SANS

A SANS Spotlight

Back to Basics: Building a Foundation for Cyber Integrity

Written by **Barbara Filkins**

June 2018

Sponsored by:

Tripwire

Introduction

Applications depend on file-based architectures to process data and store content, as do the networks and endpoints that support these applications. Core operating system and application binaries, system and application configuration data, and network and security logs are also stored in files—placing *file integrity* at the heart of maintaining a secure cyber profile.

But cyber security must also protect *system integrity*. This refers to the state of the infrastructure (encompassing applications, endpoints and networks) where "intended functions are being performed without degradation or being impaired by other changes or disruptions to its environments."[1]

Risks to Cyber Integrity by Major File Types

File/Data Type	Risk
Configuration that determines how network, server, application and other assets should operate and authorize access	Authorized or unauthorized modification introduces unanticipated vulnerabilities that allow malicious compromise (e.g., ransomware attack)
Logs used to track actions and activities that take place across the operating system and applications	Attacker modifies log data/deletes log files to hide tracks
Content that stores business and other sensitive information	Attacker exfiltrates sensitive information for competitive advantage/financial gain

Cyber integrity builds upon these two concepts. It weaves people, processes and technology together into a holistic framework that guards the modern enterprise against changes, whether authorized or unauthorized, that weaken security and destabilize operations.

[1] The Law Dictionary, https://thelawdictionary.org/system-integrity

Building cyber integrity can be a significant effort. The Center for Internet Security's Critical Security Controls (a.k.a. the CIS Controls) provide a valuable, effective framework for establishing cyber integrity within an organization. Informed by real-world attacks and effective defenses, the controls presented in Figure 1 can be used to create a prioritized set of actions for establishing cyber integrity within an organization. This paper was developed to explain how to use selected controls to establish and maintain cyber integrity.

Focus on People, Process and Technology

Cyber integrity depends on a holistic approach to security. Technology does not stand alone—skilled staff and proven processes are needed to guard the modern enterprise against damaging interference, whether authorized or unauthorized. Table 1 presents the key controls related to establishing and maintaining cyber integrity.

Table 1. How Critical Security Controls Support Cyber Integrity

Category	Control Title(s)	Why It's So Important
Technology	**CIS Control #3: Continuous Vulnerability Management** **CIS Control #5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers** **CIS Control #11: Secure Configurations for Network Devices, such as Firewalls, Routers, and Switches**	• Implement integrated configuration/vulnerability management • Harden critical endpoint/network infrastructure against compromise • Monitor what is normal and remediate what's abnormal • Establish/maintain visibility into changes, whether legitimate or adversarial
People	**CIS Control #17: Implement a Security Awareness and Training Program**	• Develop awareness • Implement training • Maintain skills and competencies
Process	**CIS Control #6: Maintenance, Monitoring and Analysis of Audit Logs**	• Develop policy • Implement proactive change management • Formalize reviews, both for routine maintenance and identification of anomalies and abnormal events, and enforce/remediate

Basic CIS Controls

1. Inventory and Control of Hardware
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Assessment and Remediation
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Figure 1. The CIS Controls, Version 7[2]

Striding Toward Cyber Integrity

In order to establish a secure configuration baseline, you need to know your assets. The first step to establishing cyber integrity is to develop an asset inventory—a list of what you have. Think of inventory in terms of hardware (CIS Control #1: Inventory and Control of Hardware Assets) and software (CIS Control #2: Inventory and Control of Software Assets).

[2] Center for Internet Security, www.cisecurity.org/critical-controls.cfm

1. Establish the configuration baseline for your infrastructure.

Once you know your assets, the next step is understanding how they are configured. Use both CIS Controls #5 and #11 to help you develop your initial configuration baseline, which enables management of present, approved configurations; cataloging of approved exceptions; and alerting when unauthorized changes occur.

- Avoid the snowflake syndrome. That's an IT environment where no two endpoints are the same. The more unique systems that have to be managed in the infrastructure, the more difficult it is to secure the infrastructure, because each endpoint must be handled individually. Establish secure configurations for hardware and software on endpoints (CIS #5.1), and then maintain all endpoints based on those standards (CIS #5.2).
- Understand the network. Establish standard security configurations for network devices (CIS #11.1) and document traffic configuration rules (CIS #11.2).

2. Determine the critical files and processes you need to monitor your established baseline.

Use the Foundational controls (CIS Controls #7–16) to help you refine your monitoring requirements, especially in terms of the file types and the metrics associated with each type of file and process.

