The CIS Critical Security Controls

for

Effective Cyber Defense

Version 6.1

Center for Internet Security®

The Center for Internet Security
Critical Security Controls for Effective Cyber Defense
Version 6.1
August 31, 2016

The CIS Critical Security Controls for Effective Cyber Defense

Introduction	**1**
CSC 1: Inventory of Authorized and Unauthorized Devices	**6**
CSC 2: Inventory of Authorized and Unauthorized Software	**10**
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**13**
CSC 4: Continuous Vulnerability Assessment and Remediation	**17**
CSC 5: Controlled Use of Administrative Privileges	**21**
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	**24**
CSC 7: Email and Web Browser Protections	**27**
CSC 8: Malware Defenses	**31**
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	**34**
CSC 10: Data Recovery Capability	**36**
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**38**
CSC 12: Boundary Defense	**41**
CSC 13: Data Protection	**46**
CSC 14: Controlled Access Based on the Need to Know	**50**
CSC 15: Wireless Access Control	**53**
CSC 16: Account Monitoring and Control	**56**
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	**59**
CSC 18: Application Software Security	**63**
CSC 19: Incident Response and Management	**66**
CSC 20: Penetration Tests and Red Team Exercises	**69**
Appendix A: Evolving An Attack Model for the CIS Critical Security Controls.	**73**

Appendix B: Attack Types **76**

Appendix C: The NIST Framework for Improving Critical Infrastructure Cybersecurity **78**

Appendix D: The National Cyber Hygiene Campaign **80**

Appendix E: Critical Governance Controls and the CIS Critical Security Controls **81**

Appendix F: Toward A Privacy Impact Assessment (PIA) for the CIS Critical Security Controls **85**

Appendix G: Categorization for the CIS Critical Security Controls **91**

Introduction

We are at a fascinating point in the evolution of what we now call cyber defense. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life for all of us in cyberspace.

Ironically, as defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. To help us understand the threat, we've seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure.

But all of this technology, information, and oversight has become a veritable "Fog of More": competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

So how can we as a community – the community-at-large, as well as within industries, sectors, partnerships, and coalitions – band together to establish priority of action, support each other, and keep our knowledge and technology current in the face of a rapidly evolving problem and an apparently infinite number of possible solutions? What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program? Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals, and guidance to measure and improve? Which defensive steps have the greatest value?

These are the kinds of issues that led to and now drive the CIS Critical Security Controls. They started as a grass-roots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. And **value** here is determined by knowledge and data – the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Led by the Center for Internet Security (CIS), the CIS Critical Security Controls ("the Controls") have been matured by an international community of individuals and institutions that:

- share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- document stories of adoption and share tools to solve problems;
- track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- map the Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- share tools, working aids, and translations; and
- identify common problems (like initial assessment and implementation roadmaps) and solve them as a community instead of alone.

These activities ensure that the Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

> The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.
>
> For additional information, go to <http://www.cisecurity.org/>

Why the CIS Critical Security Controls Work: Methodology and Contributors

The CIS Critical Security Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to evolve the consensus list of Controls, representing the best defensive techniques to prevent or track them. This ensures that the Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defenses identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defense and response capability that can be maintained and improved.

The five critical tenets of an effective cyber defense system as reflected in the CIS Critical Security Controls are:

Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

How to Get Started

The CIS Critical Security Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "what should my enterprise do" to "what should we ALL be doing" to improve security across a broad scale.

But this is not a one-size-fits-all solution, in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversary actions that could impact your ability to be successful in the business or operations. Even a relatively small number of Controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.

Controls CSC 1 through CSC 5 are essential to success and should be considered among the very first things to be done. We refer to these as "Foundational Cyber Hygiene" – the basic things that you must do to create a strong foundation for your defense. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program, one of the partners in the CIS Critical Security Controls. A similar approach is recommended by our partners in the Australian Signals Directorate (ASD) with their "Top Four Strategies to

Mitigate Targeted Intrusions"[1] – a well-regarded and demonstrably effective set of cyber-defense actions that map very closely into the CIS Critical Security Controls. This also closely corresponds to the message of the US CERT (Computer Emergency Readiness Team).

For a plain-language, accessible, and low-cost approach to these ideas, consider the Center for Internet Security's "National Cyber Hygiene Campaign". (Appendix D and www.cisecurity.org)

This Version of the CIS Critical Security Controls

The Controls were developed based on specific knowledge of the threat environment as well as the current technologies in the marketplace upon which our communications and data rely. One of the key benefits of the Controls is that they are not static; they are updated regularly and are tailored to address the security issues of the day. This version of the Controls reflects deliberation and consideration to ensure that every control and sub-control is accurate, essential, concise and relevant.

Changes from version 5.1 to Version 6.0 include the following:

- Re-ordering so that "Controlled Use of Administrative Privileges" is higher in priority (it moved from Control #12 to Controls #5)
- Deletion of Control #19 "Secure Network Engineering"
- New Control # 7 "Email and Web Browser Protections"
- New categorization scheme based on "families" of Controls and removal of the "quick win" categories.
- Each sub-Control is grouped into one of three Families:
  - System
  - Network
  - Application
- New appendices on the NIST Cybersecurity Framework, the National Hygiene Campaign for Cyber Hygiene and security governance.

Changes from Version 6.0 to Version 6.1 include the following:

- Each sub-Control is identified as either "Foundational" or "Advanced" as an aid to prioritization and planning. This replaces the original scheme found in Version 5 but dropped in Version 6.0. See Appendix G for a detailed explanation.
- Correction of a few minor typos or formatting errors.
- No change was made to the wording or ordering of any Control or sub-Control.

[1] http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

In addition to technical content, the Controls have a new home and new name. In 2015, the Center for Internet Security integrated with the Council on Cybersecurity, so they are now referred to as the "CIS Critical Security Controls."

Other Resources

The true power of the Controls is not about creating the best list of things to do, it's about harnessing the experience of a community of individuals and enterprises that make security improvements through prioritization, sharing ideas, and collective action.

To support this, the Center for Internet Security acts as a catalyst and clearinghouse to help us all learn from each other. Please contact the Center for Internet Security for the following kinds of working aids and other support materials:

- Mappings from the Controls to a very wide variety for formal Risk Management Frameworks (like FISMA, ISO, etc.).
- Use Cases of enterprise adoption
- Pointers to vendor white papers and other materials that support the Controls.
- Documentation on alignment with the NIST Cybersecurity Framework.

Structure of the CIS Critical Security Controls Document

The presentation of each Control in this document includes the following elements:

- A description of the importance of the Control **(Why is This Control Critical)** in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control.
- A chart of the specific actions ("sub-controls") that organizations are taking to implement, automate, and measure effectiveness of this control.
- Procedures and Tools that enable implementation and automation.
- Sample **Entity Relationship Diagrams** that show components of implementation.

In addition to this document, we strongly recommend "A Measurement Companion to the CIS Critical Security Controls", available from the Center for Internet Security.

Acknowledgements

The Center for Internet Security would like to thank the many security experts who volunteered their time and talent to support the Controls effort. Many of the individuals who worked on this version continue to lend their expertise year after year. We are extremely grateful for their time and expertise. Special recognition also goes to The SANS Institute, a major contributor to the effort.

CSC 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal jump points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

As new technology continues to come out, BYOD (bring your own device) — where employees bring personal devices into work and connect them to the enterprise network — is becoming very common. These devices could already be compromised and be used to infect internal resources.

Managed control of all devices also plays a critical role in planning and executing system backup and recovery.

CSC 1: Inventory of Authorized and Unauthorized Devices				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**1.1**	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	**Y**	*Use a mix of active and passive tools, and apply as part of a continuous monitoring program.*
System	**1.2**	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	**1.3**	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	**Y**	
System	**1.4**	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	**Y**	
System	**1.5**	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	**Y**	*Authentication mechanisms are closely coupled to management of hardware inventory*
System	**1.6**	Use client certificates to validate and authenticate systems prior to connecting to the private network.		**Y**

CSC 1 Procedures and Tools

This Control requires both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organizations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

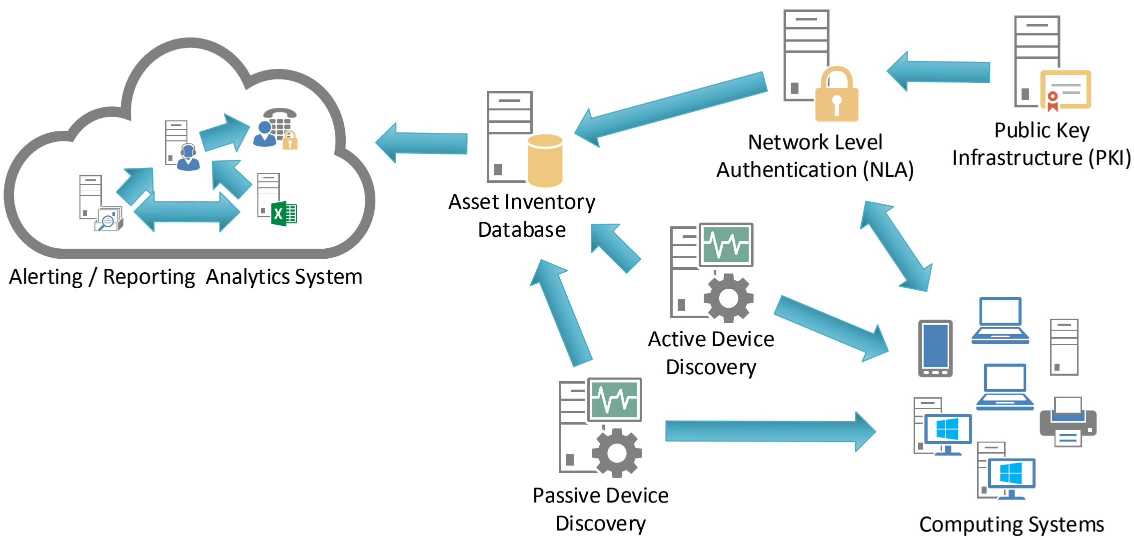
Maintaining a current and accurate view of IT assets is an ongoing and dynamic process. Organizations can actively scan on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.

