Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(5):401-407**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Enhancing Cybersecurity with CIS Controls

Mohammed Mustafa Khan

Abstract: The field of cybersecurity is a growing concern for individuals, public, and private sectors. Cybersecurity professionals need to apply superior controls at different levels of IT infrastructure to protect against growing threats. Protecting servers, networks, and user workstations is crucial to safeguard against modern threats. Organizations ought to prioritize cyber defenses, but without a proper roadmap, they cannot shield their IT infrastructure. To help organizations strategize their security posture, the Center for Internet Security (CIS) controls come in. The CIS controls are a known set of cyber defense best practices that provide appropriate and formidable actions and approaches to shield against ubiquitous and malicious attacks worldwide. Keeping ahead of cybercriminals requires superior controls, expertise, and technology. Organizations do not need to start from scratch to defend their IT infrastructure. There is a shoulder to lean on that acts as a baseline to help organizations protect from common attack vectors, which is CIS controls. The paper discusses the CIS controls and how they can be properly implemented to protect a business's IT infrastructure against malicious attacks orchestrated by cybercriminals.

Keywords: CIS Controls, IT infrastructure, malicious attacks, security posture

1. Introduction

Investigations conducted after data breaches and security incidents show that the major causes of those incidences are well-known security controls and improper implementation of cyber defense best practices. Inadequate controls to govern the use of IT infrastructure to defend against real-world threats endanger the data, applications, and services of a business in today's digital economy where Cybercrime as a service is prevalent to infect the IT infrastructure to cause data breaches, theft of intellectual property, credit card/bank incidents, denial of services and other reasons [1]. This is putting a lot of pressure on IT and security teams to ensure their IT infrastructure follows security standards like the CIS controls to minimize risks. The CIS controls target to reduce or eliminate the IT infrastructure vulnerabilities that attackers exploit to gain access to the organizational data, applications, and services by setting up security controls that govern the use and implementation of IT infrastructure [3].

On average, it takes 280 days for some companies to detect and contain data breaches, according to the Ponemon Institute [2]. This is a long timeframe that allows cybercriminals to successfully carry out their malicious activities, imposing businesses to face detrimental effects such as loss of revenue, damages to business reputations, loss of intellectual property, and revoke or reclaiming of their operating licenses from regulatory bodies like HIPAA, PCI-DSS, GDPR and other bodies. It is a tremendous factor to incorporate a proper plan to secure the company's information and assets from cyberattacks by implementing CIS controls. The paper provides an overview of CIS controls, strategies for implementing them, the challenges that organizations face during the implementation of these controls, and ways to overcome the woes. Additionally, alignment of CIS Controls with other cybersecurity standards and the impact of CIS controls on compliance and regulatory requirements.

2. Overview of CIS Controls

Historical Background and Evolution of CIS Controls

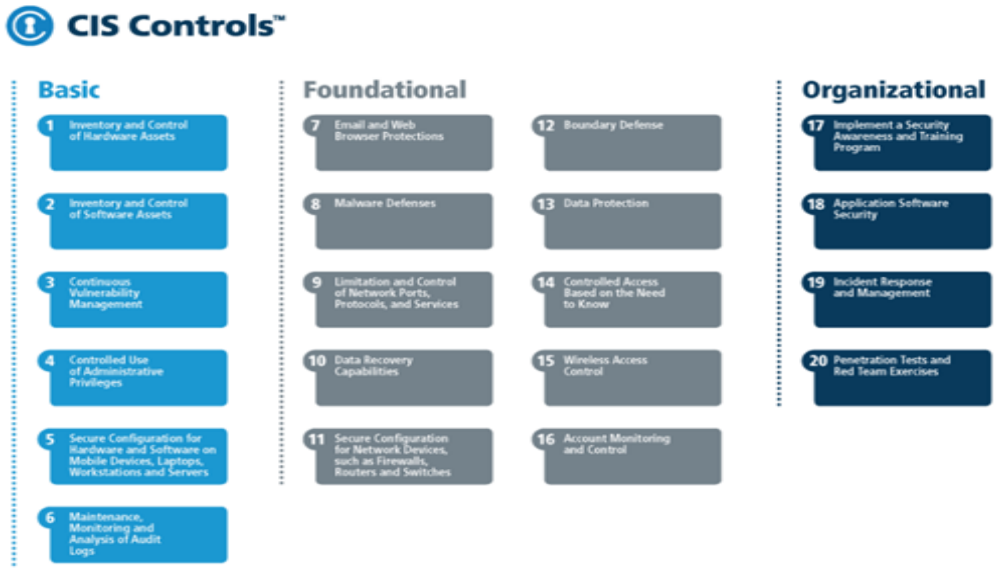
Several organizations experienced data breaches, and they were compelled to contract the U.S. Department of Defense (DoD), who asked the U.S. National Security Council and the SANS Institute to discover the appropriate security controls that will shield organizations defend against common attacks. The premier foundation of CIS Controls focused on a list of controls to combat possible major attacks.

