Confidence in the Connected World

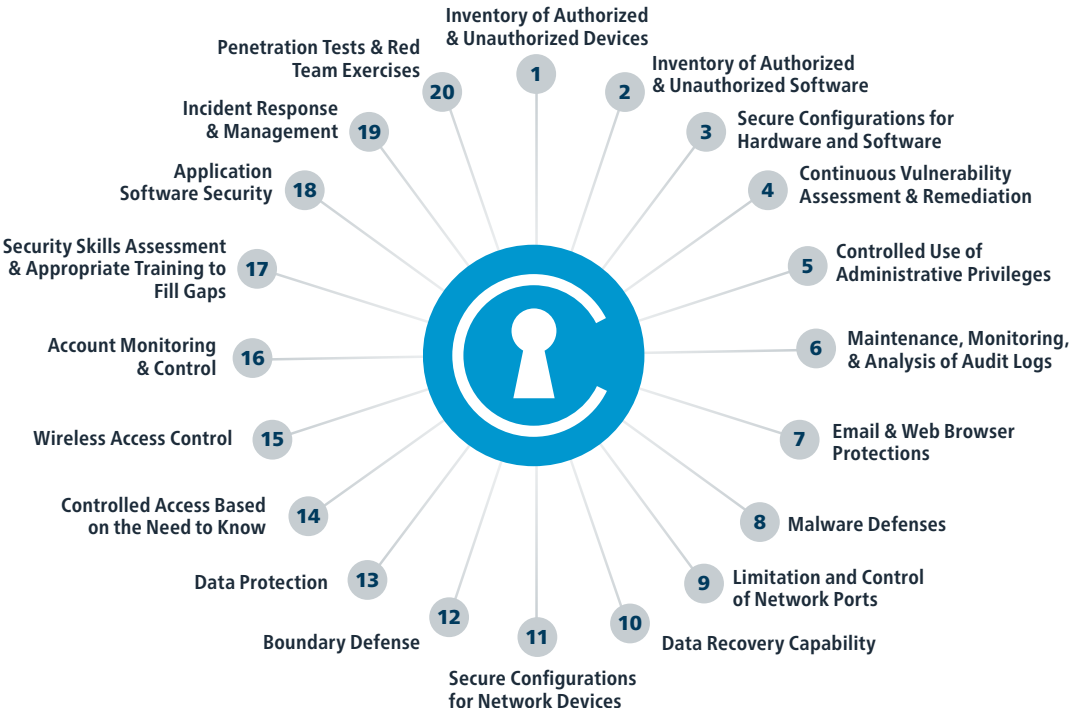
Center for Internet Security®

Contact Information:
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

CIS Controls

Implementation Guide

for Small- and Medium-Sized Enterprises (SMEs)



Confidence in the Connected World

Center for Internet Security®

CIS Controls

Contact Information:
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

CIS Controls Implementation Guide for SMEs

Contents

Introduction

Credit card breaches, identity theft, ransomware, 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 organizations with small budgets and limited staff respond to the continuing cyber problem? This guide seeks to empower the owners of small and medium-sized enterprises (SMEs) to help them protect their businesses with a small number of high priority actions based on the Center for Internet Security's Critical Security Controls (CIS Controls). The CIS Controls are a comprehensive set of cybersecurity best practices developed by IT experts that address the most common threats and vulnerabilities.

Some of the many concerns for SMEs include:

Theft of company information –
External hackers and dissatisfied employees steal company information and customer lists.

Website defacement –
Hackers corrupt your website to benefit competitors.

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

Ransomware –
Types of malicious software block access to a computer so that criminals can hold your data for ransom.

Data loss due to natural events and accidents.

This guide contains a small sub-set of the CIS Controls specifically selected to help protect SMEs. Since such resources change from time to time, please contact CIS or check out our website for the most recent information (www.cisecurity.org).

Overview

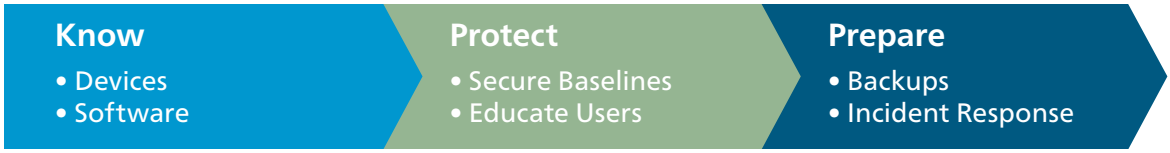
Security and good IT management go hand-in-hand: a well-managed network is more difficult to attack than a poorly managed one. To understand how well your organization is managing its cybersecurity, start by asking yourself these questions:

- Do you know what is connected to your computers and networks?
- Do you know what software is running on your systems and networks?
- 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 organization from cyber incidents?

To address each of these 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/no cost that any SME can leverage to improve its cybersecurity.

To help you prioritize your efforts, this Guide recommends using a phased approach. Phase 1 involves knowing what's on your network and understanding your cybersecurity baseline. Phase 2 focuses on protecting your security baseline through education and prevention. Phase 3 helps your organization to prepare in advance for disruptive events.