Key files can include:

- Endpoint master images
- Operating system binaries, libraries and directories, and paging files
- Application binaries, directories and files
- Web server directories
- Configuration files that define how network devices, endpoints and applications operate (note: Many times these files are typically read-only at service or application startup.)
- Log files containing transaction and activity history
- Digital keys and credentials
- Content files

Key processes include any that will touch these files (create, read, update or delete) as well as processes that involve logging and alerting, especially around the use of administrative privileges and the capture and maintenance of audit logs (CIS Control #6).

3. Document your static and dynamic configuration monitoring procedures.

Look to CIS Controls #3.1 and #3.2 for how to configure your automated scanning tools to detect all potential vulnerabilities, both static and dynamic:

- *Static monitoring* can range from the simple tracking of a file's time/date stamp against other network parameters to more rigorous methods, such as periodically comparing the current cryptographic checksum for a monitored file (e.g., using MD5 or SHA-2 hashing algorithms) against a previously calculated and validated checksum.

File integrity monitoring (FIM) is an internal control or process. FIM performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline. This approach is woven throughout the CIS Controls. However, organizations need to realize that FIM needs to encompass not just static changes in file structures, but also dynamic ones that can result from a user writing data to a file or an administrator changing its permissions.

- *Dynamic monitoring* provides real-time change notification, typically implemented within or as an extension to the kernel of the operating system that flags when a file is accessed or modified.

4. Implement continuous vulnerability monitoring.

Evaluate the scope of what you intend to include in your continuous monitoring program in order to develop an actionable approach and select the proper tools. Is the challenge meeting regulatory compliance demands (such as PCI DSS, NERC CIP-007 or NIST), protecting intellectual property, defending an infrastructure with lots of assets, or a combination of all three?

Follow the guidance provided by CIS Control #3 to ensure notification when suspicious activities take place on critical files or when authorized changes result in misconfigurations or situations exposing the organization to increased risk and compromise.

Your IT and security teams must work together to ensure cyber integrity.

Consider this: In most organizations, the IT team is responsible for configuration management, while the security team is responsible for vulnerability assessment. Look to see how these two teams can work together to ensure that cyber integrity is fully realized.

5. Establish formal change management processes to evaluate requests and track outcomes.

The goal of change management is to make changes in a planned, managed, systematic fashion, with the ability to recover if the change proves problematic. Organizations benefit from a culture of change that supports cyber integrity. Is there an established change control board (CCB) with representatives who have the power to act quickly on high-priority issues? Can the impact of change requests that affect the approved configuration baseline be captured by current or updated continuous monitoring procedures?

Assess whether change management problems exist that impede achieving cyber integrity. Does the organization use a risk-rating process to prioritize (and approve) the remediation of discovered vulnerabilities (Control #3.7)? Are there unapproved, non-process changes being implemented? Does the change management process result in a known, updated and approved configuration baseline? Is an inordinate amount of time during problem resolution spent in determining the exact location and nature of the problem? Does the organization suffer from snowflake syndrome?

Start tracking how much time IT and security teams currently spend in troubleshooting. Ask the teams to document "unplanned" work. Recheck periodically as your organization improves its cyber integrity profile. The time needed for "unplanned" work should decrease, demonstrating a clear benefit to the organization in improved allocation of valuable staff resources.

6. Establish training for your staff.

CIS Control #18 provides guidance on how to focus the necessary training and awareness around cyber integrity:

- Perform a gap analysis to understand the skills and behaviors needed for workforce members to adhere to cyber integrity, then use this information to build your baseline education and training road map.
- Deliver training to address the skills gap identified to positively affect workforce members' security behavior around cyber integrity.
- Create an awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the cyber integrity of the organization.

Summary

Establishing and maintaining cyber integrity can be a daunting task. Using a pragmatic approach like the CIS Controls makes it easier, because the concept of cyber integrity is actually woven throughout the entire set of controls. For that reason, consider the CIS Controls a "force multiplier" in establishing your approach to cyber integrity governance that encompasses processes and people as well as technology, following the steps outlined in this paper:

1. Establish the configuration baseline for your infrastructure.
2. Determine the key files and processes you need to monitor your established baseline.
3. Document your static and dynamic configuration monitoring procedures.
4. Implement continuous vulnerability monitoring.
5. Establish formal change management processes to evaluate requests and track outcomes.
6. Establish training for your staff.

Additionally, make plans to continually measure and improve cyber integrity's value to the business through reduced risk and improved cyber hygiene, such as using the defined measures and metrics for CIS Controls V7. When done right, cyber integrity will improve security and reduce unplanned work for IT operations.

About the Author

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

SANS would like to thank this paper's sponsor: