CIS Assessment

Presented by: Jason Winder

An Aerstone™ White Paper

I. Introduction

The 2016 California Data Breach Report presented an analysis of the full set of reported breaches in the state between 2012 and 2015. One of the recommendations that came out of this report was the specific use of the Center for Internet Security (CIS) Critical Security Controls, which are deemed to comply with California's information security statute. This statute specifically requires businesses to use "reasonable security procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure." While California is clearly leading the country in cybersecurity legislation, it seems likely that other states will soon follow suit. It behooves all organizations, both public and private, to consider the CIS Critical Security Controls as part of an overall cyberdefense program. This paper addresses the notion of threats and risks, provides background on the CIS Critical Security Controls and CIS Benchmarks, defines the process for compliance and assessment, and presents lessons learned from Aerstone's experience as a CIS assessor.

"WHILE THERE IS NO PERFECT SECURITY, ORGANIZATIONS HAVE A RESPONSIBILITY TO PROTECT PERSONAL INFORMATION."

2016 California Data Breach Report

II. Threats and Risks

In the assessment of cybersecurity posture, it's incredibly important to differentiate between a threat and a risk. Threats encompasses the full set of events that *might* occur – including a cyber intrusion, a malicious insider attack, an earthquake, or an alien space invasion. Some of these occurrences may be considered more likely to occur, and some are less likely to occur. The chance of a specific event *actually* occurring is the risk of that event, which is of course dependent on the presence of a facilitating vulnerability. It has been shown time and time again that human beings tend to overestimate the risk associated with threats they are familiar with, or which happened to occur in the past, and grossly underestimate the risk associated with threats that they are not familiar with. This backdrop requires a very methodical and thoughtful evaluation

of risk, starting with the potential loss to the organization if a specific event were to occur. It's also clear that some internal systems are more important than others – i.e., that a loss in confidentiality, integrity, or availability of a given system may have a lesser or greater effect on the organization's ability to operate. And it's equally clear that mitigating security controls may overlap, and attack surfaces may change over time – all of which requires a comprehensive, ongoing, and mature approach to risk assessment.

III. The Center for Internet Security

About CIS

CIS is a not-for-profit organization "dedicated to enhancing the cybersecurity readiness and response among public and private sector entities." CIS partners with industry and government to fight evolving cybersecurity challenges, and helps organizations (public and private) adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls.

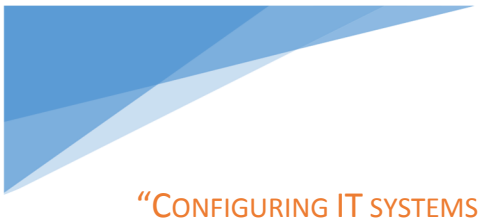
The CIS mission is threefold:

- Identify, develop, validate, promote, and sustain best practices in cybersecurity
- Deliver world-class security solutions to prevent and rapidly respond to cyber incidents
- Build and lead communities to enable an environment of trust in cyberspace.

CIS Security Benchmarks

The **CIS Security Benchmarks** program delivers a set of well-defined and consensus-based industry best practices to help organizations assess and improve their security. Key resources delivered by this program include secure configuration benchmarks, automated configuration assessment tools and content, security metrics, and security software product certifications.

The CIS Security Benchmarks themselves, available free of charge, are a set of technical controls recommended for hardening operating systems, software applications, and network devices. At the time of this writing, CIS had published benchmark guidance for 131 systems and applications, with more regularly being added – including operating systems and software applications for a wide variety of UNIX, Windows, and mobile platforms. CIS Benchmarks are commonly used by organizations as system hardening standards, with an eye towards meeting compliance requirements for FISMA, PCI, HIPAA, and other security requirements. For CIS Security Benchmarks members, CIS also makes available a number of additional resources, including The "CIS-CAT" configuration assessment tool, pre-hardened virtual AWS Amazon Machine Images (AMIs), Word/Excel versions of the CIS Benchmarks, and automated remediation kits for implementing and assessing Benchmark guidance.



"CONFIGURING IT SYSTEMS IN COMPLIANCE WITH CIS BENCHMARKS HAS BEEN SHOWN TO ELIMINATE 80-95% OF KNOWN SECURITY VULNERABILITIES."

Center for Internet Security

CIS Critical Security Controls

The **CIS Critical Security Controls for Effective Cyber Defense** ("the Controls"), formerly known as the SANS Top 20, are a recommended set of 20 security measures that are considered the "priority actions" that may be considered the starting point for an organization's security program. SANS describes them as "the prioritized guidance that cost-conscious executives are looking for when determining where best to invest their limited technology budgets." Driven by lessons learned from actual attacks and breaches, the Controls are a consensus list of the ways to detect, prevent, respond to, and mitigate damage from cyberattacks. They are updated periodically to keep up with technological advances and changing threats, and are aligned with the most authoritative comprehensive security standards and legal requirements. CIS provides specific guidance and resources for implementing the Controls, each of which is presented with an explanation of why it is critical.

Each Control is followed by a set of detailed sub-controls that address one element of the Control, along with procedures and tools for proper implementation. CIS also provides real-world metrics for each sub-control, in the form of a range of acceptable values that provide reasonable compliance thresholds based on the risk profile of the system, as well as a set of "effectiveness tests" that provide practical compliance guidance to IT managers, cybersecurity practitioners, and assessors. The full set of controls ultimately support what CIS believes to be the five critical tenets of an effective cyberdefense system: "offense informs defense," prioritization, metrics, continuous monitoring, and automation.

