A SIMPLE INTRODUCTION TO THE **18 CIS CONTROLS**

BARR ADVISORY

TABLE OF CONTENTS

INTRODUCTION

The cost of not having a comprehensive cybersecurity program could be detrimental to any organization, no matter its age or size. From now until 2025, cybercrime is expected to cost the world over **$10.5 trillion each year**, according to Cybercrime Magazine. Having a plan and set of security standards will not only protect your organization's data and sensitive information from being compromised, but also your customers' data.

The Center for Internet Security (CIS) recently released version eight of its controls, consolidating the 20 controls of previous versions. The CIS 18 Controls are now organized in a prioritized list by activity, rather than previously organized by who manages the devices.

DID YOU KNOW?

From now until 2025, cybercrime is expected to cost the world more than $10.5 trillion each year.

Source: Cybercrime Magazine

Version eight includes 18 controls—a set of standardized best practices to safeguard data and protect against cyberattacks. These controls establish a foundation on which organizations of all sizes can build, mature, and maintain solid cybersecurity programs.

Explore the 18 CIS Controls, why they are important, and how you can easily implement them into your cybersecurity program.

CONTROL 1:
INVENTORY AND CONTROL OF ENTERPRISE ASSETS

DESCRIPTION

Source: Center for Internet Security

“Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, and department for each asset, in addition to whether the asset has been approved to connect to the network. For mobile end-user devices, Mobile device management tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise’s network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.”

WHY IT'S IMPORTANT

Preventing unauthorized devices from gaining access to your network, systems, and sensitive data helps ensure the security of hardware devices and assets.

HOW TO IMPLEMENT THIS CONTROL

Maintain a spreadsheet in Microsoft Excel or Google Sheets of all hardware assets, including laptops, servers, firewalls, etc. Consider leveraging tools like Vanta, Asset Panda, Axonius, and Divvycloud to facilitate the management of hardware.

CONTROL 2:
INVENTORY AND CONTROL OF SOFTWARE ASSETS

DESCRIPTION

Source: Center for Internet Security

"Actively manage (e.g., inventory, track, and correct) all software (e.g., operating systems and applications) on the network so only authorized software is installed and executed, and unauthorized and unmanaged software is found and prevented from installation or execution."

WHY IT'S IMPORTANT

Cybercriminals target and scan vulnerable software that can be remotely exploited through easy-to-deploy applications or clickable links. All it takes is one click or vulnerable application and the whole network could be compromised.

HOW TO IMPLEMENT THIS CONTROL

Maintain a spreadsheet in Microsoft Excel or Google Sheets of all software, including software installed on endpoints, software installed on servers, and Software as a Service (SaaS) solutions. Consider a tool such as those mentioned in Control No. 1 to inventory, track, and manage software.

CONTROL 3:
DATA PROTECTION

DESCRIPTION

Source: Center for Internet Security

“Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.”

WHY IT'S IMPORTANT

It is critical to protect your organization’s data whether it resides within a corporate network or in the cloud. Data could include financial data, intellectual property, and customer data. Protection of customer data is even more important if international regulations and laws apply. It is critical for organizations to have processes and technical controls to manage data through its entire lifecycle, including retention, disposal, and encryption. Data should be protected based on its classification or sensitivity level and some data may require more stringent controls than others.

HOW TO IMPLEMENT THIS CONTROL

Document a data classification and handling policy in which sensitive information is defined. Policy should include, but is not limited to, limiting production data from non-production environments, encrypting workstations, etc.

CONTROL 4:
SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

DESCRIPTION

Source: Center for Internet Security

“Establish and maintain the secure configuration of enterprise assets (e.g., end-user devices, network devices, non-computing/IoT devices, and servers) and software (e.g., operating systems and applications).”

WHY IT'S IMPORTANT

Default configurations for devices, operating systems, and applications can be vulnerable in the original state when delivered from a seller or manufacturer. It’s critical to develop robust configuration settings with sound security properties to ensure the system and software are secure. Once initial configurations are implemented, it is critical to monitor and ensure those configurations do not drift from an organization’s hardening baseline.

HOW TO IMPLEMENT THIS CONTROL

Review your baseline hardening configurations against the CIS Benchmarks to ensure devices, operating systems, and software are hardened according to best practices. Consider leveraging tools to monitor and enforce policies on enterprise assets.

