Center for Internet Security

CIS Critical Security Controls

Practical Guidance for Implementing the Critical Security Controls *(V6)*

Understanding the CIS Critical Security Controls

In 2008, the Center for Internet Security's Critical Security Controls ("CIS Controls") were created as a collaboration between representatives from the U.S. government and private sector security research organizations. A set of practical defenses specifically targeted toward stopping cyber attacks, these proposed defenses were technical in nature and intended to define specific, practical steps an organization could take to stop the most common cyber threats from compromising their information systems. The CIS Controls were crafted to answer the frequent question: "Where should I start when I want to improve my cyber defenses?"

Setting Expectations for Organizations Implementing the Controls

Many organizations facing the current cybersecurity environment are overwhelmed by what we call the "Fog of More" – a constant stream of new information and problems. They are challenged by competing expert opinions, a noisy and fast-changing marketplace of potential solutions, and unclear or overwhelming regulatory and compliance requirements. The CIS Controls are designed to bring priority and focus to this daunting task, to harness the power of a large expert community to identify and support high-value practices and foundational steps, and to stop "admiring the problem."

The CIS Controls embrace the Pareto 80/20 Principle, the idea that taking just a small portion of *all* the security actions you could possibly take, yields a very large percentage of the benefit of taking *all* those possible actions.

While the CIS Controls are focused on technical action, the developers of the Controls recognized that many of these recommendations would force technical operational teams to change practices to improve both operational controls and security, re-evaluate their basic strategies for defense, and become more structured and disciplined in their activities. There is no "magic box" solution for security. Therefore, success with the CIS Controls (or any defensive program) depends on organizations developing and operating from a new comprehensive roadmap for improved cyber-defense.

When some organizations are introduced to the CIS Controls, they may become discouraged thinking that the Controls reflect too high a bar and are unachievable for their organization. In practice, this could not be further from the truth – however, successful implementation of the Controls will require many organizations to shift their mindset on security and how they approach IT operations and defense.

Information and the technology that supports it is now the lifeblood of every organization. No longer can employees be allowed to install software at random or travel with sensitive data in their pockets. It has been established that the cultural acceptance of changes needed to implement the technical controls is a necessary

prerequisite for success. This is probably the most significant obstacle most organizations need to overcome. In this regard, buy-in and reinforcement from senior management are essential.

It should be noted that many organizations have had success in implementing the Controls in a *phased approach*, tackling some controls and sub-controls early and implementing others according to a plan coordinated and approved by senior management. In addition, dividing the work of implementing the Controls among several individuals/teams has also proven to accelerate implementation progress. Organizations rarely implement every sub-control described in the CIS Controls (Version 6.0, for example, has 149 sub-controls). Most sub-controls are foundational to effective cyber defense, while others provide advice on advanced techniques (a new categorization guide for the Controls Version 6.0 will clarify this concept).

Organizations that have the strongest security are continuously reviewing and updating their cyber posture and monitoring their defenses in light of evolving threats and changing business practices. Organizations implementing the CIS Controls should assume that their efforts will take, on average, between one and three years to achieve an initial level of conformance with the most critical CIS Controls (i.e., the first five) and possibly up to five years of dedicated effort to successfully implement all or most of the Controls. Ultimately, the speed of implementation will largely depend on investments committed to the effort and the level of support from senior management.

General Guidance for Implementing the Controls

Organizations considering implementing the CIS Controls need to carefully plan how they will achieve better cyber hygiene. Most organizations will find that creating an organizational structure for the CIS Controls will help ensure the program's success. Some organizations may establish a "Governance, Risk, and Compliance (GRC)" program. Other successful tactics include assigning program managers to coordinate the many tasks involved with implementation of the CIS Controls by server administrators, workstation specialists, network engineers, software developers, and even professionals outside of Information Technology such as human resource specialists, trainers, and compliance officers.

It should be noted that many organizations may already be pursuing a security architecture using other security standards or regulations as its foundation. In many organizations security regimes such as the NIST Cybersecurity Framework, NIST guidelines, and the ISO 27000 series or regulations such as PCI DSS, HIPAA, NERC CIP, FISMA are already being used to define controls for defense. Pursing a standard such as NIST 800-53 does not preclude organizations from using the CIS Controls as an effective "on ramp" towards achieving additional standards. Mappings have been defined for the CIS Controls for all major security standards to show how implementing the Controls will help an organization prioritize their implementation of another standard.

Some organizations may believe the CIS Controls' uniquely technical and prescriptive approach to cybersecurity defense is beyond their resources. In reality, a phased implementation approach helps ensure the most significant benefits achieved by implementing the highest priority controls (i.e., the first five of the CIS Controls). In fact, implementation of asset inventory (CIS Controls 1 & 2) and standard configurations (Control 3) often results in overall cost savings for an enterprise as fewer systems and network administrators are required to manage the organization's cyber environment. The cost of implementing the CIS Controls will be proportionate to the size of the organization. Larger organizations may spend more overall resources for defense, but smaller organizations will likely spend a greater percentage of their budget on defense due to economies of scale. Organizations should realize that protecting an organization from cyber-attacks has become a necessary cost associated with using technology as a business tool in the Internet age.