In 2009, the first draft of the CIS Controls was published, and various security organizations and IT leaders, together with researchers, evaluated the draft and proposed their suggestions to be validated by the U.S. DoD [4]. After the validation of the draft, the implementation of the security controls took effect and made massive waves in minimizing the number of cyber attacks by identifying cyber vulnerabilities and remediating them before being exploited. In that period, the CIS Controls was known as the "Consensus Audit Guideline" since it was produced through brainstorming between a consortium of private and public sector organizations. In 2013, the ownership of CIS controls was transferred to the SANS Institute, which had 20 critical security controls, which was then transferred to the Council on Cyber Security (CCS). In 2015, the CCS was again transferred to its current name, the Center for Internet Security Controls [4]. The current version of CIS controls is v8, which was released on May 18, 2021. The v8 reduced the 20 controls to 18 controls to keep pace with the ever-changing cyber ecosystem.

Description of the CIS Controls

CIS Controls v7

The CIS controls v7 was classified into three major classes. The basis that was used to classify was dependent on their role in securing IT infrastructure. It classifies the CIS controls into three major classes: basic, foundational, and organizational [9]. The basic controls are regarded as being essential, the foundational controls offer additional defenses, and organizational controls center their actions on governance and policy.



Source: www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/

CIS Control V8

As businesses are shifting their data, workloads, and applications to clouds and hybrid platforms, virtualization, Bring Your Own Device policy, use of distributed systems, and remote work, among others, are exponentially growing, the CIS controls embraced these changes at an accelerated pace by boosting their controls to address modern threats to software and systems. The CIS control v8 was released as an ideal solution to address the emerging trends in cyberattacks [8]. The previous categories of CIS control v7 were scrapped to streamline the controls and align them with the current security practices needed to protect organizations against modern threats. The CIS Controlv8 adopted the implementation groups to address specific security functions and align them with modern cybersecurity frameworks [8]. The CIS 20 controls were reduced to 18 controls.

Implementation Groups (IG)

The CIS controls are segmented into three implementation groups (IG) that can be self-accessed by organizations. The IG1 is the least standard enterprise information security that describes basic cyber hygiene. The IG1 has 56 safeguards. The IG2 is built on the basis of IG1 and it offers clear security benefits. It is appropriate for organizations enriched with numerous resources and sensitive data. IG2 provides 74 safeguards. The IG3 controls is built on the aforementioned implementation groups to address the people and processes included in the cybersecurity function of an organization. IG3 fits an organization that deals with highly sensitive information where compliance is strictly needed. It adds 23 safeguards to the CIS control [8]. IG 3 utilizes advanced technologies such as vulnerability assessment and penetration testing to discover the advanced cyber threats such as web application hacking, insider, malware and ransomware. It requires skilled and experience cybersecurity professionals to carry out the vulnerability assessment and penetration testing. The purpose of these groups was to aid organizations in prioritizing CIS controls based on their size, resources, and level of risk. The resources are classified into various asset classes.

Organizations must strive to streamline their security programs to align with the 18 CIS controls to achieve optimal security posture. The table demonstrates a brief overview of each control and the IT infrastructure it protects.