In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Many organizations also pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems very dynamic. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

CSC 1 System Entity Relationship Diagram



CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why Is This Control Critical?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all software also plays a critical role in planning and executing system backup and recovery.

CSC 2: Inventory of Authorized and Unauthorized Software				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**2.1**	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	**Y**	*File integrity is verified as part of a continuous monitoring program.*

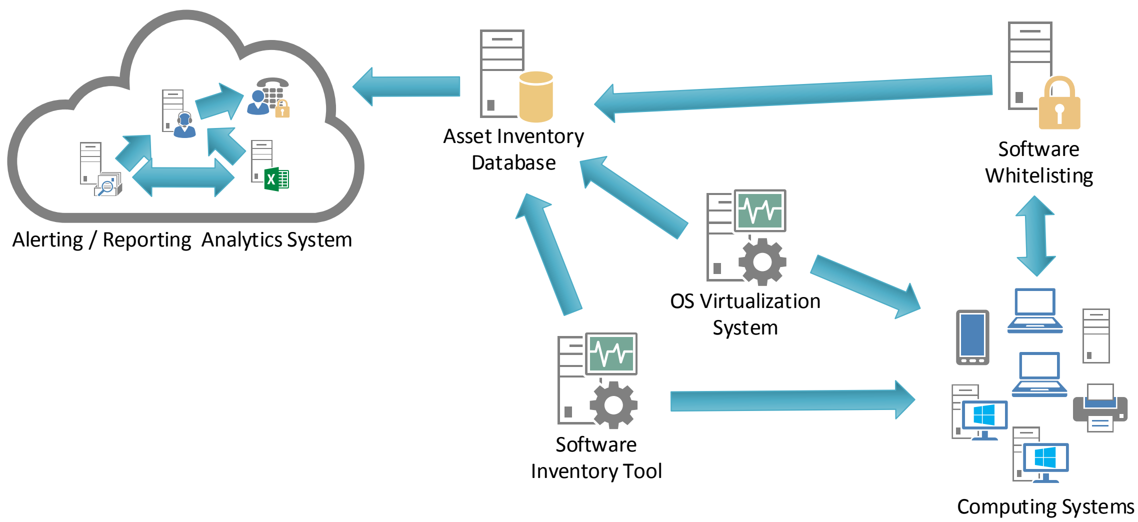
Family	CSC	Control Description	Foun-dational	Advanced
System	**2.2**	Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.	**Y**	*Whitelist application libraries (such as DLLs) in addition to executable binaries (such as EXEs and MSIs.*
System	**2.3**	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	**Y**	*Hardware and software inventory management are closely coupled, and managed centrally.*
System	**2.4**	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.		**Y**

CSC 2 Procedures and Tools

Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and with Windows. Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Features that implement whitelists are included in many modern endpoint security suites. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with application white and black listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom whitelists based on executable path, hash, or regular expression matching. Some even include a gray list function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day.

CSC 2 System Entity Relationship Diagram



CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This Control Critical?

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tool section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software.

CSC 3: Secure Configurations for Hardware and Software				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**3.1**	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	**Y**	
System	**3.2**	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	**3.3**	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	**Y**	*File integrity of master images are verified as part of a continuous monitoring program.*
System	**3.4**	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	**Y**	
System	**3.5**	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	**Y**	*File integrity of critical system files are verified as part of a continuous monitoring program.*
System	**3.6**	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	**3.7**	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.	**Y**	

CSC 3 Procedures and Tools

Rather than start from scratch developing a security baseline for each software system, organizations should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Excellent resources include:

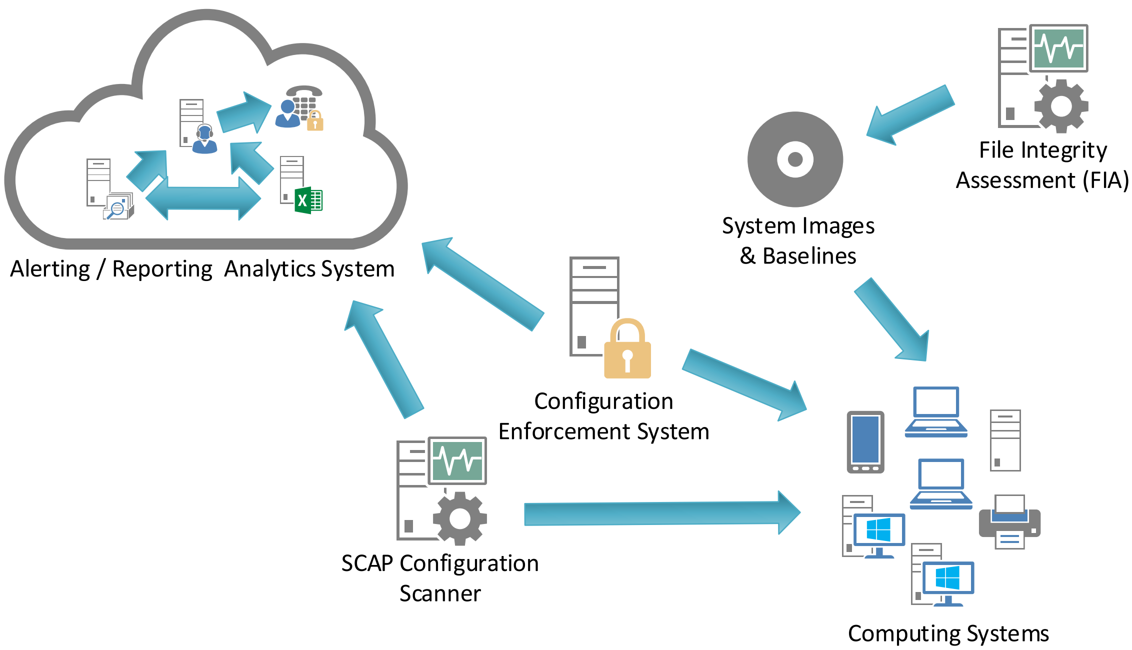
- The Center for Internet Security Benchmarks Program (www.cisecurity.org)
- The NIST National Checklist Program (checklists.nist.gov)

Organizations should augment or adjust these baselines to satisfy local policies and requirements, but deviations and rationale should be documented to facilitate later reviews or audits.

For a complex enterprise, the establishment of a single security baseline configuration (for example, a single installation image for all workstations across the entire enterprise) is sometimes not practical or deemed unacceptable. It is likely that you will need to support different standardized images, based on the proper hardening to address risks and needed functionality of the intended deployment (example, a web server in the DMZ vs. an email or other application server in the internal network). The number of variations should be kept to a minimum in order to better understand and manage the security properties of each, but organizations then must be prepared to manage multiple baselines.

Commercial and/or free configuration management tools can then be employed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Typical configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems by remotely logging in to each managed machine using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

CSC 3 System Entity Relationship Diagram



CSC 4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Why Is This Control Critical?

Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to "weaponize", deploy an attack, exploit); vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).

Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes-uncertain side effects.

CSC 4: Continuous Vulnerability Assessment and Remediation				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**4.1**	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	**Y**	*Vulnerability risk scoring is centrally measured and managed, and integrated into action planning.*
System	**4.2**	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	**4.3**	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	**Y**	
System	**4.4**	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	**Y**	
System	**4.5**	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.	**Y**	
System	**4.6**	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.	**Y**	
System	**4.7**	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	**Y**	
System	**4.8**	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	**Y**	

CSC 4 Procedures and Tools

A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an organization or even across organizations, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.

Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive scans than can be achieved without login credentials. The frequency of scanning activities, however, should increase as the diversity of an organization's systems increases to account for the varying patch cycles of each vendor.

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators.