The Five Critical Tenets of Effective Cyberdefense

Offense Informs Defense

Practical defenses can only be built from the knowledge of actual and likely threats

Prioritization

The greatest risks from the most devastating attacks should be mitigated first

Metrics

Metrics are essential to gauge program effectiveness and to communicate risk

Continuous Monitoring

Continues measurement and assessment of system effectiveness must drive planning

Automation

Automating system defenses helps solution scalability and reliability

The full set of Controls themselves (as shown in Table 1) are designed to be implementable and scalable, and are intended to apply to organizations of all sizes. Organizations can implement the controls by adopting the sub-controls that fit the complexity and criticality of their systems, as well as the nature of their data.

Table 1 – CIS Critical Security Controls

Control	Description
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

IV. CIS Compliance and Assessment

The goal of complying with CIS standards can be arduous, but like most processes, becomes more straightforward with a clear and proven approach. Complying with CIS Benchmarks and CIS Security Controls are really two different processes, with overlapping goals and some efforts in common.

CIS Security Control Compliance

The first step in CIS Security Control compliance is to perform a full audit of all systems in the environment. For this purpose, a system may be defined as a collection of hardware and software that performs a specific function (or collection of related functions) in the organization. These systems might be used longitudinally across the organization by all employees (e.g., email or

phones) or used by a small subset of users to enable specific support or operational functions (e.g., finance or shipping). Once inventoried, these systems should be ranked in order of criticality – specifically, the impact to the organization based on a loss of confidentiality, integrity, or availability. Organizations (even private companies) are encouraged to reference FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," which is the document used by the federal government to guide this process. Notice that the CIS Security Controls leverage the exact same nomenclature as used in this document.

This categorization process results in an assignment of either "Low," "Moderate," or "High" for each system, which in turn drives the appropriate settings and goals for each control. Noting that security comes with a cost, higher categorized systems will ultimately have a more stringent set of controls applied than lower categorized systems. This approach helps ensure a positive return on security investment (ROSI). Note further that controls often include a combination of both technical and policy requirements, which helps underscore the importance of sound cybersecurity processes and procedures. In an audit, assessors will review system categorization, and look for evidence to confirm the implementation of the guidance associated with each applicable control; evidence will usually include a combination of policy documents, interviews, and screenshots of technical settings. Any controls that have not been implemented should be documented in a "plans of action and milestones" (POA&Ms) document, which delineates each missing control, along with an actionable plan for remediation.

CIS Benchmark Compliance

Whereas the process of complying with CIS Security Controls results in overall system security posture, the process of complying with CIS Benchmarks results in actual system component hardening. The system categorization should be used to prioritize achieving benchmark compliance, starting with the "high" systems first, followed by "moderate" and "low" systems. Subject matter experts for each system should work to identify the full set of hardware, software, and operating systems used for each solution, then download and peruse the actual Benchmark instructions for each system component. These Benchmark documents represent hardening instructions, including default values, remediation instructions, an impact assessment, and

auditing instructions. Auditors may use a combination of scripts, tools, and visual inspection to validate compliance. This process is not dissimilar to the Defense Information Systems Agency's "Security Technical Implementation Guide" (STIG) process; in fact, the technical guidance between CIS Benchmarks and STIG instructions are in many cases identical.

V. Lessons Learned

Compliance with CIS benchmarks and security controls are not just a legal imperative in some jurisdictions; CIS compliance makes your organization more secure, and allows faster recovery from cyber intrusions. In any jurisdiction, CIS compliance is a meaningful step towards meeting the benchmark of "reasonable care" in protecting personal. The following lessons learned are offered:

"THE FAILURE TO IMPLEMENT ALL THE CONTROLS THAT APPLY TO AN ORGANIZATION'S ENVIRONMENT CONSTITUTES A LACK OF REASONABLE SECURITY."

2016 California Data Breach Report

Security mindset drives security compliance

Policies must be written, approved, championed, and enforced in order to achieve the desired security posture across an organization. If the company leadership doesn't care, employees will not care either.

Third party confirmation is better than doing it yourself

Auditors understandably prefer assessment results produced by someone *other* than the system owners and implementers.

Style is just as important to the auditors as substance

Although perhaps somewhat trite, repeat experience has confirmed this without room for doubt or compromise. System auditors dramatically prefer "paperwork" (security assessment reports,

control documentation, and penetration testing reports) that looks and feels familiar. How information is presented is just as important as the information itself.

Perfection isn't the required standard

Most systems have failed controls, particularly in their first assessments or audits. This isn't a problem. Correctly documenting any failures, and showing the intent to mitigate in a plan of actions and milestones (POA&Ms) will cover most sins – at least long enough to resolve any real issues.

Moving into the cloud both helps and hurts

By moving systems into the cloud, organizations can inherit many security controls provided by the cloud service provider (CSP). That said, ensuring proper documentation of the CSP provided controls *and* the controls provided by the entity itself is challenging.

Most real problems come from poor configuration management

Regardless of the access control family, most problems have configuration management issues at their root. This includes issues like build control, patching, and change management. After the system security plan, the next most important document is the configuration management plan.

Don't try to be clever!

While there are always work-around options, these paths will invariably prove more cumbersome and time-consuming than implementing the controls as envisioned and intended. The audit exception process exists for a series of good reasons, but it is never the preferred route to compliance.

VI. For More Information

Contact info@aerstone.com to schedule a free CIS Critical Security Controls or CIS Benchmarks compliance consultation – or visit us on the web at www.aerstone.com.

VII. References

1. The 2016 California Data Breach Report
   https://oag.ca.gov/breachreport2016
2. Center for Internet Security (CIS)
   https://www.cisecurity.org
3. CIS Benchmarks
   https://benchmarks.cisecurity.org/downloads/index.cfm
4. CIS Critical Security Controls
   http://www.cisecurity.org/critical-controls.cfm
5. FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems"
   http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf