DEVELOPMENT OF A DEFENSIVE CYBERSECURITY PROGRAM FOR PROACTIVE DEFENSES THROUGH STRUCTURED CYBERSECURITY FRAMEWORKS

This publication was produced at the request of the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

MODULE 4 - INTRODUCTION

A fact of doing business in today's hyper-internet-connected world is the need for organizations, regardless of size or sector, to protect their enterprises against a constant onslaught of malicious actors, insider threats, and a slew of other cybersecurity risks. It's more a matter of "when," not "if" your organization will face an attack.

Fortunately, cybersecurity frameworks have been developed that comprise best practices, standards, and guidelines designed to manage risks and combat these threats so you can protect your greatest assets: people, property and data.

Even if you are not mandated to adhere to any particular regulations, it still makes sense for your business to be proactive in managing risk. All frameworks include guidance for good cybersecurity hygiene, such as effective inventory and asset management, contingency planning, personnel security, system access control, and staff awareness and training, to list a few.

To prepare for the aftermath of a cyber incident, frameworks provide incident response guidelines you can follow to recover and try to limit the damage. Establishing a framework can not only help your organization follow best practices but also bring rigorous cyber discipline to your organization.

NIST VARIETY OF FRAMEWORK AND STANDARDS

NIST is a U.S. government agency that has developed several useful cybersecurity frameworks that represent the basis for most other frameworks. Detailed in special publications (SPs), these frameworks offer specific controls—best practices—that organizations in both the public and private sectors can follow to achieve the stated objective of the special publication.

NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (known as RMF) is built around seven steps: prepare, categorize, select, implement, assess, authorize, and monitor. This process helps organizations prioritize their risk management efforts by measuring, tracking, and identifying risks.

NIST SP 800-53, Security Privacy Controls for Information Systems and Organizations is a tried-and-true framework that focuses on privacy controls in recognition that privacy is a critical concern in the cybersecurity realm.

NIST SP 800-171, Protecting Controlled Unclassified Information in non-federal Systems and Organizations, focuses on assisting organizations that store, transfer, or transmit controlled unclassified information, referred to as CUI.[1] NIST 800-171's controls are aimed at helping non-federal organizations that do business with the federal government protect CUI confidentiality. These are good guidelines for any organization to follow to safeguard its own and its customers' data.

The NIST Cybersecurity Framework, known as CSF, centers on basic cyber defense functions that are required to determine risks and protect assets: identify, protect, detect, respond, and recover. It is designed to be customizable so that organizations can create a cyber security program that suits their individual risks, situations, and requirements. They can then prioritize their investment and maximize their spending on the most effective cybersecurity risk management.

IMPLEMENTING A FRAMEWORK

It can definitely be a daunting task to decide on a framework and then implement it effectively. Some firms may have the resources but could use help with interpreting the controls as they apply them to their organization. Other firms may need an outside expert to handle the whole process.

Third-party risk management firms can help in both situations by advising businesses on where to start and what frameworks make the most sense for them.

A keyway a risk management firm can help is by starting with a gap analysis. This evaluates your company's "as is" cybersecurity status and determines how to get to the "should be" status. The third-party experts will identify, quantify, and prioritize your organization's risks and weaknesses and suggest remediation steps to address them. This can include advising on the most appropriate framework that can best protect your organization's people, property and data and maximize your cybersecurity investment. Once a baseline is established and you address the gaps, you use the guidelines in your chosen framework to continuously measure your organization against this benchmark.

Given the complexity, artfulness, and range of cybercrimes that organizations face, it is important to use every available tool to combat these attacks. Adopting a proven cybersecurity framework that is suited to your business needs and risks gives you the tools to protect your enterprise against threats confronting you today and will continue to fend off tomorrow.

CRITICAL SECURITY CONTROLS FRAMEWORK

The major crux faced by IT security professionals across the industry today is that threats evolve at the same speed as technology. Technology is vital to business, especially as more professionals work outside the standard office environment, and that creates additional vulnerabilities.

The CIS Critical Security Controls framework is so widely used, that there are several different ways to reference them:

- CIS CSC
- CIS 20 / 18 (Newest Version)
- CCS CSC
- SANS Top 20
- CAG 20

The key to mitigating risk is having a solid security foundation on which to build industry or business specific security protocols. The CIS 18 Critical Security Controls (CSC) are that foundation.