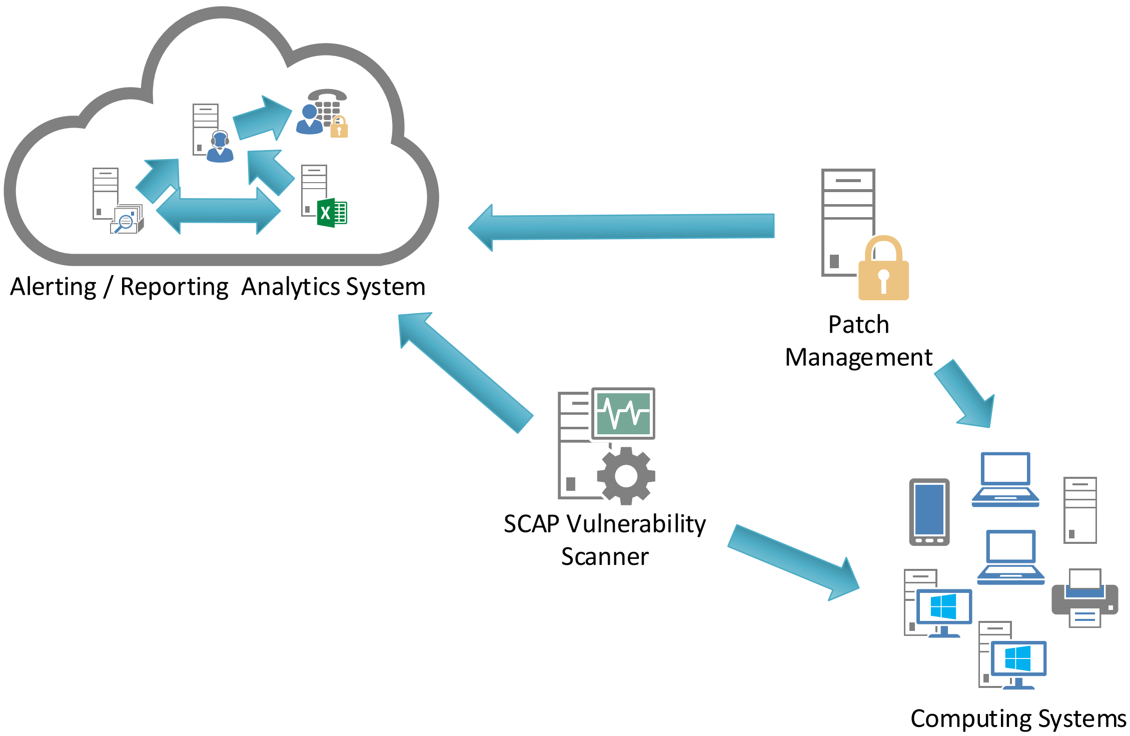
Effective organizations link their vulnerability scanners with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management to ensure the problems are solved.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan. If this time window exceeds the organization's benchmarks for deployment of the given patch's criticality level, security personnel should note the delay and determine if a deviation was formally documented for the system and its patch. If not, the security team should work with management to improve the patching process.

Additionally, some automated patching tools may not detect or install certain patches due to an error by the vendor or administrator. Because of this, all patch checks should reconcile system patches with a list of patches each vendor has announced on its website.

CSC 4 System Entity Relationship Diagram



CSC 5: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Why Is This Control Critical?

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user, is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data. Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

CSC 5: Controlled Use of Administrative Privileges				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**5.1**	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	**Y**	
System	**5.2**	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	**Y**	
System	**5.3**	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	**Y**	

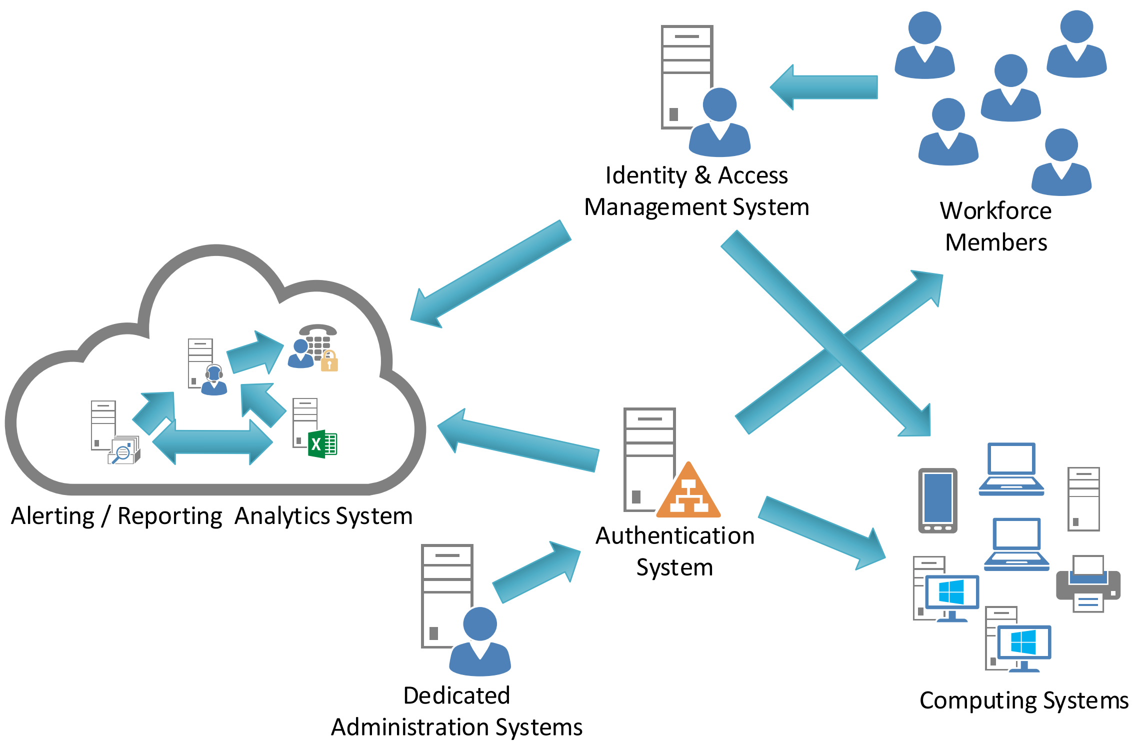
Family	CSC	Control Description	Foun-dational	Advanced
System	**5.4**	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	**Y**	
System	**5.5**	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	**Y**	
System	**5.6**	Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	**Y**	
System	**5.7**	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	**Y**	
System	**5.8**	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	**Y**	
System	**5.9**	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		**Y**

CSC 5 Procedures and Tools

Built-in operating system features can extract lists of accounts with super-user privileges, both locally on individual systems and on overall domain controllers. To verify that users with high-privileged accounts do not use such accounts for day-to-day web surfing and email reading, security personnel should periodically gather a list of running processes to determine whether any browsers or email readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, email readers, and document editing programs running with high privileges on machines. Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control.

To enforce the requirement for strong passwords, built-in operating system features for minimum password length can be configured to prevent users from choosing short passwords. To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcement tools can be applied.

CSC 5 System Entity Relationship Diagram



CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Why Is This Control Critical?

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even through the evidence of the attack has been recorded in unexamined log files.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs				
Family	CSC	Control Description	Foun-dational	Advanced
System	**6.1**	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.	**Y**	
System	**6.2**	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.	**Y**	
System	**6.3**	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.	**Y**	
System	**6.4**	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.	**Y**	

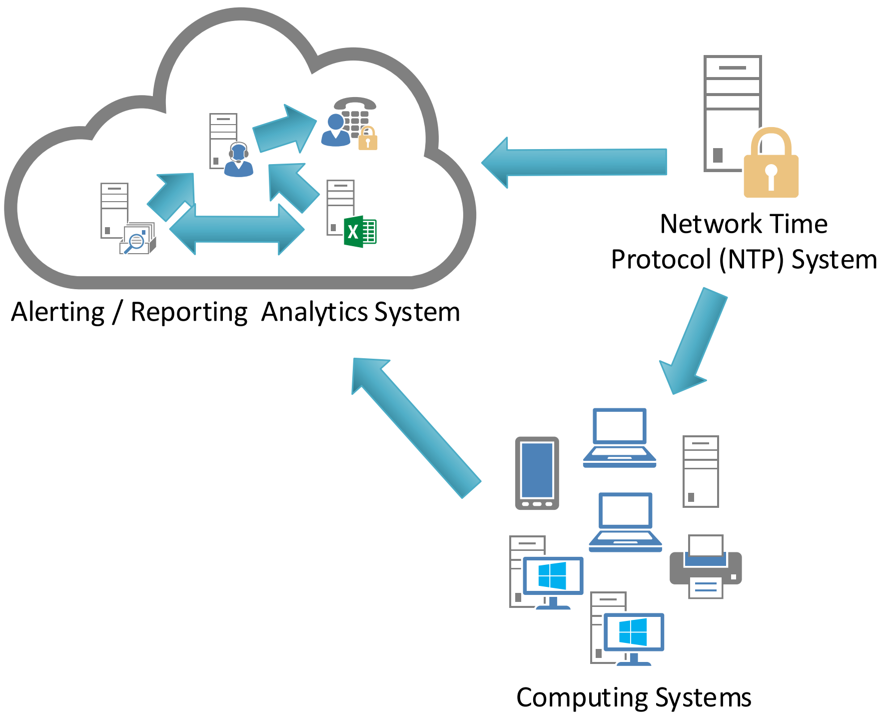
Family	CSC	Control Description	Foun-dational	Advanced
System	**6.5**	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.	**Y**	
System	**6.6**	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	**Y**	

CSC 6 Procedures and Tools

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled as part of Critical Control 1 in order to ensure that each managed item actively connected to the network is periodically generating logs.

