Phase 2 **Complete the Asset  
Protection Worksheet.**

Phase 3 **Complete the Account  
Security Worksheet.**

Phase 4 **Complete the Backup and  
Recovery Worksheet.**

► Phase 5 **Complete the Incident  
Response Worksheet.**

Phase 6 Ensure all employees  
review training  
options listed in Cyber  
Education Worksheet.

# Have an Incident Response Plan in Place Prior to an Attack

A comprehensive cybersecurity program includes getting ready for an attack on your computer systems, but also plans and procedures for what to do if an attack is successful. This is sometimes overlooked, but it's critical. Incident response is about stopping the damage an attack can cause in your network once it gets in, and removing any infection to prevent further harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.



## Create a policy and complete accompanying worksheet

Create a policy for responding to computer incidents, like hacking. This policy will help you identify key elements that should be in your incident response plan. Additionally, the [Incident Response Worksheet](#) (see [page A10](#)) should be completed to help you along the way in case your systems are compromised. Make sure the people that are selected to help with a computer incident are up to the task and understand the importance of this activity.



## Update every three months

The first time will take the longest. It will be easier the second time.

The [Incident Response Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## What you can do to prepare:

- ☐ Identify those within your enterprise who will serve as the lead in case of an incident.
- ☐ Have contact information available for IT staff and/or third-party organizations.
- ☐ Join InfraGard®, Information Sharing and Analysis Centers (ISACs), or other associations that focus on sharing information and promoting cybersecurity.
- ☐ Keep a list of external contacts as part of your plan. These could include legal counsel, insurance agents if you carry cyber-risk coverage, and security consultants.
- ☐ Familiarize yourself with your state's data breach notification laws.
- ☐ Leverage the [CIS Incident Response Policy Template](#).



## What to do if an incident occurs:

- ☐ U.S. State, Local, Tribal, and Territorial (SLTT) entities can report incidents to the CIS Multi-State Information Sharing and Analysis Center® (MS-ISAC®).
  - ☐ 866-787-4722 (24/7)
  - ☐ [SOC@msisac.org](mailto:SOC@msisac.org)
- ☐ Many MS-ISAC resources for incident response are available here:
  - ☐ <https://www.cisecurity.org/ms-isac/services>
- ☐ MS-ISAC members can offer access to a library of cybersecurity resources for IR through the Homeland Security Information Network (HSIN):
  - ☐ The HSIN portal also allows for reporting, secure email, and document sharing.
  - ☐ The HSIN offers tabletop exercises, working groups, and access to colleagues.
- ☐ Consider contacting an IT or cybersecurity consultant if the nature and extent of the incident aren't clear to you.
- ☐ Consider contacting legal counsel if it appears that personal information was involved in the incident.
- ☐ Prepare to notify any affected individuals whose personal information was involved in a breach.
- ☐ Inform law enforcement as needed.

# Phase 6

## Complete Your Cyber Education Worksheet

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise than it is to find a network exploit to do it directly. Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites. No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. This will increase the culture of security and discourage risky workarounds.

### PROGRESS METER

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| Phase 1   | Complete the five inventory worksheets:                                           |
|           | Enterprise Asset Inventory Worksheet                                              |
|           | Software Asset Inventory Worksheet                                                |
|           | Data Inventory Worksheet                                                          |
|           | Service Provider Inventory Worksheet                                              |
|           | Account Inventory Worksheet                                                       |
| Phase 2   | Complete the Asset Protection Worksheet.                                          |
| Phase 3   | Complete the Account Security Worksheet.                                          |
| Phase 4   | Complete the Backup and Recovery Worksheet.                                       |
| Phase 5   | Complete the Incident Response Worksheet.                                         |
| ► Phase 6 | Ensure all employees review training options listed in Cyber Education Worksheet. |

# Ensure All Employees Are Trained to Recognize and Prevent Cybersecurity Incidents

Cybersecurity is not just about technology; it is also about process and people. Solely managing security tools and software is insufficient to defend yourself in a modern environment. To help secure your enterprise, your staff must also practice strong cybersecurity behaviors. You need to expose employees to safe online behaviors to keep your assets protected. How you choose to communicate this information is up to you; but the right communication method for the right employee can make a difference in their retaining and following these behaviors.



## Create a policy and complete accompanying worksheet

Create a policy for cybersecurity education in your enterprise. This policy will act as the foundation for your cybersecurity training and awareness program. Additionally, the [Cyber Education Worksheet](#) (see page A11) should be completed. This worksheet contains video options that employees can watch. Ensure at least one video from each category is viewed by each member of your workforce. Be sure that all staff understand that cybersecurity is an important part of their job. Do what you can so they understand how to protect your enterprise and how this protection also applies to their personal lives. Verify that all employees review the required training. Feel free to modify the worksheet as needed with other videos and resources.



## Update every three months

Make sure you ask other local businesses in the area what forms of security training they provide to their employees. Other strategies working in your area might work well for you too.

The [Cyber Education Worksheet](#) is included in this guide. It is also [downloadable](#) as a Microsoft Word document or [Microsoft Excel spreadsheet](#).



## What to communicate:

- ☐ Identify those within your enterprise who have access to, or handle sensitive data, and ensure they understand their role in protecting that information.
- ☐ Two very common attack methods include phishing email and phone call attacks. Be sure your employees can explain and identify common indicators of an attack. These can include someone creating a strong sense of urgency, someone asking for very sensitive or private information, someone using confusing or technical terms, and someone asking the employee to ignore or bypass security procedures.
- ☐ Ensure that everyone knows that common sense is ultimately your best defense. If something seems odd, suspicious, or too good to be true, it is most likely an attempted attack.
- ☐ Encourage the use of strong, unique passphrases for every account and multi-factor authentication where possible.
- ☐ Require everyone to use "screen lock" on their mobile devices.
- ☐ Make sure all staff understand how to keep their devices and software updated and current.
- ☐ [Leverage the CIS Security Awareness Skills Training Policy Template.](#)



## Cost-effective solutions

- ☐ SANS *Ouch!* newsletters, video of the month, daily tips, and posters (<https://www.sans.org/newsletters/ouch/>)
- ☐ MS-ISAC monthly newsletters (<https://msisac.cisecurity.org/newsletters/>)
- ☐ Learn how to protect yourself, your family, and your devices with tips and resources from the National Cybersecurity Alliance (<https://staysafeonline.org/stay-safe-online>)

# Appendix A

## Cybersecurity Worksheets Summary

The following worksheets will help you along the way in each phase of the process outlined in this document. Each worksheet contains small, discrete tasks that you can accomplish. Many of the tasks from the worksheets will have to be performed for each laptop or computer within your network. Once a worksheet is completed, you can print them out and put them into a binder for safekeeping and organization, slowly creating an up-to-date record of your cybersecurity posture. Alternatively, these worksheets can be stored digitally in a spreadsheet. Remember that these documents should be protected since they contain sensitive data. Physical worksheets and binders should be locked up in a safe location, and the files should be stored on a password protected computer in line with cyber hygiene best practices.

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| <b>Phase 1</b> | <a href="#">Enterprise Asset Inventory Worksheet (see page A2)</a> |
|                | <a href="#">Software Asset Inventory Worksheet (see page A3)</a>   |
|                | <a href="#">Data Inventory Worksheet (see page A4)</a>             |
|                | <a href="#">Service Provider Inventory Worksheet (see page A5)</a> |
|                | <a href="#">Account Inventory Worksheet (see page A6)</a>          |
| <b>Phase 2</b> | <a href="#">Asset Protection Worksheet (see page A7)</a>           |
| <b>Phase 3</b> | <a href="#">Account Security Worksheet (see page A8)</a>           |
| <b>Phase 4</b> | <a href="#">Backup and Recovery Worksheet (see page A9)</a>        |
| <b>Phase 5</b> | <a href="#">Incident Response Worksheet (see page A10)</a>         |
| <b>Phase 6</b> | <a href="#">Cyber Education Worksheet (see page A11)</a>           |

# Enterprise Asset Inventory Worksheet

**TIME ESTIMATE**  
First time: 4 hours  
After: 15 minutes

Print out the worksheet and list all the technology in your enterprise. Multiple sheets may be needed. Refer to Step 1 of the guide for further instructions. Sign and date when complete. If this is not the first time you've taken an inventory, remove any unwanted devices you've discovered that do not belong to your company.

| Name | Type | Physical Location in Office | Serial Number |
|------|------|-----------------------------|---------------|
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |
|      |      |                             |               |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Software Asset Inventory Worksheet

**TIME ESTIMATE**  
First time: 4 hours  
After: 15 minutes

Print out the worksheet and list all the software you regularly use. Multiple sheets may be needed. Refer to Step 1 of the guide for further instructions. Sign and date when complete. If this is not the first time you've taken an inventory, remove any unwanted devices you've discovered that do not belong to your company.

| Product Name | Description | License Information |
|--------------|-------------|---------------------|
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |
|              |             |                     |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Data Inventory Worksheet

**TIME ESTIMATE**  
First time: **2 hours**  
After: **15 minutes**

Print out the worksheet and list all the sensitive information within your enterprise (e.g., PII, financial records). Multiple sheets may be needed. Refer to Step 1 of the guide for further instructions. Sign and date when complete.

| Filename | Location | Media Type | Reasons for Sensitivity |
|----------|----------|------------|-------------------------|
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |
|          |          |            |                         |

▲ **Signature**

▲ **Date and Time of Completion**

▲ **Date of Next Update** Update this sheet every 3 months

# Service Provider Inventory Worksheet

**TIME ESTIMATE**  
First time: 4 hours  
After: 15 minutes

Print out the worksheet and list all service providers you use in your enterprise. Multiple sheets may be needed. Refer to Step 1 of the guide for further instructions. Sign and date when complete.

| Product Name | Description | Primary User |
|--------------|-------------|--------------|
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |
|              |             |              |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Account Inventory Worksheet

**TIME ESTIMATE**  
First time: 2 hours  
After: 15 minutes

Print out the worksheet and list the important or critical accounts you have for your entire enterprise. Multiple sheets may be needed. Refer to Step 1 of the guide for further instructions. Sign and date when complete.

| Service Provider or Product | Account Owner | Username | Shared Account? (Y / N) |
|-----------------------------|---------------|----------|-------------------------|
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |
|                             |               |          |                         |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Asset Protection Worksheet

## TIME ESTIMATE

30 minutes  
per computer

Print out the worksheet and complete the following actions for each asset in the enterprise. Multiple sheets may be needed. Refer to Step 2 of the guide for further instructions. Sign and date when complete. Make sure to complete the *Authentication Worksheet* as well.

|                          | Asset Name:                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Make sure all software installed on this system is up-to-date.                                    |
| <input type="checkbox"/> | Check to see if this device is encrypted. Not all devices easily support this.                    |
| <input type="checkbox"/> | Make sure this device's screen automatically locks after 10 minutes (600 seconds).                |
| <input type="checkbox"/> | Turn on firewall and network protection, if supported.                                            |
| <input type="checkbox"/> | Make sure automatic updates are turned on for the operating system (e.g., Windows, MacOS).        |
| <input type="checkbox"/> | Make sure automatic updates are turned on within each application, if supported.                  |
| <input type="checkbox"/> | Only use up-to-date and modern internet browsers.                                                 |
| <input type="checkbox"/> | Only use up-to-date and modern email applications. N/A if you use webmail (e.g., Gmail, M365).    |
| <input type="checkbox"/> | Use secure DNS services such as Quad9 ( <a href="#">Windows</a> , <a href="#">MacOS</a> ).        |
| <input type="checkbox"/> | Install and turn on anti-virus software. This may already be installed by default, but make sure. |
| <input type="checkbox"/> | Make sure all anti-virus software and signatures are up-to-date.                                  |
| <input type="checkbox"/> | Disable autorun and autoplay for Windows users.                                                   |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Account Security Worksheet

## TIME ESTIMATE

5 minutes  
per account

Print out the worksheet and complete the following actions for each account used in the enterprise. Multiple sheets may be needed. Refer to Step 3 of the guide for further instructions. Sign and date when complete. Make sure to complete the *Asset Protection Worksheet* as well for all assets.

|                          |                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                          | <b>Account Name:</b>                                                                                                             |
| <input type="checkbox"/> | Create some form of password, PIN, or passcode for this account.                                                                 |
| <input type="checkbox"/> | Ensure the password for this account is not being used for any other account you own, to include personal and business accounts. |
| <input type="checkbox"/> | If this account is no longer in use, delete or disable it.                                                                       |
| <input type="checkbox"/> | Turn on multi-factor authentication for this account, if supported.                                                              |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Backup and Recovery Worksheet

**TIME ESTIMATE**  
30 minutes  
per computer

Print out the worksheet and complete the following actions to backup data on each asset in the enterprise. Multiple sheets will be needed. Refer to Step 4 of the guide for further instructions. Sign and date when complete.

Note: It's possible that there's no data worth backing up on this machine.

|                          |                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <b>Asset Name:</b>                                                                                                                           |
| <input type="checkbox"/> | Decide how long valuable data on this device should be stored.                                                                               |
| <input type="checkbox"/> | Delete unneeded data in a secure way (refer to <a href="#">Phase 4</a> for additional information) (e.g., USB drive).                        |
| <input type="checkbox"/> | Automate backups via either a tool, a service, or by physically copying information to removable media on a regular basis.                   |
| <input type="checkbox"/> | Keep a copy of your valuable and sensitive data offline. Putting it on a USB drive accomplishes this.                                        |
| <input type="checkbox"/> | Verify that any backup services your company is using will encrypt your data.                                                                |
| <input type="checkbox"/> | Keep any physical copies of backups (e.g., paper, USB sticks) safe from theft or destruction.                                                |
| <input type="checkbox"/> | Keep one copy of your most sensitive and valuable data offsite at another physical location. This may include using a cloud storage company. |

▲ **Signature**

▲ **Date and Time of Completion**

▲ **Date of Next Update** Update this sheet every 3 months

# Incident Response Worksheet

## TIME ESTIMATE

30 minutes  
per computer

Print out the worksheet and complete the following actions within your enterprise to ensure you're ready just in case your enterprise experiences a cybersecurity incident. Refer to Step 5 of the guide for further instructions. Sign and date when complete.

|                          |                                                                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | <p>Assign an employee to be the lead person to handle cybersecurity incidents.</p> <p><b>Designated Employee:</b></p> <p><b>Telephone:</b></p> <p><b>Email:</b></p>                                                                                          |
| <input type="checkbox"/> | <p>Who should the designated personnel contact if there is an incident? Include contact information. This may be law enforcement, IT technician, or other employees.</p> <p><b>Person or organization:</b></p> <p><b>Telephone:</b></p> <p><b>Email:</b></p> |
| <input type="checkbox"/> | <p>Train employees on the personnel they should contact if a cyber incident occurs.</p>                                                                                                                                                                      |
| <input type="checkbox"/> | <p>Request that any technical personnel handling the incident store and maintain log files from the compromised systems. This includes logs from applications and operating systems.</p>                                                                     |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

# Cyber Education Worksheet

## TIME ESTIMATE

4 hours  
per employee

Below are lists of options in each category for security awareness training in a variety of categories. Select one or more of the options presented below for you and your employees to view. Edit the lists to reflect your selections, if desired. Print out and provide this worksheet to each employee. Make sure all employees review the required training.

Note: This is an illustrative list. Feel free to find other trainings in each category that fit your needs.