WHAT ARE THE CIS CRITICAL SECURITY CONTROLS?

The CSC are a security foundation of actionable best practices developed by the Center for Internet Security (CIS) and the SANS Institute. Knowledge is garnered from a wide array of security professionals, condensed, and clarified by industry experts, and presented in a format that can be adapted by any organization to counter the leading forms of cyber-attack and protect data assets.

These basic principles allow IT professionals to respond swiftly and effectively against growing security concerns, which allows organizations to reduce cybersecurity risks.

HOW DO THE CIS CCS APPLY TO YOUR ORGANIZATION?

All organizations must navigate the deep and complex waters that are risk and compliance. Industry standards often define the specific dive level an organization must make into those murky depths, but they rarely indicate how. The CIS Critical Security Controls are a set of best practices that recommend how to combat the most common cybersecurity threats and are applicable to all organizations.

The CSC are broken into three implementation groups, each set of controls being a progression based upon an organization's needs:

- **Basic implementation** is applying controls 1 – 6 and is advised for all organizations. These six controls can be implemented with conservative resources and will provide a basic level of protection that even the smallest of organizations can utilize.

- **Foundational implementatio**n is applying the basic controls and controls 7 – 16 and is advised for mid-level organizations that have more resources and cybersecurity professionals to implement security measures.

- **Organizational implementation** is applying all 18 security controls and is intended for developed organizations that have rich resources and robust cybersecurity expertise.

By segmenting the controls into resource and expertise specific sections, an organization is given the option of choosing the best fit for their infrastructure.

WHY USE CIS CONTROLS FOR SECURITY AND COMPLIANCE?

The CIS top 18 Critical Security Controls are an evolution of worldwide knowledge from IT professionals that are arm-deep in security each and every day.

The results of using the CSC are phenomenal; studies have shown that 85% of cyberattacks can be thwarted by using just the basic implementation of CSC. Using the organizational implementation of all 18 Critical Security Controls has a staggering 97% success rate.

By using these outlined best practices, an organization will have a strong security base that has already proven its worth. A base that is perfect for building in any additional industry specific security requirements.

HOW DO THE CIS CRITICAL SECURITY CONTROLS WORK WITH OTHER STANDARDS?

The CSC are cross-compatible because they are effective best-practices that encompass a large threat range. Industry specific standards and security framework ideologies are growing and evolving with technology, and the CSC helps organizations keep up with the ever changing security environment.

For example, the California Consumer Privacy Act (CCPA) and General Data Protection Act (GDPR) require organizations to maintain reasonable security to protect consumers' private data. In addition, the IoT Cybersecurity Act requires connected devices to meet a minimum level of cybersecurity. Using the CIS Top 18 Critical Security Controls allows an organization to meet these thresholds.

Also, the CSC maps well to other well-known security standards:

- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Control Objectives for Information and Related Technologies (COBIT)
- Federal Information Security Modernization Act of 2014 (FISMA)
- NERC Critical Infrastructure Protection Standards (NERC CIP)
- Federal Financial Institutions Examinations Council (FFIEC)
- Department of Homeland Security Continuous Diagnostics and Mitigation (DHS CDM)
- National Security Agency Manageable Network Plan Guide (NSA MNP)
- Data Security and Protection Toolkit Standard (NHS DSP Toolkit)

The CSC are beneficial aids for organizations that need to meet these complex industry standards or regulations.

AN OVERVIEW OF THE CIS CONTROLS

Basic CIS Controls

The basic level of implementation is applying controls 1 – 6, and is considered the minimum amount of security that all organizations should use to be ready against cyber-attacks.

Control 1: Inventory and Control of Enterprise Assets

Knowing who and what is using the network is key to preventing unauthorized access. This includes maintaining a detailed inventory via both active and passive discovery and using access controls. An in-depth view of all the devices that use an organization's network provides a first line of defense.

Control 2: Inventory and Control of Software Assets

Software needs to be inventoried and monitored in a way that allows the organization to see what's been installed, who did the installing, and what the software is doing. Implementing authorization lists, installation rights, and integrity management are a must. Just like hardware assets, software can be used as a vulnerable point of entry into the protected network.

Control 3: Data Protection

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

Control 4: Secure Configuration of Enterprise Assets and Software

Update default configurations and automate processes that manage them. Configuration management is necessary to lock-down unnecessary risks that attackers can exploit.