Analytical programs such as SIM/SEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, even including, importantly, just a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

CSC 6 System Entity Relationship Diagram



CSC 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

Why Is This Control Critical?

Web browsers and email clients are very common points of entry and attack because of their high technical complexity and flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks.

CSC 7: Email and Web Browser Protections				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**7.1**	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.	**Y**	
System	**7.2**	Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.	**Y**	
System	**7.3**	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.	**Y**	
System	**7.4**	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	**Y**	*Include mobile devices.*
System	**7.5**	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	**7.6**	The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	**Y**	
System	**7.7**	To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.	**Y**	
System	**7.8**	Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.	**Y**	

CSC 7 Procedures and Tools

Web Browser

Most web browsers today have basic security features, but it is not adequate to rely on one aspect of security. A web server is made up of layers that provide multiple avenues of attack. The foundation of any web browser is the operating system and the secret to ensuring that it remains secure is simple: keep it updated with the latest security patches. Ensure that your patches are up-to-date and installed properly, as any server running old patches will become a victim.

Update any software components that run on a web server. Anything that is non-essential, such as DNS servers and remote administration tools like VNC or Remote Desktop, should be disabled or removed. If remote administration tools are essential, however, then avoid using default passwords or anything that can be easily guessed. This is not only applicable for remote access tools, but user accounts, switches and routers as well.

A flexible firewall is one of the strongest forms of defense against security breaches. When a web server is targeted the attack will attempt to upload hacking tools or malware immediately, so as to take advantage of the security breach before it is fixed. Without a good anti-virus package, a breach in security can go unnoticed for a significant amount of time.

Cybercriminals can exploit cookies in malicious ways. Changing your browser settings to block third party cookies will help reduce this risk. The autocomplete or autofill feature saves keystrokes by storing information you recently typed. However, autocomplete for login information poses a big risk if your laptop is lost or stolen. And restricting add-ons to an absolute minimum will reduce the attack surface. Add-ons can harbor malware and increase the possibilities for attacking your browser. Configure your browsers to prevent them from installing add-ons without a prompt.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. Make sure that you and your users enable content filters. And turn on the popup blockers. Popups are not only annoying, they also can host embedded malware directly or lure users into clicking on something using social engineering tricks. Be sure that your selected browser has popup blocking enabled

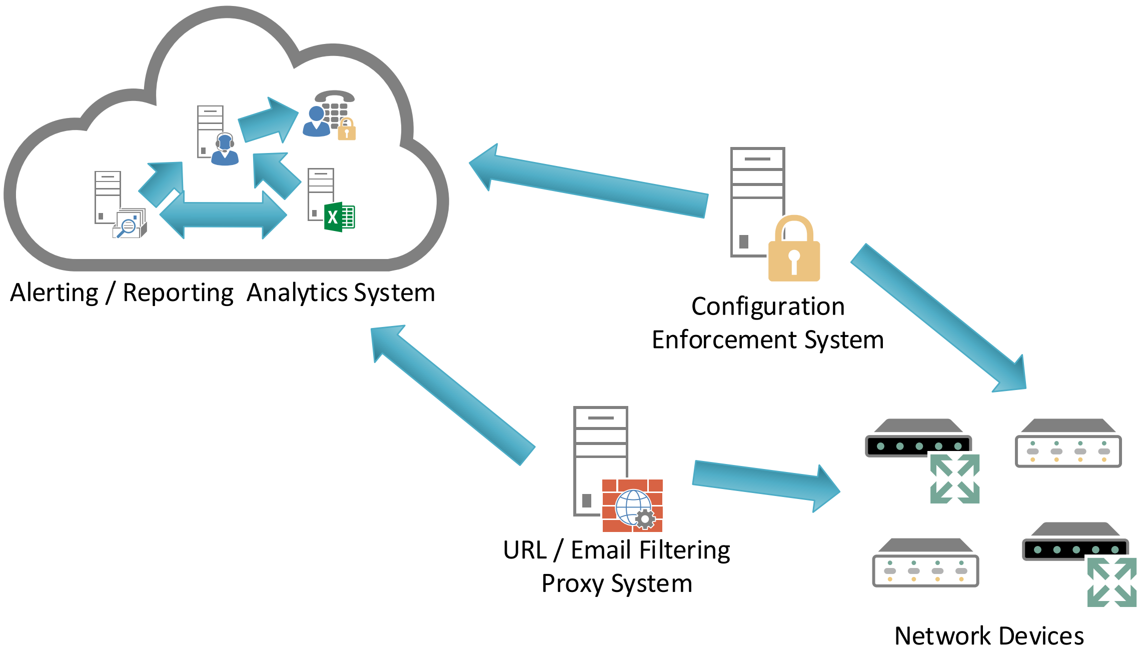
Email

Email represents one the most interactive ways humans work with computers, encouraging the right behavior is just as important as the technical settings.

Passwords containing common words or phrases are easy to crack. Ensure complex passwords are created; a combination of letters, numbers and special characters is complex enough. Passwords should be changed on a regular basis, every 45-60 days.

Implementing two-factor authentication is another way to ensure the user is authentic, reducing the attack surface. Using a spam-filtering tool reduces the number of malicious emails that come into your network. Initiating a Sender Policy Framework to verify that the domain an email is coming from is authentic, helps reduce Spam and Phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and networked based security.

CSC 7 System Entity Relationship Diagram



CSC 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Why Is This Control Critical?

Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack your systems, devices, or your data. It can be fast-moving, fast-changing, and enter through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware can be designed to avoid defenses, or to attack or disable them.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like Incident Response. They must also be deployed at multiple possible points-of-attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.

CSC 8: Malware Defenses				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**8.1**	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	**Y**	
System	**8.2**	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	**Y**	
System	**8.3**	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	**Y**	*Actively monitor the use of external devices (in addition to logging).*

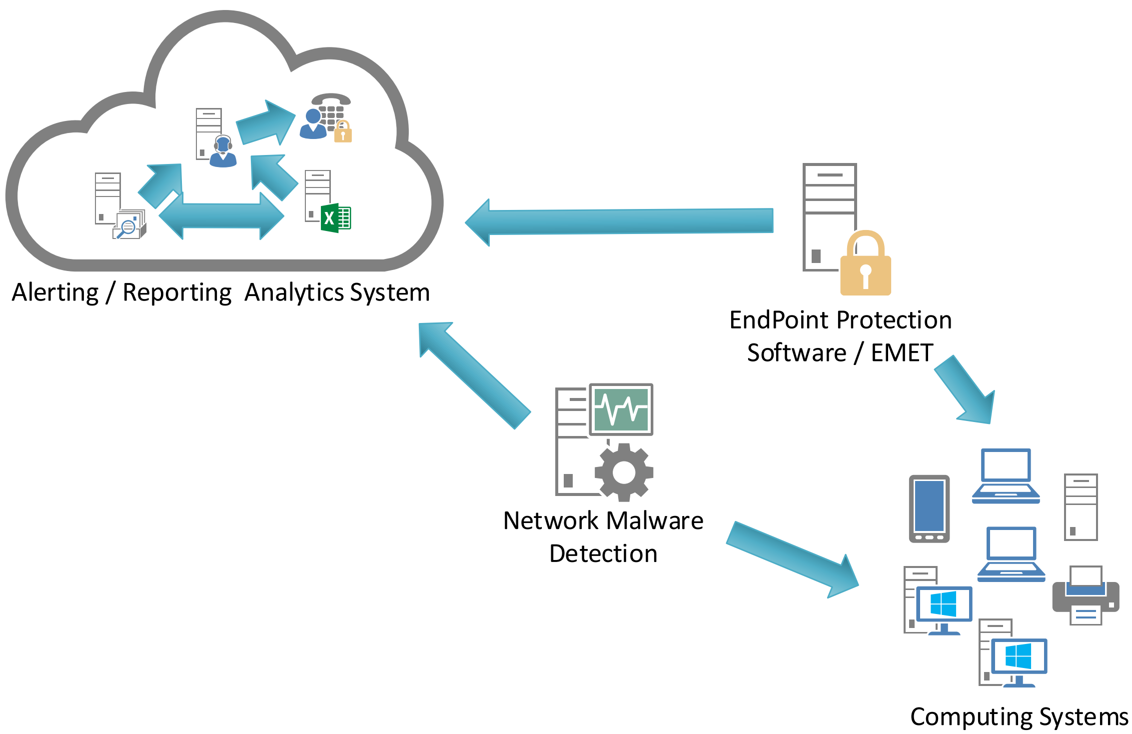
Family	CSC	Control Description	Foun-dational	Advanced
System	**8.4**	Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.	**Y**	
System	**8.5**	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.		**Y**
System	**8.6**	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.	**Y**	

CSC 8 Procedures and Tools

To ensure anti-virus signatures are up to date, organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Some enterprises deploy free or commercial honeypot and “tarpit” tools to identify attackers in their environment. Security personnel should continuously monitor these tools to determine whether traffic is directed to them and account logins are attempted. When they identify such events, these personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.

CSC 8 System Entity Relationship Diagram



CSC 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Why Is This Control Critical?