There are a few practical considerations an organization should make when embarking on this journey. Keeping these suggestions in mind and building them into the program's plan will help to ensure its success. Specifically, an organization should:

- Make a formal, conscious top-level decision to make the CIS Controls part of the organization's standard for defense. Senior management and the Board of Directors should be on board for support and accountability.
- Assign a program manager who will be empowered and responsible for the implementation of the CIS Controls.
- Decide who will be responsible for the long-term sustainability of maintaining cyber defenses.
- Start with a gap analysis, assessment or audit of the current organization's state against the CIS Controls and develop an implementation plan scheduled with priority focus on the first five Controls.
- Document the long-term plan (3-5 years) for implementing cyber defenses that are not already a part of the entity's defensive strategy.
- Embed the definitions or goals of the CIS Controls into the organization's documented security policies to streamline their implementation.
- Ensure that internal and external auditors use the CIS Controls as a part of their benchmark for assessing the organization's security stance.
- Educate workforce members on the organization's security goals and enlist their help as a part of the long-term defense of the organization's data.

While there may be other steps that help improve an organization's chances of success, these considerations are a good starting point for structuring an organization's defensive program.

A Place to Start: Specific Guidance for Basic Cyber Hygiene

The first five CIS Critical Security Controls are often referred to as providing cybersecurity "hygiene," as a number of studies show that implementation of the first five controls provides an effective defense against the most common cyber-attacks (~80% of attacks). In an effort to help organizations practically implement the first five CIS Controls, the objectives of these Controls are plainly described below. These top-level objectives should be used when determining how the first five CIS Controls and their sub-controls will be implemented.

CSC 1 |Inventory of Authorized and Unauthorized Devices. The purpose of this Control is to help organizations define a baseline of what must be defended. Without an understanding of what devices and data are connected, they cannot be defended. Scanners (both active and passive) placed on the organization's network that can detect devices is the place to start. This inventory process should be as comprehensive as possible. After an organization has accurately inventoried their systems, the next step is to prevent unauthorized devices from joining a network – this is where implementation of network level authentication excels. The initial goal is not to prevent attackers from joining the network, as much as it is to understand what is on the network so it can be defended.

CSC 2 | Inventory of Authorized and Unauthorized Software. The purpose of this Control is to ensure that only authorized software is allowed to execute on an organization's information systems. While an inventory of software is important, the most crucial control an organization can implement here is application whitelisting, which limits the ability to run applications to only those which are explicitly approved. While not

a silver bullet for defense, this Control is often considered one of the most effective at preventing and detecting cyberattacks, although application whitelisting is often not easily implemented. This effort will require an organization to reconsider their operational models – no longer will users be able to install software whenever and wherever they like. But this Control, already successfully implemented by numerous organizations, will likely provide immediate returns to an organization attempting to prevent and detect specific attacks.

CSC 3 | Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. By default, most technology systems are installed with a focus on ease-of-use and not necessarily security. Systems may have the ability to be secured, but likely there are configurations a system must have in place in order to be highly secured. Most organizations already have the technology systems necessary to securely configure their systems at scale. Microsoft® Active Directory Group Policy Objects and Unix Puppet or Chef are commonly in place already in organizations. By utilizing configuration standards or benchmarks, such as those defined by the Center for Internet Security, or found in the NIST National Checklist Program Repository, this Control is achievable by most organizations.

CSC 4 | Continuous Vulnerability Assessment and Remediation. The goal of this Control is to understand the technical software weaknesses that exist in an organization's information systems and to remove or remediate those weaknesses. Successful organizations implement patch management systems that cover both operating system and third-party application vulnerabilities. This allows for the automatic, ongoing, and proactive installation of updates to address software vulnerabilities. In addition to patch management systems, organizations must implement a commercial vulnerability management system to give themselves the ability to detect where exploitable software weaknesses currently exist so they can be remediated.

CSC 5 | Controlled Use of Administrative Privileges. The purpose of this Control is to ensure that workforce members have only the system rights, privileges and permissions that they need in order to do their job - no more and no less than necessary. Unfortunately, for the sake of speed and convenience, many organizations allow staff to have local system or even domain administrator rights which are too generous and open the door for abuse, accidental or otherwise. The simple answer for this Control is to remove unnecessary system rights or permissions. Fortunately, for larger organizations struggling with doing this task at scale, there are privilege management vendors who can provide endpoint management solutions to help lessen the administrative burden.

The Future of the CIS Controls

The goal of the CIS Controls was to describe what organizations can do to effectively defend their information systems against the most common attacks and to provide a phased approach to implement a stronger cyber defense. The CIS Controls should be the yardstick for organizations trying to understand whether they have met a standard of defensive due care. The Controls will continue to evolve and change to reflect the most current threats facing information systems.

The Center for Internet Security (CIS) is a 501(c)(3) organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing & Analysis Center (MS-ISAC®), CIS Security Benchmarks, and CIS Critical Security Controls. To learn more, visit CISecurity.org and follow us on Twitter @CISecurity.

An effective cyber defense **is** achievable, with hard work and dedication. As we know, rarely do worthy rewards and accolades come easily. Organizations must assume that implementing and then maintaining these technical defenses will be an ongoing program, not a short-term project with a defined end date. As with any program, appropriate resources such as time, budgets, and people must be dedicated to the effort to ensure its success.

Current information about the CIS Controls as well as numerous working aids to assist in your implementation may be found at http://www.cisecurity.org.