Each phase has specific questions that you will want to answer, along with action items and tools that will help you achieve your goals. You may want to assign one person in your organization to be the cybersecurity leader to report regularly on security activities.



Phase 1: Know your environment

The first step that will help you move forward with your cybersecurity efforts is to know your network, including your connected devices, critical data, and software. Without a clear understanding of what you have to protect, you'll have a hard time ensuring coverage of your cybersecurity efforts.

Here are a few key questions that are important to think about:

- Do you know what's connected to your network?
- Do you know what software is installed?
- Do you know if your administrators and users are using strong passwords?
- Do you know which online platforms are being used by your employees (i.e., work productivity or chat tools)?
- Do you know where your most important data is stored on your network?

Know what's connected to your environment

If your company data is lost, stolen, or corrupted, you could be put out of business. Accidents and natural events can potentially destroy the data you rely on for your business operations. Also, bad guys target data they can steal that has potential value to them. This could be external hackers or employees inside your company who want to steal your customers, credit card information, or intellectual property. Your network is the means to get the data they want to exploit.

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 information such as credit card and health information. Here are some examples of data you will want to identify and inventory:

- Credit card, banking, and financial information
- Personally identifiable information (PII), such as Social Security numbers, health information, usernames and passwords, home addresses, birth dates, etc.
- Customer lists, product lists, pricing, etc.
- Company trade secrets, formulas, methodologies, models, etc.

Know which devices are connected to your 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.

Phase 1: Know your environment *continued*

What you can do:

- If on a wireless network, check your router to see which devices are connected and password-protected by using strong encryption (WPA2).
- For larger networks, use a network scanner (commercial or open source) to identify all the devices on your network.
- Enable Dynamic Host Configuration Protocol (DHCP) logging on your networking devices to allow for easy tracking of all devices that have been on your network. (Consult your IT experts if you need assistance with this.)
- For smaller organizations, keep an inventory list of your hardware assets (computers, servers, laptops, printers, phones, etc.) and critical data on a spreadsheet, which you should update whenever there are new devices or data added.

Cost-effective solutions:

- **Nmap:** Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to your network (https://nmap.org/)
- **ZenMap:** Easy-to-use graphic user interface for Nmap (https://nmap.org/zenmap/)
- **Spiceworks:** Free IT inventory and asset management software to identify devices and software on your network (https://www.spiceworks.com/)

Know what software is on your systems

Managing software is a key component of both good IT management and effective cybersecurity. Rogue software within your environment can pose risks that must be mitigated, including legal liability for using unlicensed software. In addition, unpatched software is a common way for malware to infiltrate and attack your systems. By understanding what software is on your network, controlling individuals' ability to add software to your network, and protecting accounts with administrative privileges, you'll reduce both the likelihood and impact of cyber events.

What you can do:

- Create an inventory of applications that are running on your system and the web services or cloud solutions your organization uses:
  - Manually check the install/uninstall features of the operating system to get a list of software that has been installed on the system.
  - Periodically check to see what software is running on your systems using available inventory or auditing tools.
  - Check with your employees to identify which online services, such as online file-sharing platforms or HR systems, they are using as part of their job.

Phase 1: Know your environment *continued*

- Limit the number of individuals with administrator privileges to a very small number. Don't allow general users to function as administrators.
- Use unique strong passwords for administrative accounts since admins have the ability to make system changes. Provide instructions for employees on developing strong passwords.
- Ensure that system administrators use a separate non-administrative account for reading email, accessing the Internet, and composing documents.
- Develop a company process for downloading software to your network, and prevent the use of non-approved applications via application whitelisting tools like Applocker.

Cost-effective solutions:

- **Applocker:** Free Microsoft® Windows tool to identify and restrict the software that is allowed to run (https://technet.microsoft.com/en-us/library/dd759117(v=ws.11).aspx)
- **Netwrix:** Variety of free tools to identify information about administrative access on your systems (https://www.netwrix.com)
- **OpenAudIT:** Inventory applications and software on workstation servers and network devices (http://www.open-audit.org/)

Phase 2: Protect your assets

As the old business saying goes, employees are your most valuable asset and that is true when it comes to security. Protecting your information requires not only technological solutions, but also employee awareness to prevent accidentally damaging your systems. This phase will focus on both protecting your computers and educating your users on their role in cybersecurity.

Here are some questions you'll seek to answer:

- Do you set up your computers with security in mind?
- Does your network run up-to-date anti-malware software?
- Do you educate your users on cybersecurity best practices?

Configuring a secure baseline

Malware and malicious cyber actors take advantage of either insecure configurations or vulnerabilities in the applications that are running on the system. To protect your company, 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 security and anti-malware functions that may be built-in to your operating system to help secure your environment. Examples include Windows Device Guard, Bitlocker, and others mentioned below.

What you can do:

- Periodically run Microsoft® Baseline Security Analyzer to identify which patches are missing for Windows products and what configuration changes need to be made.
- Ensure that your browsers and all plugins are up-to-date. Consider using a browser that automatically updates itself, such as Google Chrome™ browser.
- Run up-to-date anti-malware software to protect systems from malware. Utilize cloud-based lookup capabilities to check for updates if your anti-malware product supports this.
- Limit the use of removable media (USBs, CDs, DVDs) to those with an approved business need.
- Deploy the Enhanced Mitigation Experience Toolkit (EMET) on Microsoft® Windows machines to protect against code-based vulnerabilities. (https://www.microsoft.com/en-us/download/details.aspx?id=50766)
- Require the use of multi-factor authentication 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 just passwords.
- Change default passwords for all applications, operating systems, routers, firewalls, wireless access points, printer/scanners, and other devices when adding them to the network.
- 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) to securely configure devices and applications.

Phase 2: Protect your assets *continued*

Cost-effective solutions:

- **Bitlocker:** Built-in encryption for Microsoft® Windows devices (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)
- **Microsoft Baseline Security Analyzer:** Free Microsoft® tool to understand how Windows computers can be securely configured (https://www.microsoft.com/en-us/download/details.aspx?id=7558)
- **CIS Benchmarks:** Free PDFs with consensus-based configuration guidelines for 100+ technologies.

Developing "cyber secure" behaviors

Cybersecurity is not just about technology; it is also about process and people. Having only security tools and software isn't sufficient. To help secure your organization, your employees and staff must also practice strong cybersecurity behaviors. There are two key considerations for "cyber securing" your staff: what you communicate and how you communicate.

What to communicate:

- Identify those within your organization who have access to or who 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 attack.
- Encourage the use of strong, unique pass-phrases for every account and/or two-step verification when possible.
- Require everyone to use "screen lock" on their mobile devices.
- Make sure all staff keep their devices and software updated and current.

Phase 2: Protect your assets *continued*

How to communicate:

- Engage your employees at an emotional level, making sure they understand how to protect your organization and how this protection also applies to their personal lives.
- Be sure all staff understand that cybersecurity is an important part of their job.
- Disseminate to your staff free cybersecurity awareness materials, such as the SANS OUCH! newsletter and MS-ISAC's monthly cyber-tip newsletters.
- Use online resources such as the National Cyber Security Alliance's StaySafeOnline.org.

Cost-effective solutions:

- SANS Ouch! Newsletter, Video of the Month, Daily Tips and Posters (http://securingthehuman.sans.org/ouch/archives)
- MS-ISAC Monthly Newsletters (https://msisac.cisecurity.org/newsletters/)
- Staysafeonline.com

Phase 3: Prepare your organization

Once your organization has developed a strong cybersecurity foundation, you should build your capabilities for response. This includes the ability to know how to handle a cybersecurity incident and how to get back to business.

Here are key questions for you to answer:

- Do you know the last time your critical files were backed up?
- Do you periodically verify that the backups are complete?
- Do you know who to contact if an incident occurs?

Managing backups

Making and managing backups can be a tedious task; however, it is one of the best ways to secure your data, recover after an incident, and get your business back in order. This is especially crucial considering that ransomware malware 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.

What you can do:

- Perform weekly backups of all computers that contain important information in an automated fashion. Consider using secure cloud solutions where available.
- Periodically test your backups by trying to restore a system using a backup.
- 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.

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 (http://blog.bacula.org/)

Phase 3: Prepare your organization *continued*

Preparing for an incident

No one wants a cybersecurity incident to happen, but the better prepared you are, the better position you'll be in to get your business back up and running. Cyber incidents include a denial-of-service 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.

What you can do to prepare:

- Identify those within your organization 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 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.

What to do if an incident occurs:

- Consider contacting an IT or cybersecurity consultant if the nature and extent of the incident isn'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.

Helpful Resources

CIS® (Center for Internet Security)
CIS is a forward-thinking nonprofit entity that harnesses the power of the global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls and CIS Benchmarks are global standards and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing & Analysis Center (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial governments. (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.(www.bbb.org/council/for-businesses/cybersecurity/)

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)

"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)

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)

SANS Institute
SANS is the largest source for information security training (https://www.sans.org/find-training/) and security certification (http://www.giac.org) 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 (https://isc.sans.edu/). Several documents address incident handling. (https://www.sans.org/reading-room/whitepapers/incident)

SANS also offers a cybersecurity glossary of terms. (https://www.sans.org/security-resources/glossary-of-terms/)

Helpful Resources *continued*

U.S. Chamber of Commerce
"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. (www.uschamber.com/issue-brief/internet-security-essentials-business-20)

U.S. Department of Homeland Security
"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. (www.us-cert.gov/ccubedvp/smb)

"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. (www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card_04.07.pdf)

U.S. Small Business Administration
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. (www.sba.gov/managing-business/cybersecurity)

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

Acknowledgments

The Center for Internet Security gratefully acknowledges the contributions provided by:

Hardeep Mehrotara, CISSP, CISA, GSEC, ISSMA, CICP

Lance Spitzner, Director, SANS Security Awareness

Russell Eubanks, ICS Handler, SANS Instructor

and other expert volunteers from the CIS Community for the content and editing of this guide.