| Done                     | Training Name                          | Training Location                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | <b>Social Engineering Awareness</b>    | Security Awareness: Phishing & Ransomware ( <a href="https://youtu.be/D_yAYhjNE-0">https://youtu.be/D_yAYhjNE-0</a> )<br>Security Awareness: Vishing <a href="https://www.youtube.com/watch?v=Hc01oZPvByg">https://www.youtube.com/watch?v=Hc01oZPvByg</a><br>(ISC) <sup>2</sup> U.S. Military Germany <a href="https://www.youtube.com/watch?v=CTMETY6hWN4">https://www.youtube.com/watch?v=CTMETY6hWN4</a><br>SANS Security Awareness: Social Engineering <a href="https://www.youtube.com/watch?v=0JJbS4Ly90g">https://www.youtube.com/watch?v=0JJbS4Ly90g</a><br>Social Engineering Webinar <a href="https://www.youtube.com/watch?v=5tmcp5fpb18">https://www.youtube.com/watch?v=5tmcp5fpb18</a><br>Professor Messer <a href="https://www.youtube.com/watch?v=QUgLxIl_P58">https://www.youtube.com/watch?v=QUgLxIl_P58</a> |
| <input type="checkbox"/> | <b>Authentication</b>                  | Security Awareness: Passwords <a href="https://www.youtube.com/watch?v=0Wd3JoUHXno">https://www.youtube.com/watch?v=0Wd3JoUHXno</a><br>Professor Messer: Authentication Methods <a href="https://youtu.be/cPvgt-Bo3k0">https://youtu.be/cPvgt-Bo3k0</a><br>Professor Messer: Password Attacks <a href="https://www.youtube.com/watch?v=hNhak8lilrA&amp;t=578s">https://www.youtube.com/watch?v=hNhak8lilrA&amp;t=578s</a>                                                                                                                                                                                                                                                                                                                                                                                                       |
| <input type="checkbox"/> | <b>Data Handling</b>                   | Security Awareness on Data Handling <a href="https://youtu.be/hsNRrEnB_aM">https://youtu.be/hsNRrEnB_aM</a><br>SANS Data Security <a href="https://youtu.be/Y6Vn-lrLFrl">https://youtu.be/Y6Vn-lrLFrl</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <input type="checkbox"/> | <b>Unintentional Data Exposure</b>     | Security Awareness: Removable Media <a href="https://www.youtube.com/watch?v=FRxrHduwPjY">https://www.youtube.com/watch?v=FRxrHduwPjY</a><br>Security Awareness: Data Leakage <a href="https://youtu.be/yj0Lc0pwZa0">https://youtu.be/yj0Lc0pwZa0</a><br>Physical Security Awareness <a href="https://youtu.be/2ZYgfSEbsol">https://youtu.be/2ZYgfSEbsol</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <input type="checkbox"/> | <b>Reporting Security Incidents</b>    | Security Awareness Training: Reporting an Incident <a href="https://www.youtube.com/watch?v=wKiT0ulhNFs&amp;t=42s">https://www.youtube.com/watch?v=wKiT0ulhNFs&amp;t=42s</a><br>Incident Reporting <a href="https://youtu.be/lmshxkxt0V0">https://youtu.be/lmshxkxt0V0</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <input type="checkbox"/> | <b>Missing Security Updates</b>        | Software Updates <a href="https://www.youtube.com/watch?v=xc20JvvTL04">https://www.youtube.com/watch?v=xc20JvvTL04</a><br>End User Browsing <a href="https://youtu.be/ycyTSbD7E48">https://youtu.be/ycyTSbD7E48</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <input type="checkbox"/> | <b>Connecting to Unsecure Networks</b> | Security Awareness: Wi-Fi <a href="https://www.youtube.com/watch?v=RQttayB5ymA">https://www.youtube.com/watch?v=RQttayB5ymA</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

▲ Signature

▲ Date and Time of Completion

▲ Date of Next Update Update this sheet every 3 months

## Appendix B

# Mapping the CIS Controls to This Guide

This guide is meant to fast-track a company looking to put Implementation Group 1 into place. All of the 56 IG1 Safeguards are represented in this guide, with the exception of the following seven Safeguards. While Safeguards were omitted for a variety of reasons, the primary factor for omission was the difficulty in providing step-by-step guidance for a specific activity.

| CIS Safeguard | Title                                                  |
|---------------|--------------------------------------------------------|
| 3.3           | Configure Data Access Control Lists                    |
| 4.4           | Implement and Manage a Firewall on Servers             |
| 4.6           | Securely Manage Enterprise Assets and Software         |
| 6.5           | Require MFA for Administrative Access                  |
| 8.1           | Establish and Maintain an Audit Log Management Process |
| 8.2           | Collect Audit Logs                                     |
| 12.1          | Ensure Network Infrastructure Is Up-to-Date            |

## Appendix C

# Helpful Resources

---

**Center for Internet Security, Inc. (CIS®)**

CIS makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit <https://www.cisecurity.org>.

---

**Better Business Bureau (BBB®)**

“BBB Cybersecurity” is a business education resource created to provide SMEs/SMBs with valuable tools, tips, and content to help them manage cyber risks and learn about cybersecurity best practices in the modern business environment. (<https://www.bbb.org/all/cyber-security-resources>)

---

**Federal Trade Commission (FTC)**

The FTC provides guidance for businesses on protecting personal information and on securing connected devices. ([www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business](http://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business))

“Start with Security: A Guide for Business” outlines various “Lessons Learned from FTC Cases.” (<https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>)

---

**National Cyber Security Alliance (NCSA®)**

The National Cyber Security Alliance builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work, and school with the information they need to keep themselves, their organizations, their systems, and their sensitive information safe and secure online and encourage a culture of cybersecurity. ([www.staysafeonline.org](http://www.staysafeonline.org))

---

**PCI Security Standards Council®**

PCI Payment Protection Resources for Small Merchants provide simple guidance on why and how to keep customer payment data safe. Start educating your small business customers and partners on payment security basics by downloading these resources now. ([www.pcisecuritystandards.org/pci\\_security/small\\_merchant](http://www.pcisecuritystandards.org/pci_security/small_merchant))

---

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SANS Institute</b>                       | <p>SANS is the largest source for information security training (<a href="https://www.sans.org/find-training/">https://www.sans.org/find-training/</a>) and security certification (<a href="http://www.giac.org">http://www.giac.org</a>) in the world. It also develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center (<a href="https://isc.sans.edu/">https://isc.sans.edu/</a>). Several documents address incident handling. (<a href="https://www.sans.org/reading-room/whitepapers/incident">https://www.sans.org/reading-room/whitepapers/incident</a>)</p> <p>SANS also offers a cybersecurity glossary of terms. (<a href="https://www.sans.org/security-resources/glossary-of-terms/">https://www.sans.org/security-resources/glossary-of-terms/</a>)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>U.S. Chamber of Commerce</b>             | <p>"Internet Security Essentials for Business 2.0:" The U.S. Chamber, Bank of America, Microsoft Trustworthy Computing, Splunk, and Visa have teamed up to provide businesses with this cyber guidebook, which gives small and medium-sized businesses tools for protecting computers and networks and responding to cyber incidents. (<a href="http://www.uschamber.com/issue-brief/internet-security-essentials-business-20">www.uschamber.com/issue-brief/internet-security-essentials-business-20</a>)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>U.S. Department of Homeland Security</b> | <p>"Critical Infrastructure Cyber Community C3 Voluntary Program:" Cybersecurity is critical to any business enterprise, no matter how small. However, leaders of small and midsize businesses (SMB) often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources. To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs/SMEs recognize and address their cybersecurity risks. (<a href="https://www.cisa.gov/resources-tools/programs/protecting-critical-infrastructure-critical-infrastructure-cyber-community-voluntary-program-c3vp">https://www.cisa.gov/resources-tools/programs/protecting-critical-infrastructure-critical-infrastructure-cyber-community-voluntary-program-c3vp</a>)</p> <p>"Small Business Tip Card:" America thrives with small businesses in society. There are numerous opportunities for small businesses to fill needed niches within the industry. However, many small businesses may not have all the resources they need to have a strong cybersecurity posture. By implementing simple cybersecurity practices throughout their organizations, small businesses can safeguard their information and data for increased profits. (<a href="http://www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card_04.07.pdf">www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card_04.07.pdf</a>)</p> |
| <b>U.S. Small Business Administration</b>   | <p>Is your business prepared in the event of a cybersecurity breach? Now is the time to take stock of your cybersecurity health, including the importance of securing information through best cybersecurity practices; identifying your risk and the types of cyber threats; and learning best practices for guarding against cyber threats. (<a href="http://www.sba.gov/managing-business/cybersecurity">www.sba.gov/managing-business/cybersecurity</a>)</p> <p><i>All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Contact Information</b>                  | <p>Center for Internet Security<br/>31 Tech Valley Drive<br/>East Greenbush, NY 12061<br/>518-266-3460<br/><a href="mailto:controlsinfo@cisecurity.org">controlsinfo@cisecurity.org</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit [CISecurity.org](https://CISecurity.org) or follow us on Twitter: @CISecurity.



# NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide



# NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview

## Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

## What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance 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. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

## Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the [CSF 2.0 Implementation Examples](#). If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).



## EXPLORE MORE CSF 2.0 RESOURCES

[nist.gov/cyberframework](https://nist.gov/cyberframework)

Quickly find what you need, including:

- ✓ A suite of NEW Quick Start Guides
- ✓ Implementation Examples
- ✓ Search tools
- ✓ FAQs
- ✓ And much more!

# GOVERN



The Govern Function helps you establish and monitor your business’s cybersecurity risk management strategy, expectations, and policy.

## Actions to Consider

### Understand

- Understand how cybersecurity risks can disrupt achievement of your business’s mission. *(GV.OC-01)*
- Understand your legal, regulatory, and contractual cybersecurity requirements. *(GV.OC-03)*
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. *(GV.RR-02)*

### Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.OC-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

### Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

### Communicate

- Communicate leadership’s support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

## Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

| Setting Organizational Context                                       |  | Documenting Cybersecurity Requirements |  |
|----------------------------------------------------------------------|--|----------------------------------------|--|
| Our business mission statement:                                      |  | List your legal requirements:          |  |
| What cybersecurity risks may prevent us from achieving this mission? |  | List your regulatory requirements:     |  |
|                                                                      |  | List your contractual requirements:    |  |

**Technical Deep Dive:** [Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight](#)

### Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

### Related Resources

- [Securing Small and Medium-Sized Supply Chains Resource Handbook](#)
- [Choosing A Vendor/Service Provider](#)

[View all NIST CSF 2.0 Resources Here](#)

# IDENTIFY



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

## Actions to Consider

### Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. *(ID.AM-01/02/04)*

### Assess

- Assess your assets (IT and physical) for potential vulnerabilities. *(ID.RA-01)*
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. *(ID.IM-01)*

### Prioritize

- Prioritize inventorying and classifying your business data. *(ID.AM-07)*
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. *(ID.RA)*

### Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. *(ID.IM-04)*
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. *(ID.IM)*

## Getting Started with Identifying Current Cybersecurity Risk to Your Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all your business assets.

| Software/<br>hardware/<br>system/<br>service | Asset's<br>official<br>use: | Asset<br>administrator<br>or owner: | Identify<br>sensitive data<br>the asset has<br>access to: | Is multi-factor<br>authentication<br>required to<br>access this<br>asset? | Risk to<br>business if<br>we lose<br>access to this<br>asset |
|----------------------------------------------|-----------------------------|-------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------|
|                                              |                             |                                     |                                                           |                                                                           |                                                              |

Technical Deep Dive: [Integrating Cybersecurity and Enterprise Risk Management](#)

## Questions to Consider

- What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the cybersecurity and privacy risks associated with each asset?
- What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

## Related Resources

- [NIST Risk Register Template](#)
- [Take Stock. Know What Sensitive Information You Have](#)
- [Evaluating Your Operational Resilience and Cybersecurity Practices](#)

[View all NIST CSF 2.0 Resources Here](#)

# PROTECT



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

## Actions to Consider

### Understand

- Understand what information employees should or do have access to. Restrict sensitive information access to only those employees who need it to do their jobs. *(PR.AA-05)*

### Assess

- Assess the timeliness, quality, and frequency of your company’s cybersecurity training for employees. *(PR.AT-01/02)*

### Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. *(PR.AA-03)*
- Prioritize changing default manufacturer passwords. *(PR.AA-01)*
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. *(PR.PS-02)*
- Prioritize regularly backing up your data and testing your backups. *(PR.DS-11)*
- Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data. *(PR.DS-01)*

### Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. *(PR.AT-01/02)*

## Getting Started with Protecting Your Business

Enabling multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that can access the most sensitive information. Use this checklist to give you a head start, but remember your own list will be longer than this:

| Account                                       | MFA Enabled (Y/N) |
|-----------------------------------------------|-------------------|
| 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)                            |                   |

**Technical Deep Dive:** [NIST Digital Identity Guidelines](#)

### Questions to Consider

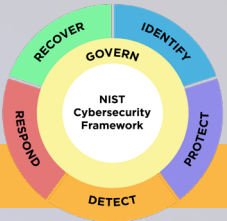
- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they’re no longer needed?
- Do employees possess the knowledge and skills to perform their jobs with security in mind?