CIS Control	Purpose
Control 1: Inventory and Control of Enterprise Assets	Ensure all hardware devices within the organization are accounted for and managed to prevent unauthorized and unmanaged devices from being used [8].
Control 2: Inventory and Control of Software Assets	Track and manage software installed on organizational devices. Ensure only authorized software is installed and unauthorized software is removed [8].
Control 3: Data Protection	Protect sensitive data through appropriate classification, handling, and encryption practices, preventing data breaches and unauthorized access [8].
Control 4: Secure Configuration of Enterprise Assets and Software	Establish and maintain secure configurations for all hardware and software, regularly reviewing and updating settings [8].
Control 5: Account Management	Manage the lifecycle of user accounts, including creation, modification, and deletion, with strict control over administrative privileges [8].
Control 6: Access Control Management	Implement policies and procedures to manage and limit access to networks and systems based on the principle of least privilege [8].
Control 7: Continuous Vulnerability Management	Regularly identify, prioritize, and remediate vulnerabilities to minimize the risk of exploitation by attackers [8].
Control 8: Audit Log Management	Collect, manage, and analyze logs from various systems and applications to detect and respond to incidents [8].
Control 9: Email and Web Browser Protections	Implement security controls for email and web browsers, such as filtering, anti-malware, and secure configurations [8].
Control 10: Malware Defenses	Deploy and manage anti-malware solutions across the organization, ensuring they are regularly updated and effective [8].
Control 11: Data Recovery	Ensure the ability to recover from data loss through regular backups and testing of recovery processes [8].
Control 12: Network Infrastructure Management	Secure the organization's network infrastructure, including routers, switches, and firewalls, through proper configuration and management [8].
Control 13: Security Awareness and Skills Training	Provide regular security awareness training to employees and ensure staff have the skills needed to protect against security threats [8].
Control 14: Service Provider Management	Manage and monitor third-party service providers to ensure they adhere to security standards and protect organizational data [8].
Control 15: Application Software Security	Develop secure software by integrating security practices into the development lifecycle to prevent vulnerabilities in applications [8].
Control 16: Incident Response Management	Establish and maintain an incident response plan to discover, respond to, and recover from security incidents [8].
Control 17: Penetration Testing	Regularly test the security posture through simulated attacks to identify security loopholes in people, processes, and technology and address vulnerabilities before exploitation by attackers [8].
Control 18: Security Incident Management	Monitor, detect, and respond to security incidents using tools and processes designed to mitigate and recover from attacks [8] quickly.

3. Strategies For Implementing Cis Controls

Organizations have invested millions of dollars in cybersecurity, but despite their huge investment, they still fall into the arms of cyber criminals. The most disturbing aspect is that some of the attacks would have been prevented by simply adopting strategies that ensure proper implementation of the CIS controls. So, what next is the organization supposed to do? The core factor organizations are supposed to employ getting facts right by embracing strategies that enable them to implement CIS Controls efficiently and effectively.

Implementation Groups

The current version of CIS control v8 has just simplified the 18 CIS controls and put them into three implementation groups to have clear visibility of the size, resources, and risk level of enterprises. Enterprises vary in size, the number of resources, and the assets they have, so the risk level definitely varies. Additionally, the implementation group was adopted to align with the modern threats [8]. For a clear overview of each implementation group, refer to the later sections of this paper, which were well explained. It is crucial to select the right implementation group and categorize an enterprise into the correct group so that appropriate and effective security controls are deployed to secure the IT infrastructure based on its resources and risk profile. After choosing the right implementation group, the following three-phased approach can guide the implementation team in successfully accomplishing their task.

Understand the Environment

Today's business enterprises have complex IT infrastructures that support their workflow operations. It is essential to know the network architecture of the organizations, including connected devices, software, and critical data, to mention a few, to ensure a comprehensive cybersecurity coverage of all the IT infrastructure [10]. For instance, a malicious insider can connect a rogue device driven by the personal gain to steal the credit card or banking details of a customer, intellectual property such as formulas for creating drugs if it is a pharmaceutical company and even corrupt the data. These incidents can put the organization out of business. Having a proper understanding of the devices connected to your environment and the applications installed makes management easier, and all devices will be protected using the controls.

Protect the assets

Employees are one of the assets that cannot be taken out of the equation since they may damage the systems unknowingly or intentionally. Protecting the information systems involves two factors: employee awareness and technological solutions [10]. It is crucial to protect the assets of organizations, like computers and tablets, and create advocacy programs that create awareness among users of the stake they have in matters related to cybersecurity. When setting up computers, it is important to ensure security by enforcing the password policy best practices and installing them with the updated anti-malware software. A secure baseline, like proper configurations of software applications, will minimize the vulnerabilities. Additionally, encryption of devices and information is implemented to enhance security.

Prepare the Organization

Once the organization has established an effective cybersecurity foundation, it is fundamental to build the capabilities for response. Cybersecurity incidents happen, and bouncing back to business depends on the preparedness of an organization. Organizations need to have a backup plan for their data. Ransomware is a detrimental attack that encrypts all your data, files, and applications and holds them for ransom [10]. Failure to pay the ransom means you lose all of your files and applications if no backup is implemented. It is important to perform regular backups and periodically evaluate if the backups are functioning by testing if the files, sytem, and applications can be restored. Additionally, backup can be offered by cloud vendors, and some companies specialize in backups such as Veeam and Commvault. Disaster recovery is key to ensuring business continuity in case of catastrophic cybersecurity incidences. Furthermore, in the case of cybersecurity incidents, it is recommended that the incident be reported to the legal authorities and that any affected person be notified about the data breach. Most organizations tend to ignore this aspect and end up endangering individuals' personal information.