CONTROL 5:
ACCOUNT MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

"Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator and service accounts, to enterprise assets and software."

WHY IT'S IMPORTANT

It's much easier to gain unauthorized access to systems, data, and networks using valid credentials than through a traditional form of "hacking." Whether it's a weak password, dormant account, unchanged service account password, or a service account included in a script, using valid credentials is the easiest and most efficient way for an attacker to gain unauthorized access. Attackers will typically try to target administrative-level accounts, which places an even greater importance on these accounts.

HOW TO IMPLEMENT THIS CONTROL

Implement robust and centralized account management controls such as period account reviews, separate administrator accounts, and regular rotations of service and shared account passwords. Use strong and unique passwords, including multi-factor authentication (MFA) whenever possible.

CONTROL 6:
ACCESS CONTROL MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

“Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.”

WHY IT'S IMPORTANT

Some user activities, while required for consistent operation of the business, are inherently higher risk. As such, it is critical to ensure only authorized users can perform activities such as configuration changes to operating systems and applications, the ability to add, change, and remove users, and accessing sensitive data or applications. Ensuring these permissions are assigned based on role and have strict authentication controls is critical to protecting sensitive systems and data.

HOW TO IMPLEMENT THIS CONTROL

Implement role-based access controls, including provisioning processes to ensure user access permissions are assigned according to the least-privilege principle. Require multi-factor authentication for cloud services systems, remote network access, and administrator accounts.

CONTROL 7:
ESTABLISH SECURITY AWARENESS TRAINING

DESCRIPTION

Source: Center for Internet Security

"Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure in order to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information."

WHY IT'S IMPORTANT

Cybersecurity information is constantly evolving with new trends, software updates, security advisories, and more. It's critical to continue to stay abreast of new vulnerabilities because the attackers have access to the same information your organization does. As such, it is critical to have vulnerability scanning tools and procedures in place to identify, triage, track, and remediate as soon as possible.

HOW TO IMPLEMENT THIS CONTROL

Establish and maintain a vulnerability management process that includes both technical controls such as vulnerability scanners and procedures to remediate identified vulnerabilities. You should perform scans on both internal enterprise assets and externally-exposed assets, including software and applications. Perform automated patch management to applications and operating systems whenever possible.

CONTROL 8:
AUDIT LOG MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

"Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack."

WHY IT'S IMPORTANT

Log collections and analysis is critical to detect and prevent malicious activity on an organization's network and assets within. It's also imperative for incident response activities in the event of a breach. This includes logging both at the system level and to identify user-level events.

HOW TO IMPLEMENT THIS CONTROL

Establish a robust process to collect, analyze, retain, and alert on audit logs. Ensure logs include sources such as DNS queries, command-line, and URL request logs. Logging systems should be synchronized to a centralized time source. Your teams should also implement procedures to review audit logs when necessary or, in some cases, on a defined cadence (e.g., monthly, quarterly).

CONTROL 9:
EMAIL AND WEB BROWSER PROTECTIONS

DESCRIPTION

Source: Center for Internet Security

“Improve protections and detections of threats from email and web vectors, as there are opportunities for attackers to manipulate human behavior through direct engagement.”

WHY IT'S IMPORTANT

Web browsers and email services are one of the most prevalent vectors used by attackers to compromise systems, networks, and data. Users can be easily tricked into clicking a bad link, providing sensitive data, or disclosing credentials. Implementing as many automated protection mechanisms as possible helps users as they go about their daily activities and may not be focused on security 100% of the time.

HOW TO IMPLEMENT THIS CONTROL

There are many controls inherently designed into SaaS-based office products such as Google Workspace and Office 365. Review your configurations against the CIS Benchmarks to ensure your organization’s account is hardened. For example:

- Ensure personnel use only supported email and web browsers.
- Implement domain-based message authentication, reporting, and conformance (DMARC) to limit the exposure to spoofed or modified emails from valid domains.
- Implement filtering at both the network and DNS level.
- Consider leveraging a Mobile Device Management (MDM) solution to monitor and/or enforce your policies.

CONTROL 10:
MALWARE DEFENSES

DESCRIPTION

Source: Center for Internet Security

"Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets."

WHY IT'S IMPORTANT

Malware, including viruses or Trojans, are one of the most commonly used attacks. Cybercriminals use them to steal credentials, exfiltrate data, encrypt or destroy data, and more. At times, it's as easy as a user clicking a link, opening an attachment, installing an external drive, or software. As such, it's critical to install malware protection at strategic points within the network, and on servers and workstations within the organization.