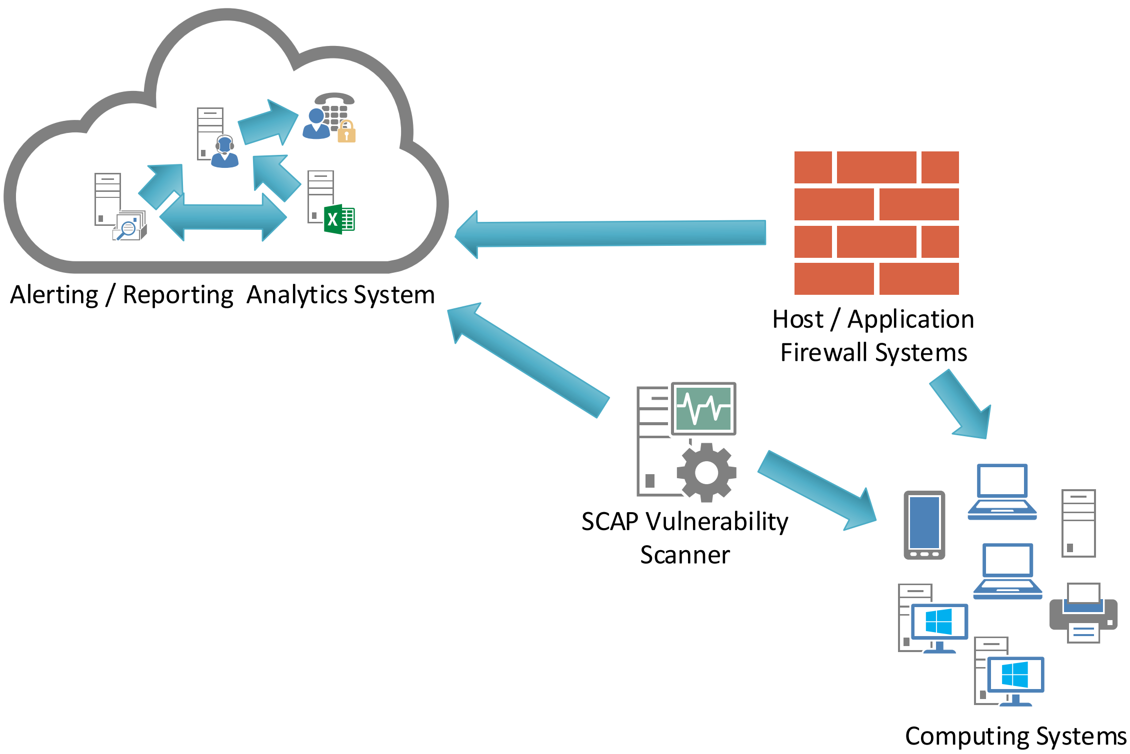
Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

CSC 9: Limitation and Control of Network Ports				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**9.1**	Ensure that only ports, protocols, and services with validated business needs are running on each system.	**Y**	
System	**9.2**	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	**Y**	
System	**9.3**	Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.	**Y**	
System	**9.4**	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.	**Y**	
System	**9.5**	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.		**Y**
System	**9.6**	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.		**Y**

CSC 9 Procedures and Tools

Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

CSC 9 System Entity Relationship Diagram



CSC 10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why Is This Control Critical?

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

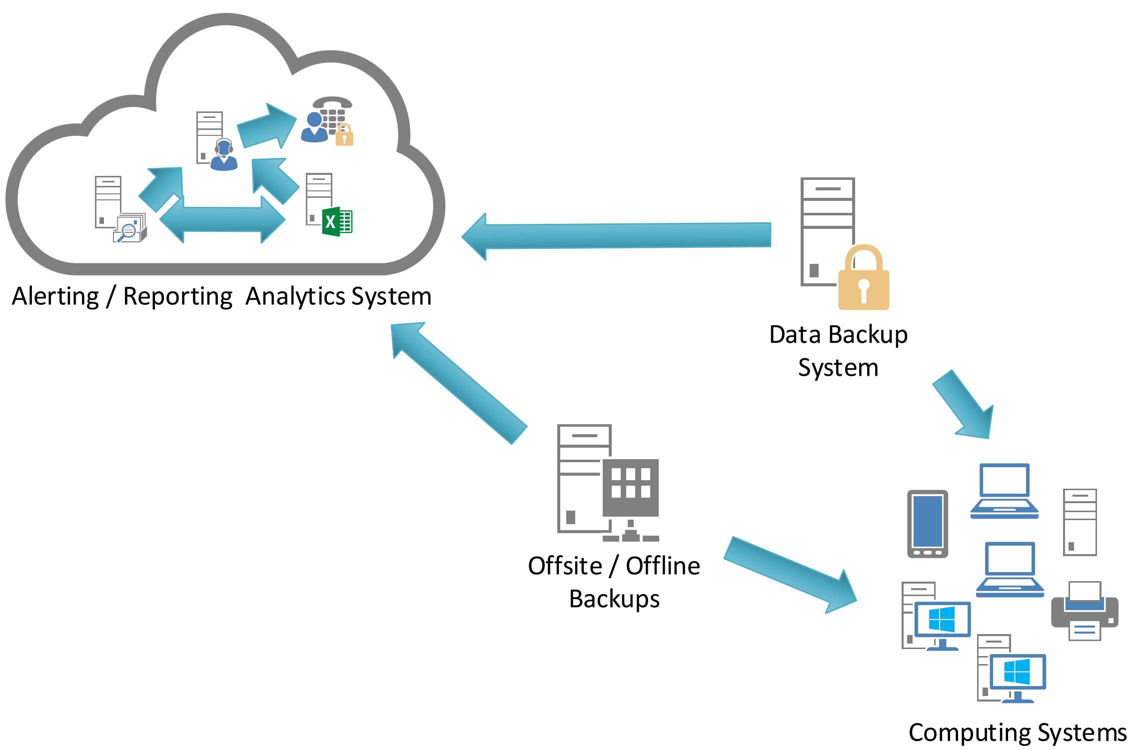
CSC 10: Data Recovery Capability				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**10.1**	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.	**Y**	
System	**10.2**	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	**Y**	
System	**10.3**	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	**Y**	
System	**10.4**	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.	**Y**	

CSC 10 Procedures and Tools

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

CSC 10 System Entity Relationship Diagram



CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This Control Critical?

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use – not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state.

Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for vulnerable default settings, electronic holes in firewalls, routers, and switches and use those to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

CSC 11: Secure Configurations for Network Devices

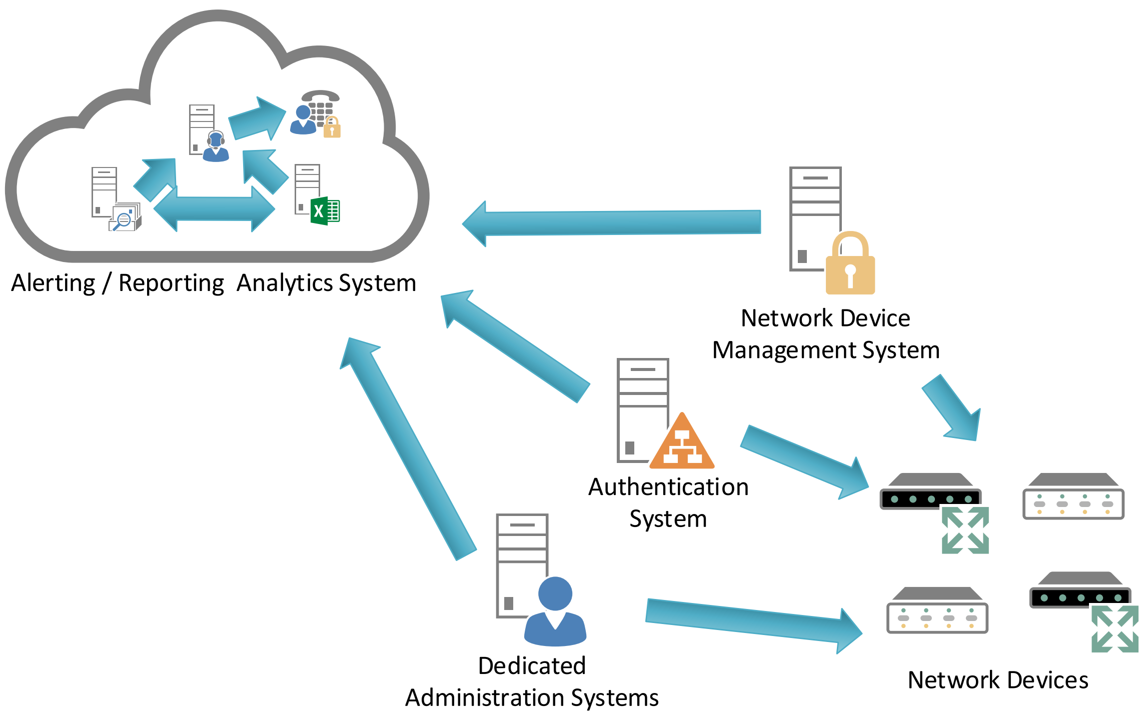
Family	CSC	Control Description	Foun-dational	Advanced
Network	**11.1**	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Network	**11.2**	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.	**Y**	
Network	**11.3**	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.	**Y**	
Network	**11.4**	Manage network devices using two-factor authentication and encrypted sessions.	**Y**	
Network	**11.5**	Install the latest stable version of any security-related updates on all network devices.	**Y**	
Network	**11.6**	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.		**Y**
Network	**11.7**	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	**Y**	

CSC 11 Procedures and Tools

Some organizations use commercial tools that evaluate the rule set of network filtering devices to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or access controls lists (ACLs) that may allow unintended services through the device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

CSC 11 System Entity Relationship Diagram



CSC 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Why Is This Control Critical?

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

CSC 12: Boundary Defense				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**12.1**	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	**Y**	
Network	**12.2**	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.	**Y**	
Network	**12.3**	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	**Y**	
Network	**12.4**	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Network	**12.5**	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.	**Y**	
Network	**12.6**	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.	**Y**	
Network	**12.7**	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.		**Y**
Network	**12.8**	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.		**Y**
Network	**12.9**	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.	**Y**	
Network	**12.10**	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.		**Y**

CSC 12 Procedures and Tools

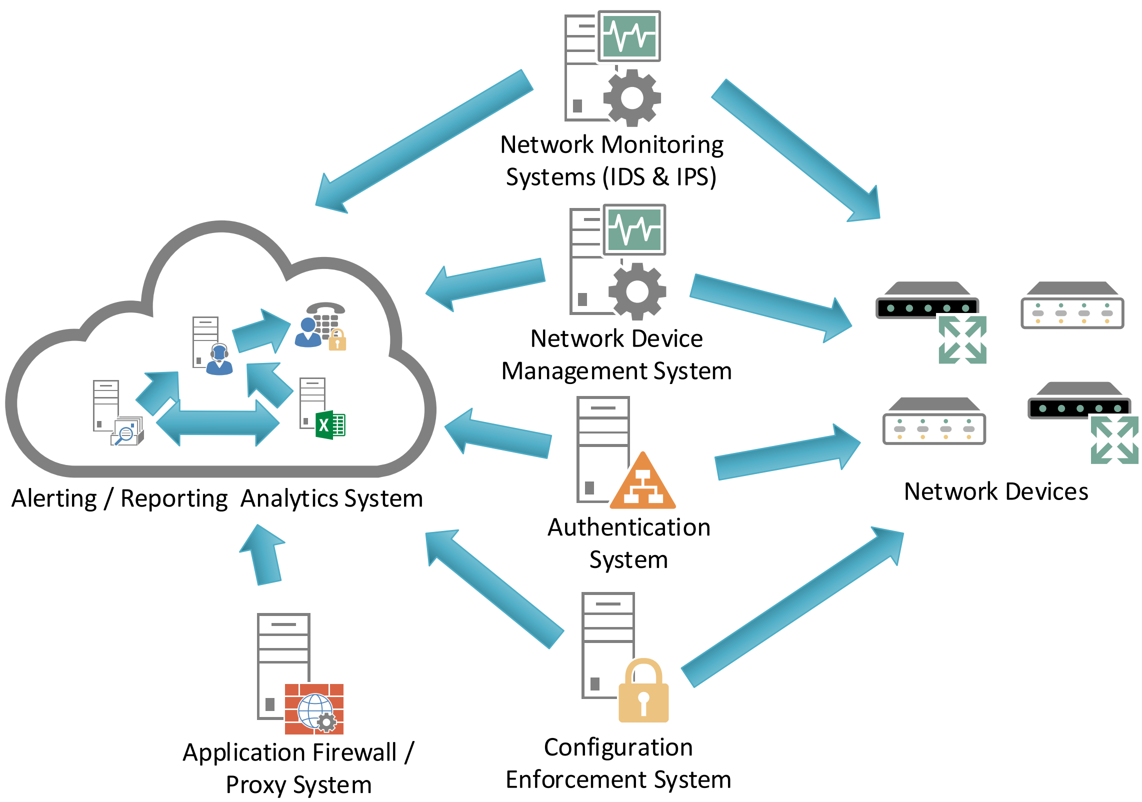
The boundary defenses included in this control build on Critical Control 10. The additional recommendations here focus on improving the overall architecture and implementation of both Internet and internal network boundary points. Internal network segmentation is central to this control because once inside a network, many intruders attempt to target the most sensitive machines. Usually, internal network protection is not set up to defend against an internal attacker. Setting up even a basic level of security segmentation across the network and protecting each segment with a proxy and a firewall will greatly reduce an intruder's access to the other parts of the network.

One element of this control can be implemented using free or commercial IDS and sniffers to look for attacks from external sources directed at DMZ and internal systems, as well as attacks originating from internal systems against the DMZ or Internet. Security personnel should regularly test these sensors by launching vulnerability-scanning tools against them to verify that the scanner traffic triggers an appropriate alert. The captured packets of the IDS sensors should be reviewed using an automated script each day to ensure that log volumes are within expected parameters and that the logs are formatted properly and have not been corrupted.

Additionally, packet sniffers should be deployed on DMZs to look for Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. By sampling traffic regularly, such as over a three-hour period once a week, information security personnel can search for HTTP traffic that is neither sourced by nor destined for a DMZ proxy, implying that the requirement for proxy use is being bypassed.

To identify back-channel connections that bypass approved DMZs, network security personnel can establish an Internet-accessible system to use as a receiver for testing outbound access. This system is configured with a free or commercial packet sniffer. Then, security personnel can connect a sending test system to various points on the organization's internal network, sending easily identifiable traffic to the sniffing receiver on the Internet. These packets can be generated using free or commercial tools with a payload that contains a custom file used for the test. When the packets arrive at the receiver system, the source address of the packets should be verified against acceptable DMZ addresses allowed for the organization. If source addresses are discovered that are not included in legitimate, registered DMZs, more detail can be gathered by using a `traceroute` tool to determine the path that packets take from the sender to the receiver system.

CSC 12 System Entity Relationship Diagram



CSC 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Why Is This Control Critical?

Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise.

The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. This is true if proper care has been taken in the processes and technologies associated with the encryption operations. An example of this is the management of cryptographic keys used by the various algorithms that protect data. The process for generation, use and destruction of keys should be based on proven processes as defined in standards such as NIST SP 800-57.

Care should also be taken to ensure that products used within an enterprise implement well known and vetted cryptographic algorithms, as identified by NIST. Re-evaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data.

For organizations that are moving data to the cloud, it is important to understand the security controls applied to data in the cloud multi-tenant environment, and determine the best course of action for application of encryption controls and security of keys. When possible, keys should be stored within secure containers such as Hardware Security Modules (HSMs).

Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources, however controls should also be put in place to mitigate the threat of data exfiltration in the first place. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet, in most cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error.

Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

CSC 13: Data Protection				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**13.1**	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.	**Y**	
Network	**13.2**	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	**Y**	
Network	**13.3**	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.		**Y**
Network	**13.4**	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.		**Y**
Network	**13.5**	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.		**Y**

Family	CSC	Control Description	Foun-dational	Advanced
Network	**13.6**	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.		**Y**
Network	**13.7**	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.		**Y**
Network	**13.8**	Block access to known file transfer and email exfiltration websites.		**Y**
Network	**13.9**	Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.		**Y**

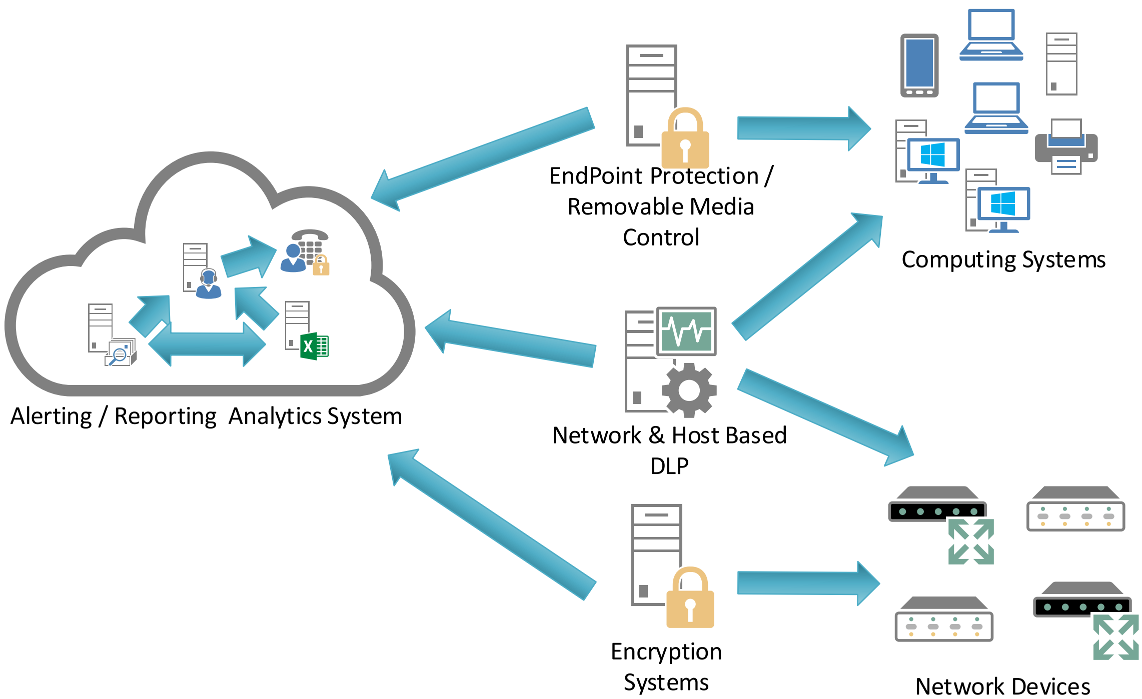
CSC 13 Procedures and Tools

Commercial tools are available to support enterprise management of encryption and key management within an enterprise and include the ability to support implementation of encryption controls within cloud and mobile environments.

Definition of life cycle processes and roles and responsibilities associated with key management should be undertaken by each organization.

Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Organizations deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the organization without authorization.

CSC 13 Entity Relationship Diagram



CSC 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Why Is This Control Critical?

Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems (e.g., SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.

CSC 14: Controlled Access Based on the Need to Know				
Family	CSC	Control Description	Foun-dational	Advanced
Application	**14.1**	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.	**Y**	
Application	**14.2**	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.	**Y**	
Application	**14.3**	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Application	**14.4**	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	**Y**	
Application	**14.5**	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.		**Y**
Application	**14.6**	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.	**Y**	
Application	**14.7**	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	**Y**	

CSC 14 Procedures and Tools

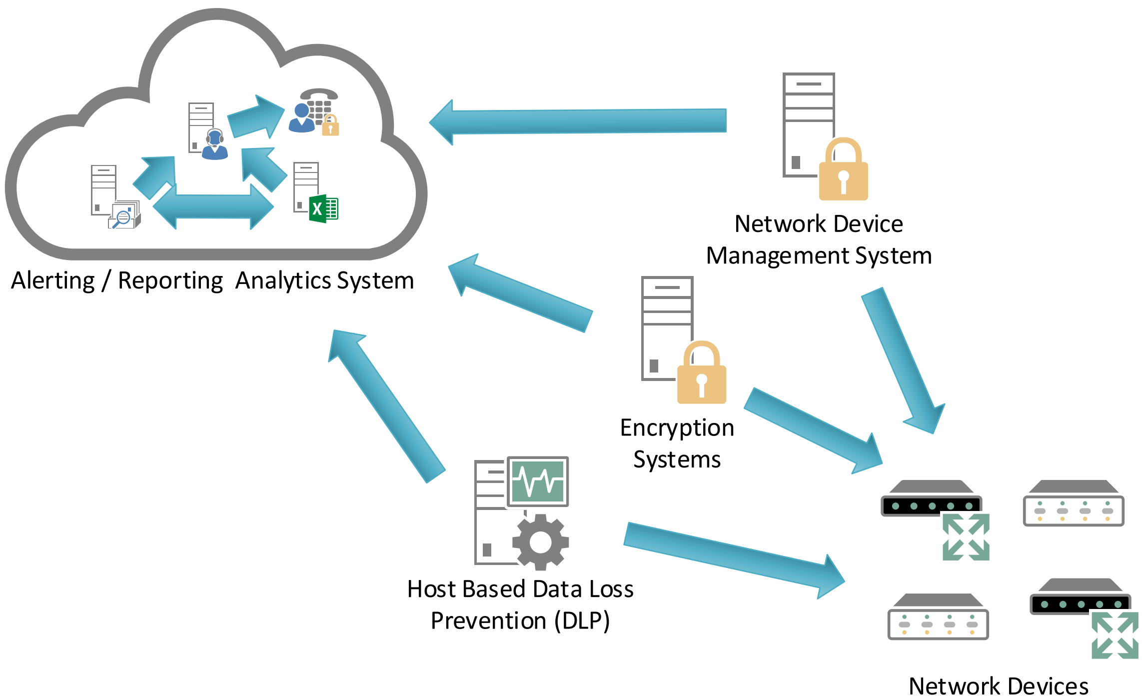
It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it. To derive sensitivity levels, organizations need to put together a list of the key types of data and the overall importance to the organization. This analysis would be used to create an overall data classification scheme for the organization. At a base level, a data classification scheme is broken down into two levels: public (unclassified) and private (classified). Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organization if it were compromised.

Once the sensitivity of the data has been identified, the data need to be traced back to business applications and the physical servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels. If possible, firewalls need to control access to each segment. If data are flowing over a network with a lower trust level, encryption should be used.

Job requirements should be created for each user group to determine what information the group needs access to in order to perform its jobs. Based on the requirements, access should only be given to the segments or servers that are needed for each job function.

Detailed logging should be turned on for all servers in order to track access and examine situations where someone is accessing data that they should not be accessing.

CSC 14 System Entity Relationship Diagram



CSC 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Why Is This Control Critical?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

CSC 15: Wireless Access Control				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**15.1**	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.	**Y**	
Network	**15.2**	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.	**Y**	
Network	**15.3**	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.		**Y**
Network	**15.4**	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).		**Y**

Family	CSC	Control Description	Foun-dational	Advanced
Network	**15.5**	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.	**Y**	
Network	**15.6**	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.	**Y**	
Network	**15.7**	Disable peer-to-peer wireless network capabilities on wireless clients.	**Y**	
Network	**15.8**	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.	**Y**	
Network	**15.9**	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.	**Y**	

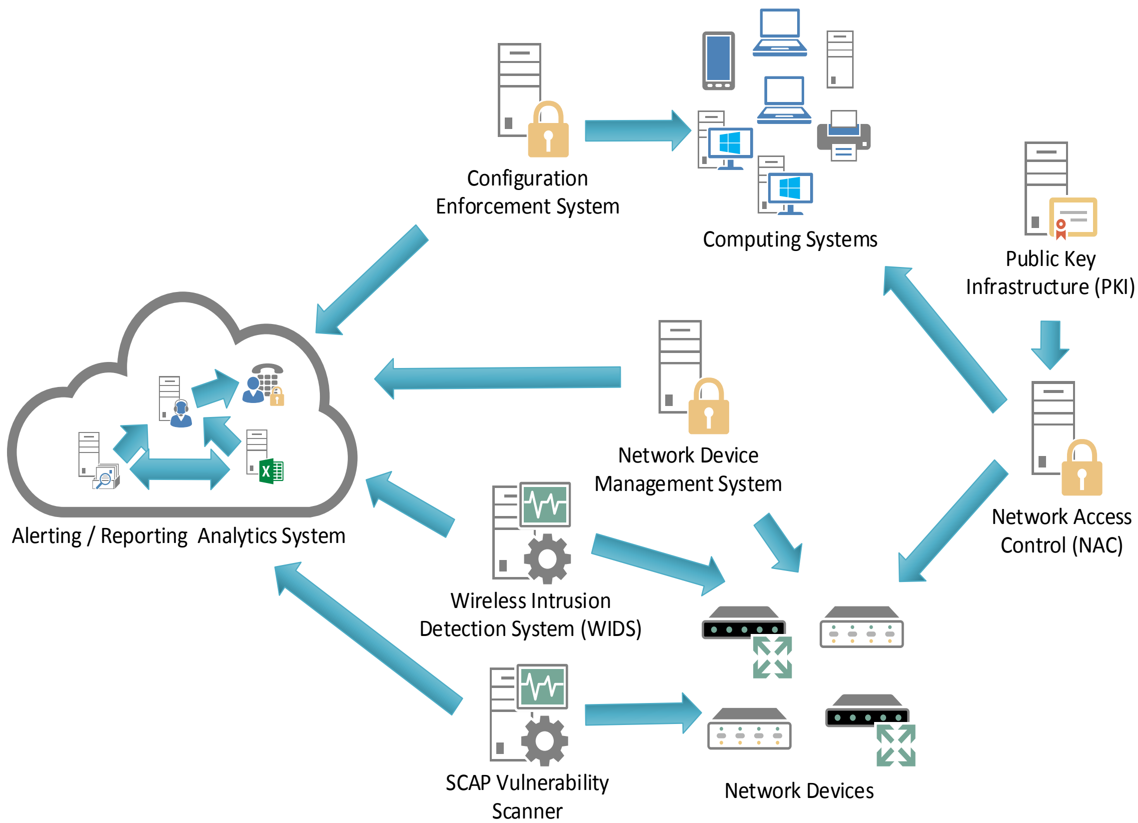
CSC 15 Procedures and Tools

Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

Additionally, the security team should periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates. When devices relying on weak wireless security settings are identified, they should be found within the organization's asset inventory and either reconfigured more securely or denied access to the organization network.

Additionally, the security team should employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to managed systems.

CSC 15 System Entity Relationship Diagram



CSC 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Why Is This Control Critical?