### Related Resources

- [Cybersecurity Training Resources](#)
- [Multi-Factor Authentication](#)
- [Protecting Your Business from Phishing](#)

[View all NIST CSF 2.0 Resources Here](#)

# DETECT



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

## Actions to Consider

### Understand

- Understand how to identify common indicators of a cybersecurity incident. *(DE.CM)*

### Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. *(DE.CM-06/09)*
- Assess your physical environment for signs of tampering or suspicious activity. *(DE.CM-02)*

### Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. *(DE.CM-09)*
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. *(DE.CM)*

### Communicate

- Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it. *(DE.AE-06/07)*

## Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:



- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator sees many bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

**Technical Deep Dive:** [NIST Computer Security Incident Handling Guide](#)

## Questions to Consider

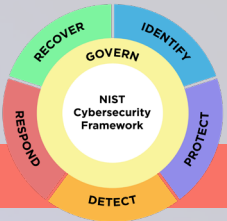
- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?

## Related Resources

- [Ransomware Protection and Response](#)
- [Detecting a Potential Intrusion](#)
- [Cybersecurity Training Resources](#)

[View all NIST CSF 2.0 Resources Here](#)

# RESPOND



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

## Actions to Consider

### Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. *(RS.MA-01)*

### Assess

- Assess your ability to respond to a cybersecurity incident. *(RS.MA-01)*
- Assess the incident to determine its severity, what happened, and its root cause. *(RS.AN-03, RS.MA-03)*

### Prioritize

- Prioritize taking steps to contain and eradicate the incident to prevent further damage. *(RS.MI)*

### Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. *(RS.CO-02/03)*

### Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response plan. This will be customized based on the business but should include:

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

**Technical Deep Dive:** [NIST Computer Security Incident Handling Guide](#)

### Questions to Consider

- Do we have a cybersecurity incident response plan? If so, have we practiced it to see if it is feasible?
- Do we know who the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

### Related Resources

- [Incident Response Plan Basics](#)
- [FBI's Internet Crime Complaint Center](#)
- [Data Breach Response: A Guide for Business](#)
- [Best Practices for Victim Response and Reporting of Cyber Incidents](#)

| Contact            | Phone |
|--------------------|-------|
| Business Leader:   |       |
| Technical Contact: |       |
| State Police:      |       |
| Legal:             |       |
| Bank:              |       |
| Insurance:         |       |

[View all NIST CSF 2.0 Resources Here](#)

# RECOVER



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

## Actions to Consider

### Understand

- Understand who within and outside your business has recovery responsibilities. *(RC.RP-01)*

### Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a vendor/partner—that documents the incident, the response and recovery actions taken, and lessons learned. *(RC.RP-06)*
- Assess the integrity of your backed-up data and assets before using them for restoration. *(RC.RP-03)*

### Prioritize

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. *(RC.RP-02)*

### Communicate

- Communicate regularly and securely with internal and external stakeholders. *(RC.CO)*
- Communicate and document completion of the incident and resumption of normal activities. *(RC.RP-06)*

### Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- ✓ A set of formal recovery processes
- ✓ Documentation of the criticality of organizational resources (e.g., people, facilities, technical components, external services)
- ✓ Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- ✓ A list of personnel who will be responsible for defining and implementing recovery plans
- ✓ A comprehensive recovery communications plan

**Technical Deep Dive:** [NIST Guide for Cybersecurity Event Recovery](#)

### Questions to Consider

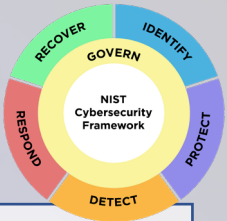
- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- What are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

### Related Resources

- [Cybersecurity Training Resources](#)
- [Creating an IT Disaster Recovery Plan](#)
- [Backup and Recover Resources](#)

[View all NIST CSF 2.0 Resources Here](#)

# Profiles and Additional Resources



## Using Organizational Profiles to Implement the Cybersecurity Framework

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the CSF Core's cybersecurity outcomes. Every Organizational Profile includes one or both of the following:

1. A **Current Profile** specifies the desired outcomes an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A **Target Profile** specifies the outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.
  - You can also use a **Community Profile** as the basis for your Target Profile. A Community Profile is a baseline of targeted outcomes for a particular sector, technology, threat type, or other use case.
  - You can also choose to use the **CSF Tiers** to inform your Profile creation. Tiers characterize the current or targeted rigor of an organization's practices by CSF Function or Category. See the [Quick-Start Guide for Using the CSF Tiers](#) for more information on Tiers and their use.

View the [Quick-Start Guide for Creating and Using Organizational Profiles](#) for more detailed information on how to get started creating Current and Target Profiles for your organization.

## Additional Resources

[The NIST Cybersecurity Framework Reference Tool](#) allows users to explore the full CSF 2.0 Core in human and machine-readable versions (in JSON and Excel), while also maintaining resources with information to help you achieve your desired outcomes, such as:

- [Mapping](#): Informative references are mappings indicating relationships between the CSF 2.0 and various standards, guidelines, regulations, and other content. They help inform how an organization may achieve the Core's outcomes.
- [Implementation examples](#) provide illustrations of concise, action-oriented steps to guide organizations in achieving the CSF outcomes. The examples are not a comprehensive list of all actions that could be taken by an organization, nor are they a baseline of required actions; they are a set of helpful examples to get organizations thinking about concrete steps.

[NIST Cybersecurity and Privacy Reference Tool \(CPRT\)](#) provides a simple way to access reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks—downloadable in common formats (XLSX and JSON).

[NIST SP 800-53](#) provides a catalog of security and privacy controls you can choose from. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. [View and export](#) from the Cybersecurity and Privacy Reference Tool (CPRT).

[The Workforce Framework for Cybersecurity \(NICE Framework\)](#) helps employers achieve the outcomes in the CSF 2.0 by assisting them to identify critical gaps in cybersecurity staffing and capabilities; determine and communicate position responsibilities and job descriptions; and provide staff training and career pathways.

# Cybersecurity Strategies for Small Businesses

March 19, 2025

Event Notes and Resources



*Disclaimer: The guidance provided in this document reflects current best practices and insights into cybersecurity for small businesses. However, the cybersecurity landscape is dynamic and subject to constant change. Readers are encouraged to consult a qualified cybersecurity professional to tailor and implement strategies suited to their specific needs and circumstances.*



CONCORDIA  
UNIVERSITY  
IRVINE

**School of Business and Economics**

# Cybersecurity

**Definition:** The technology, practices and safety measures used to mitigate and protect against cyber threats.



# DOVER CASTLE SOUTHERN ENGLAND Circa 16<sup>th</sup> Century



## DOVER CASTLE TODAY

- Dover Castle – the site was used by the Romans in the 1<sup>st</sup> century AD and later by William the Conqueror in the 11<sup>th</sup> century.
- In the 12<sup>th</sup> Century, King Henry II built what is recognizable as the castle today
- Withstood a siege by the French aligned with rebellious English nobles in 1216
- There are numerous tunnels below the castle which allowed for movement of defensive forces to confront any threats
- It was used by the British as a key Royal Navy base and was Vice-Admiral Ramsay's HQ during Operation Dynamo which evacuated 338,226 British & Allied troops from Dunkirk in 1940
- Later it was key in Operation Neptune (Naval side of D-Day) and was part of Fortitude South which deceived the Nazis into thinking the invasion was going to be at Calais.

Why the history lesson? The point is that people have been devising ways to protect what is most important to them for millennia with castles being at the forefront of such defenses for hundreds of years (albeit in different ways).



Some of the keys to effect defense include:

1. Recognizing and preparing for a threat
2. Defense in depth – a layered approach forcing bad actors to defeat multiple defenses
3. Many different ways to address a threat
4. Adapting to new threats as they arise

The analogy applies to a business' IT infrastructure.



# It is not a destination



# It is a race without a finish line

Defending against cyber attacks is a 24/7 – 365 days a year job. Preparation is key, but, businesses cannot rest easy by simply putting one solution in place.

Cyber hygiene needs to be maintained, employees need to be trained (and retrained) & software updated.

Be sure to have a clearly identified roadmap for your cyber defense.

# Cybersecurity Stats: Facts And Figures You Should Know

--Forbes 8/28/24

## The Cost of Cybercrime

---

- The total cost of damages incurred by cybercrime is expected to reach \$10.5 trillion by 2025.<sup>16</sup>
- The United States has the world's highest average data breach cost at \$9.36 million.<sup>2</sup>
- The average cost of a data breach in the healthcare industry is \$9.77 million.<sup>2</sup>

<sup>16</sup> – *Cybersecurity Ventures 2023 Official Cybercrime Report*

<sup>2</sup> – *IBM Cost of a Data Breach Report 2024*

I'm too small for anyone to attack me . . .

**NOT SO**

- Supply chain – SMBs are a gateway to their vendors, suppliers and clients
- Insurance – criminals seek easy payouts from business insurance
- Easy target – most SMBs are not well protected