4. Challenges and Solutions When Implementing the CIS Controls

Resource constraints

Organizations, specifically Small and Midsize Enterprises, lack adequate resources to implement all the 18 CIS controls [5]. Additionally, some organizations operate on a fixed budget, making it take a long time to implement the program; thus, they end up being caught by cyber criminals. The solution is to prioritize critical controls and outsource security functions to third-party providers. Additionally, maximize the use of open-source security software that can help to keep some CIS controls in check.

Complexity of Implementation

Due to the distributed nature of IT infrastructure, the implementation of CIS Controls can be complex and calls for adept comprehension of IT infrastructure and cybersecurity principles [5]. It is important to invest in training and development to impart knowledge and skills to the IT and security teams. Additionally, the IT administrators should work in tandem when implementing the CIS Controls.

Organizational Resistance

The implementation of the new version of CIS Controls may require some changes to processes and systems, leading to resistance. The solution to eliminate resistance is to communicate the benefits that can accrue with the new changes. Additionally, the involvement of all the stakeholders in the implementation process from the beginning to the end will boost the courage of each individual, thus increasing the rate of acceptance [5].

5. Alignment of CIS Controls with Other Cybersecurity Standards

The CIS Controls are designed to be compatible and operate seamlessly with other cybersecurity standards and frameworks like the NIST Cybersecurity Framework and the ISO/IEC 27001[7], [6]. This synergy enables organizations to incorporate CIS Controls into their underlying cybersecurity programs and accomplish compliance with different regulatory requirements. For instance, the NIST Cybersecurity Framework provides a high-level overview of cybersecurity posture across an organization, whereas the CIS Controls provide informative, formidable step-by-step instructions for optimizing security. Implementing the CIS Controls together with the NIST Framework is the game changer that helps organizations attain a comprehensive approach to cybersecurity that focuses on strategic and tactical objectives.

6. Impact of CIS Controls on Compliance and Regulatory Requirements

In addition to improving security, implementing CIS Controls can help organizations achieve compliance with various cybersecurity regulations and standards. Many regulatory bodies, such as the GDPR and HIPAA, require organizations to implement specific security measures to protect sensitive data [8]. The CIS Controls provide a clear, actionable framework for achieving these requirements, thus helping organizations avoid costly fines and reputational damage associated with non-compliance.

7. Conclusion

The Center for Internet Security (CIS) Controls are an essential component of any comprehensive cybersecurity strategy. By providing a prioritized set of actions, the controls help organizations improve their security posture. Despite the challenges associated with implementation, the benefits of the CIS Controls are clear. Organizations that have successfully implemented the controls have reported significant reductions in security incidents, improved compliance with regulatory requirements, and enhanced overall security. As cyber threats continue to emerge, organizations must remain cognizant, vigilant, and prescient in their approach to cybersecurity. The CIS Controls provide a proven framework for achieving this goal, offering organizations the tools and processes needed to protect their critical assets and ensure the confidentiality, integrity, and availability of their information.

Reference

[1]. HKCERT, “Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience,” www.hkcert.org, May 15, 2023. https://www.hkcert.org/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience

[2]. Ponemon Institute, “Home,” Ponemon Institute, Apr. 2023. https://www.ponemon.org/

[3]. S. Groš, "A Critical View on CIS Controls," IEEE Xplore, Jun. 01, 2021. https://ieeexplore.ieee.org/abstract/document/9495982

[4]. B. Shamma, "Implementing Cis Critical Security Controls for Organizations on a Low-Budget - ProQuest," www.proquest.com, Dec. 2018. https://search.proquest.com/openview/35c1afabcb51e016995318e859762f96/1?pq-origsite=gscholar&cbl=18750&diss=y

[5]. Hyperproof, "Unlocking the Power of the CIS Critical Security Controls®," Hyperproof, May 15, 2023. https://hyperproof.io/cis-security-controls-guide/
[6]. T. Sager, "CIS Controls v8 Mapping to ISO/IEC 27001:2022," CIS, Feb. 24, 2023. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec-27001-2022
[7]. T. Sager, "CIS Controls v8 Mapping to NIST CSF," CIS, May 18, 2021. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf
[8]. Center for Internet Security , "CIS Controls v8," CIS, May 18, 2021. https://www.cisecurity.org/insights/white-papers/cis-controls-v8
[9]. Center for Internet Security , "CIS ControlsTM V7 Poster," CIS, Sep. 10, 2018. https://www.cisecurity.org/insights/white-papers/cis-controls-v7-poster
[10]. Center for Internet Security , "CIS Controls SME Companion Guide," CIS, Sep. 12, 2019. https://www.cisecurity.org/insights/white-papers/cis-controls-sme-guide