Control 5: Account Management

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

Control 6: Access Control Management

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.

Foundational CIS Controls

The foundational level of implementation is also applying controls 7 – 18, and is considered appropriate for mid-level to large organizations that need to protect systems beyond basic needs.

Control 7: Continuous Vulnerability Management

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.

Control 8: Audit Log Management

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

Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

Control 10: Malware Defenses

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

Control 11: Data Recovery

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

Control 12: Network Infrastructure Management

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

Control 13: Network Monitoring and Defense

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.

Control 14: Security Awareness and Skills Training

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

Control 15: Service Provider Management

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.

Control 16: Application Software Security

Attackers using valid credentials is a concern that must be addressed. Two factor authentication and managing the account life cycle are common recommendations.

Control 17: Incident Response Management

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.

Control 18: Penetration Tests and Red Team Exercises

Identify points of breach and remediate as they are found. Keep testing and remediations evolving as the attack vectors change.

FREE ACTIVE DEFENSE TOOLS INTO THE WILD

Since now Governments and private companies are debating of the offensive approach to cyber security, the jump to the practice is short, a collection of open-source tools is becoming available in the public domain for private companies that decided to persecute intruders.

The "active defense" model is collecting many supporters within private industry and this is pushing a commercial offer that is proposed by specialized vendors such as CrowdStrike, HBGary and Mykonos.

The fundamental of active defense methods includes everything from honeypot-like tools to ensnare potential attackers and to track them. The capability to lure hackers studying their tactics is essential, on the defensive side there are various options, the company could directly attack the alleged criminals that menaces them, or they could choose to limit their active defense interfering with hackers, for example disturbing the attackers' reconnaissance activity and even pinpointing their physical location.

Dmitri Alperovitch, co-founder and CTO at CrowdStrike says that active defense includes activities to real-time detection of threats and identification of malicious agents, deception intelligence dissemination and destruction of attackers' systems as an extreme measure.

"Pure defensive techniques … cannot work when you're dealing with an adversary that's [advanced] and determined to get in, it will find a way in. So you need to find other ways to deter them. That's the premise behind active defense," Alperovitch says.

Another opportunity is to conduct intelligence activities on potential attackers trying to identify their way to act and the targets/information they use to refer. CrowdStrike security firm plans to release various tools for active defense, the company announced the distribution of analyzing and decoding polymorphic malware and free tools to monitor attackers' through Tor.

The market is very prolific, security experts, John Strand, Paul Asadoorian, Ethan Robish, and Benjamin Donnelly, offer a Linux distro set of tools for defense through offense.

ADHD is an active defense distribution with preconfigured strike back tools that could be used to interfere with an attacker's system fingerprinting.

The distro includes defense tools dubbed:

- *Artillery*

- *BearTrap—which opens "trigger" ports on a host to attract the hackers and automatically get spotted and blacklisted.*

- *Decloak to identify the real IP address of a Web user, even one behind a proxy.*

- *Honey Badger to pinpoint the physical location of an Internet user.*

- *Nova (Network Obfuscation and Virtualized Anti-Reconnaissance) detects network-based recon and feeds the attacker phony information on the numbers and types of systems on the targeted network, using a network of virtualized decoys. Nova doesn't use signature based detection for malware, instead it creates decoy systems for an attacker to interact with and alert the system administrator for suspicious activities.*

- *The Spidertrap is a set of web pages that may intentionally or unintentionally be used to cause a web crawler or search bot to make an infinite number of requests or cause a poorly constructed crawler to crash.*

- *Web Bug Server, embeds a Web bug inside a word processing document that can be used to a hide HTML code that ultimately reveals IP addresses and other information on the attacker.*

"We want to turn the tables without tripping into the realm of hacking back," Strand says. The expert argued legality of such tools sustaining that the offer is addressed to security experts that has clear idea of legal implication of their use. People "ask 'is it legal?' As near as we can tell it is,"

"We cannot go through the steps of getting on their computer or browsing their files even though they are bad guys or criminals. They have a right to privacy, and we try not to cross that line," Strand declared.

READING MATERIAL & LINKS

1. Module_4_Whitepaper1-LM-White-Paper-Intel-Driven-Defense

2. https://www.cisecurity.org/controls/

3. https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/

4. https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5/

5. https://www.cisecurity.org/white-papers/cis-controls-v8-cybersecurity-maturity-model-certification-mapping/