HOW TO IMPLEMENT THIS CONTROL

Deploy and maintain anti-malware software on all company assets. You should also configure the software with automated signature updates and apply the appropriate anti-malware protections to removable media devices. Consider leveraging tools such as Mobile Device Management (MDM) to monitor and/or enforce configurations, patching, and antivirus software on machines.

CONTROL 11:
DATA RECOVERY

DESCRIPTION

Source: Center for Internet Security

"Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state."

WHY IT'S IMPORTANT

Availability of data is a critical aspect of the cybersecurity triad, particularly for cloud services such as SaaS providers. Whether you need to restore after a ransomware attack or an outage at the primary data center, it's important to have the ability to restore the data and systems required to achieve business objectives, comply with laws and regulations, and satisfy customer requirements.

HOW TO IMPLEMENT THIS CONTROL

Establish and maintain a formal data recovery process that includes automated backups, encryption for recovery data, and a multi-location data storage strategy. You should also periodically perform test restorations of recovery data.

CONTROL 12:
NETWORK INFRASTRUCTURE MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

"Establish, implement, and actively manage (e.g., track, report, correct) network devices in order to prevent attackers from exploiting vulnerable network services and access points.”

WHY IT'S IMPORTANT

Attackers can exploit flaws, gaps, and inconsistencies in devices such as firewalls, routers, and switches. Improper configuration of these devices gives attackers access to networks, the ability to redirect traffic on a network, intercept information in transmission, or use the network entrance to gain access to more sensitive systems and data. It’s crucial to protect both physical network devices and virtualized networks such as those in public clouds like AWS, GCP, and Azure.

HOW TO IMPLEMENT THIS CONTROL

Establish a baseline network security architecture and configuration standards. Continuously monitor your network infrastructure configurations to ensure they are up-to-date, in line with the company baseline requirements, and the CIS Benchmarks for each applicable network component.

CONTROL 13: NETWORK MONITORING AND DEFENSE

DESCRIPTION

Source: Center for Internet Security

“Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise’s network infrastructure and user base.”

WHY IT'S IMPORTANT

Boundary protection and network defense is just one part of a comprehensive network security strategy. Not only should you have robust firewall and prevention strategies in place, but also security incident monitoring solutions to alert security teams of instances when those defenses might fail. This does not mean you need to have your own security operations center (SOC), but it does mean you should have both automated tools and manual processes in place to identify, triage, evaluate, and resolve incidents.

HOW TO IMPLEMENT THIS CONTROL

Deploy centralized security event alerting using solutions such as a security information and event management (SIEM) tool or services provided by the major public cloud providers such as AWS CloudTrail and CloudWatch. You may not have the resources to implement everything, but start with the higher risk, more critically important systems and networks and continually improve as you move forward. Deploy network and host-based intrusion detection systems and supporting escalation processes to resolve alerts or events from these systems.

CONTROL 14: SECURITY AWARENESS AND SKILLS TRAINING

DESCRIPTION

Source: Center for Internet Security

“Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.”

WHY IT'S IMPORTANT

All personnel, no matter their job title or level, play a role in the success or failure of a cybersecurity program. Attackers are conscious of unwary users and can exploit any gaps or vulnerabilities within the organization. The vast majority of personnel at a given organization are not paid to focus on cybersecurity, so it’s critical to promote a culture of cybersecurity through a formal security awareness training program that fits each person’s role and skill level.

HOW TO IMPLEMENT THIS CONTROL

Formalize a security awareness training program to ensure all employees receive training when they are onboarded and on a periodic basis (e.g., annually). Employees should receive training on topics such as recognizing social engineering attacks, password security, data leak prevention, your organization’s security incident response and reporting procedures, and more.

CONTROL 15:
SERVICE PROVIDER MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

“Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise’s critical IT platforms or processes to ensure these providers are protecting those platforms and data appropriately."

WHY IT'S IMPORTANT

All service providers play a role in the success or failure of a cybersecurity program. Many recent breaches were the result of a failure at a third-party service provider who may or may not have had the appropriate security controls and mechanisms in place. Every service provider must be consistent with the enterprise’s security requirements.