# Easy Target

Lack of defense

Fewer resources

Lack of expertise

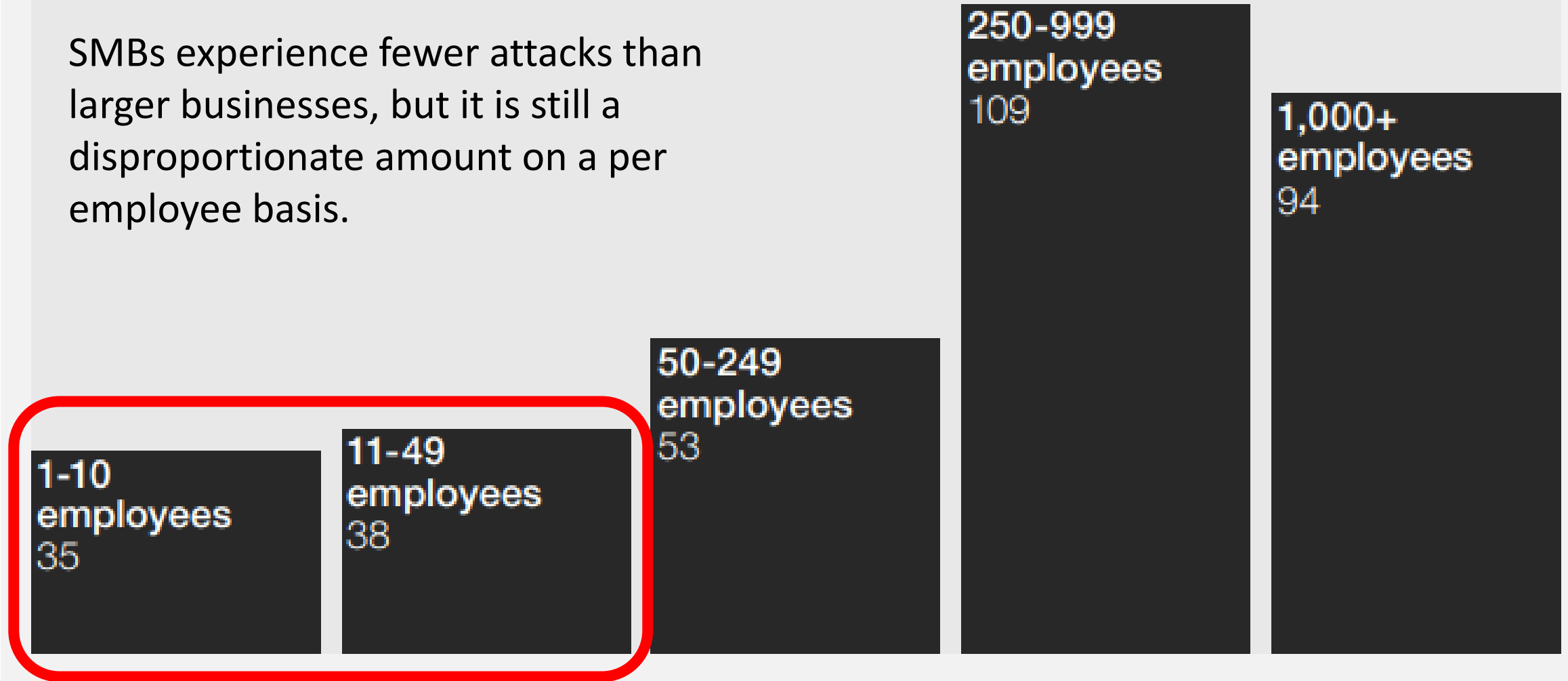


## Higher return with less effort

*SMBs do not have all the resources that enterprise companies have making them a target that takes less effort by criminals and a better chance of getting a payoff.*

## Average number of cyber attacks in the past 12 months

SMBs experience fewer attacks than larger businesses, but it is still a disproportionate amount on a per employee basis.



## Proportion of IT budget spent on cyber security (%)



# They are not just looking at you, they are looking for your clients

## Business Risk:

- 21% of victims reported losing business partners
- 40% experienced a breach via their supply chain

## Reputational Risk:

- 59% of consumers will [avoid companies](#) hit by a cyberattack according to a survey by Arcserve. Customers are likely to switch to its market rivals.



# SMBs Are an Attack Vector

- Since 2022, small businesses have experienced a [28% increase](#) in cyberattacks
- 2023 Forrester poll of more than 5,000 small-business cybersecurity professionals revealed [41%](#) experienced a cyberattack during the prior year.

“That notable rise was driven, in part, by cybercriminals targeting vendors to access their clients' data.”

– Matt Cullins – Head of Global Cyber Insurance Business at Transmission

# Some facts about SMBs:

- 43% don't have a technology solution (such as a firewall) in place
- 60% do not use cyber awareness training
- 95% of breaches are human error

*Cyber Security solutions are no longer cost-prohibitive and native security features (such as in Microsoft 365) in software are increasingly effective leaving little excuse for SMBs to practice foundational cyber defense. Awareness amongst employees is most critical.*

\*Forbes - *Preparing For 2025: The SMB Cybersecurity Gap* [Preparing For 2025: The SMB Cybersecurity Gap](#)



# Resources

The following are direct links to cybersecurity tools for small businesses



[Implementation Guide for Small- and Medium-Sized Enterprises CIS Controls IG1](#)



## Implementation Guide for Small- and Medium-Sized Enterprises

CIS Controls Implementation Group 1

[Version 2.0](#)



[Cybersecurity Framework | NIST](#)

# Some Simple Steps to Cyber Resilience

- Compliance with industry security frameworks to meet a minimum standard of security.
- Frequent security testing to identify, mitigate and prevent new vulnerabilities.
- Regular cyber training to keep employees updated on the latest threats and scams.
- Incident response planning to guide recovery efforts following a data breach or similar disruption.
- Data backups to prevent the need to give in to demands from ransomware attackers.
- System update policy and procedures to ensure the latest security patches are in place.
- Permissions management to dictate appropriate levels of access to sensitive resources.
- Password management to guide the secure creation, storage and use of credentials.

*Get help* – seek out a partner like *Managed Service Provider* that can help you build and maintain a roadmap for *cyber resilience*.

# Cyber Incident Response Plan

A robust IRP should cover the following key components:

- Preparation: Building and maintaining your incident response capabilities.
- Identification: Detecting and identifying cybersecurity incidents.
- Containment: Limiting the scope and impact of an incident.
- Eradication: Removing the threat from the organization's systems.
- Recovery & Rebuild: Restoring and returning affected systems and services to normal operations. Make changes as necessary.
- Lessons learned: Reviewing and analyzing the incident and response to improve future readiness.

# Some Definitions

# Data Breach

*An incident where confidential data or information is accessed without authorization.*

# Phishing

*Fraudulent activity in which attackers contact victims, usually by email, pretending to be from a real, reputable company to solicit personal and sensitive information.*

# Business Email Compromise (BEC)

*A specific type of phishing designed to target businesses to acquire money or sensitive data.*

# Ransomware

*Malicious software that usually locks access to some or all of your data, files and information then demands payment for its release.*

# Distributed Denial-of-Service

*Also known as DDoS attacks, occur when an attacker overloads their target's servers with internet traffic to essentially force downtime.*

# Social Media Attacks

*Social media scams often involve fraudsters creating fake profiles to communicate with users and send malicious links through spam messages.*

# Cyber Security Hygiene

Cyber Hygiene is a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data. The goal of cyber hygiene is to keep sensitive data secure and strengthen the organization's ability to recover if and when a successful attack occurs.

[What is Cyber Hygiene and Why is It Important?](#)

# The “Edge”

In the context of IT, "the edge" refers to the periphery of a network, where devices and data sources connect to the digital world, and where computing and storage resources are deployed close to the data source. The term "edge" signifies the farthest reaches of an organization's network, where things and people connect with the digital world.

*Some examples of edge devices:*

*Smartphones, Sensors, Industrial equipment, Tablets, Retail point-of-sale systems*

# BYOD

## Bring Your Own Device

The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.

*Popularized during the pandemic, it has created difficulties for IT teams to manage and properly secure such devices vs. those they procure and configure themselves.*

# Cybersecurity Strategies for Small Businesses



SCHOOL OF BUSINESS  
& ECONOMICS

CONCORDIA UNIVERSITY IRVINE

*Disclaimer: The guidance provided in this document reflects current best practices and insights into cybersecurity for small businesses. However, the cybersecurity landscape is dynamic and subject to constant change. Readers are encouraged to consult a qualified cybersecurity professional to tailor and implement strategies suited to their specific needs and circumstances.*