HOW TO IMPLEMENT THIS CONTROL

Maintain a comprehensive inventory of your service providers. Risk rank them according to the services they provide, the type(s) of data they have access to, and the criticality to your organization. Evaluate them according to the risk ranking any time a new provider is onboarded and at least annually for higher risk providers.

CONTROL 16:
APPLICATION SOFTWARE SECURITY

DESCRIPTION

Source: Center for Internet Security

“Manage the security lifecycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.”

WHY IT'S IMPORTANT

Vulnerabilities such as poorly written code, coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions can exploit sensitive information. Attackers understand the most common weaknesses in applications and can easily exploit them if they exist. They use automated mechanisms to scan source code and identify weaknesses such as buffer overflows, SQL injection, cross-site scripting, click-jacking, and more.

HOW TO IMPLEMENT THIS CONTROL

Formalize your Software Development Lifecycle (SDLC) and document secure coding principles. The SDLC should include, but is not limited to, the following:

- Procedures to identify and address vulnerabilities in application source code.
- A process to handle third-party (e.g., open source) code vulnerabilities. Maintain an inventory of open source libraries and scan them for vulnerabilities. Apply patches as soon as they are published by the third party.
- Separate development, test, and staging environments from production.
- Train developers in application security concepts such as OWASP Top 10. Provide opportunities for open discussion of secure development and encourage developers to support each other in preventing insecure coding practices.
- Use static and dynamic analysis tools to help identify common vulnerabilities or insecure coding practice before production deployments.
- Perform application penetration testing any time a major system change occurs and at least annually.

CONTROL 17:
INCIDENT RESPONSE AND MANAGEMENT

DESCRIPTION

Source: Center for Internet Security

"Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack."

WHY IT'S IMPORTANT

As mentioned previously, it's critical to have automated mechanisms in place to both prevent and detect incidents, but what happens when those protections fail? This is when a robust incident response is required to mitigate and recover from the incident in accordance with laws and regulations, customer requirements, and business objectives.

HOW TO IMPLEMENT THIS CONTROL

Establish a formal incident response plan and procedures including, but not limited to, the following:

- Roles and responsibilities for incident response.
- Contact information for response teams, external parties, and even law enforcement bodies.
- Reporting and communication processes.
- Post-incident reviews, including root-cause analysis to identify how and why an incident occurred.
- Regularly review and test the incident response plan and capabilities using tabletop tests and documentation reviews.

CONTROL 18:
PENETRATION TESTING

DESCRIPTION

Source: Center for Internet Security

“Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (e.g., people, processes, and technology), and simulating the objectives and actions of an attacker.

WHY IT'S IMPORTANT

Independent penetration testing provides a unique, objective view of an organization’s cybersecurity protections. This type of insight is invaluable to preventing breaches and identifying weaknesses in cybersecurity posture. Layered with the vulnerability management practices mentioned previously, penetration testing provides a robust threat identification and prevention practice to protect an organization’s most valuable assets, including sensitive data, intellectual property, reputation, and more.

HOW TO IMPLEMENT THIS CONTROL

Establish a penetration testing program that includes both internal and external penetration testing, remediation procedures, and requirements for modifying security measures based on the results of the tests.

CONCLUSION

While the information for each control provided here is considered industry best practices, keep in mind every business is unique. Depending on your business needs and risk appetite, there are many different ways to approach and implement the 18 CIS Controls. Working with a cybersecurity partner can provide the expertise and confidence needed to ensure your organization is secured from top to bottom.

Contact us—we're here to help.

Brad Thies
Founder and President
BARR Advisory

Mitch Evans
Director
CISO Advisory

Larry Kinkaid
Senior Consultant
CISO Advisory

CISO Advisory Team

info@barradvisory.com
barradvisory.com/contact

ABOUT BARR ADVISORY

THE SECURITY YOU NEED. THE COMPLIANCE TO SUCCEED.

BARR Advisory is a cloud-based security and compliance solutions provider, specializing in cybersecurity consulting and compliance for Software as a Service (SaaS) companies. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

BARR'S VIRTUAL CISO SERVICES INCLUDE:

- Risk Assessment
- Policy & Procedure Documentation
- Security Project Management
- Security Questionnaire Responses
- Internal Audit Service
- Vendor Assessment
- Mappings to Various Frameworks
- Ongoing Virtual CISO Support

CONNECT WITH BARR

info@barradvisory.com

barradvisory.com/contact

With BARR, you can expect a partner on your path to security and compliance every step of the way.