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

CSC 16: Account Monitoring and Control				
Family	CSC	Control Description	Foun-dational	Advanced
Application	**16.1**	Review all system accounts and disable any account that cannot be associated with a business process and owner.	**Y**	
Application	**16.2**	Ensure that all accounts have an expiration date that is monitored and enforced.	**Y**	
Application	**16.3**	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.	**Y**	
Application	**16.4**	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	**Y**	
Application	**16.5**	Configure screen locks on systems to limit access to unattended workstations.	**Y**	
Application	**16.6**	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.	**Y**	

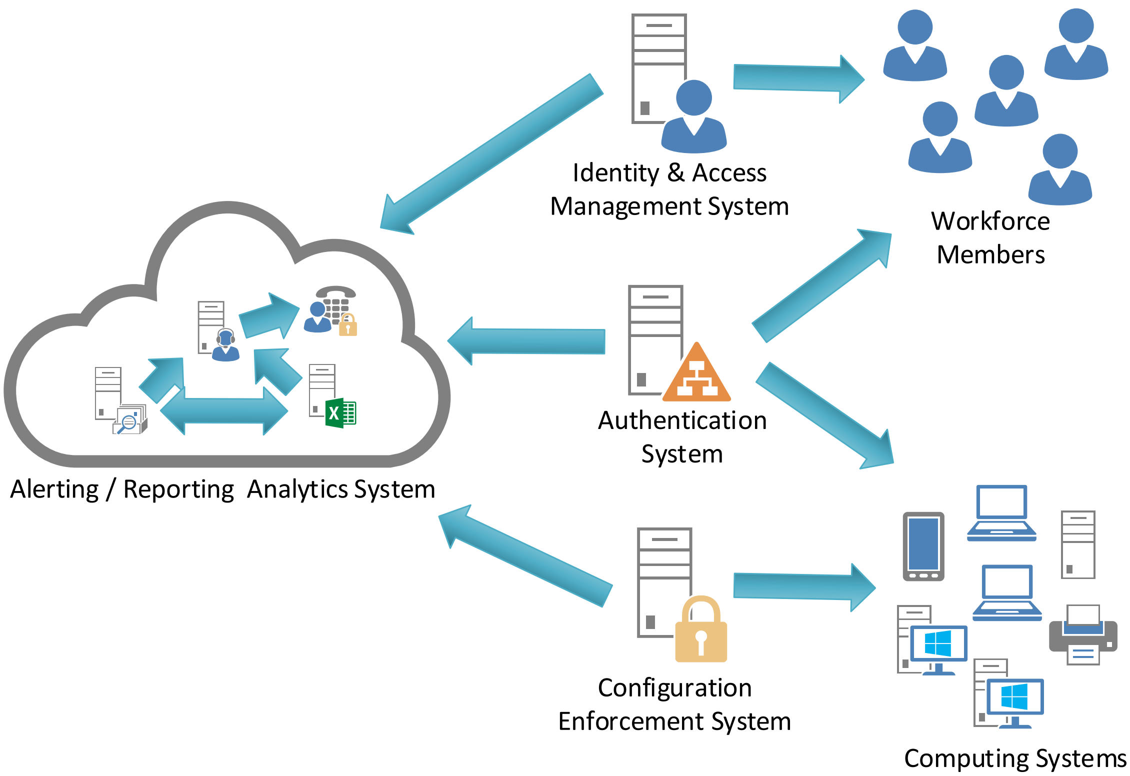
Family	CSC	Control Description	Foun-dational	Advanced
Application	**16.7**	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	**Y**	
Application	**16.8**	Monitor attempts to access deactivated accounts through audit logging.	**Y**	
Application	**16.9**	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.	**Y**	
Application	**16.10**	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.		**Y**
Application	**16.11**	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.	**Y**	
Application	**16.12**	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	**Y**	
Application	**16.13**	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	**Y**	
Application	**16.14**	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.	**Y**	

CSC Procedures and Tools

Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems.

Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system, and it must be ensured that their passwords are robust and changed on a regular basis. Users must also be logged out of the system after a period of no activity to minimize the possibility of an attacker using their system to extract information from the organization.

CSC 16 System Entity Relationship Diagram



CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Why Is This Control Critical?

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artifacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions).

Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

No cyber defense approach can effectively address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**17.1**	Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Application	**17.2**	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.	**Y**	
Application	**17.3**	Implement a security awareness program that (1) focuses on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, (5) is reliably monitored for employee completion, and 6) includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics.	**Y**	
Application	**17.4**	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.	**Y**	
Application	**17.5**	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure mastery of skills mastery.		**Y**

CSC 17 Procedures and Tools

An effective enterprise-wide training program should take a holistic approach and consider policy and technology at the same time as the training of people. For example, policies should be designed with technical measurement and enforcement when possible, reinforced by training to fill gaps, technical controls can be implemented to bound and minimize the opportunity for people to make mistakes, and so focus the training on things that cannot be managed technically.

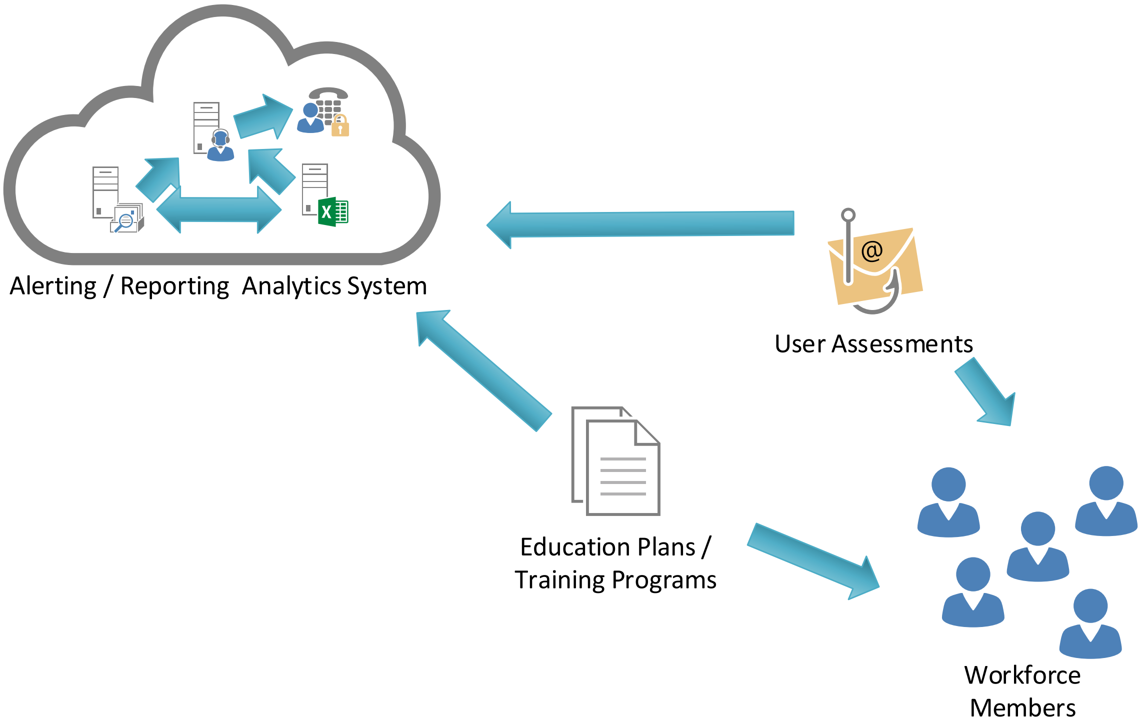
To be effective in both cost and outcome, security training should be prioritized, focused, specific, and measurable. A key way to prioritize training is to focus first on those jobs and roles that are *critical* to the mission or business outcome of the enterprise. One way to identify these mission-critical jobs is to reference the work of the 2012 Task Force on Cyber Skills established by the Secretary of Homeland Security: 1) System and Network Penetration Testers, 2) Application Penetration Testers, 3) Security Monitoring and Event Analysts, 4) Incident Responders In-Depth, 5) Counter-Intelligence/Insider Threat Analysts, 6) Risk Assessment Engineers, 7) Secure Coders and Code Reviewers, 8) Security Engineers/Architecture and Design, 9) Security Engineers/Operations, and 10) Advanced Forensics Analysts. A comprehensive taxonomy of cybersecurity roles is available through the National Cybersecurity Workforce Framework, developed by the National Institute of Standards and Technology (NIST), which maps to roles commonly found in enterprises and government organizations.

General awareness training for all users also plays an important role. But even this training should be tailored to functional roles and focused on specific actions that put the organization at risk, and measured in order to drive remediation.

The key to upgrading skills is measurement through assessments that show both the employee and the employer where knowledge is sufficient and where there are gaps. Once the gaps have been identified, those employees who have the requisite skills and knowledge can be called upon to mentor employees who need to improve their skills. In addition, the organization can develop training plans to fill the gaps and maintain employee readiness.

A full treatment of this topic is beyond the scope of the Critical Security Controls. However, the Cybersecurity Workforce Handbook published by the Center for Internet Security (www.cisecurity.org) provides foundational steps to take in optimizing the workforce for enterprise security.

CSC 17 System Entity Relationship Diagram



CSC 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Why Is This Control Critical?

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions. There is a flood of public and private information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow "weaponization" of vulnerabilities into exploits. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

CSC 18: Application Software Security				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**18.1**	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	**Y**	
Application	**18.2**	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	**Y**	*Dealing with encrypted/tunneled traffic requires more planning and resources.*

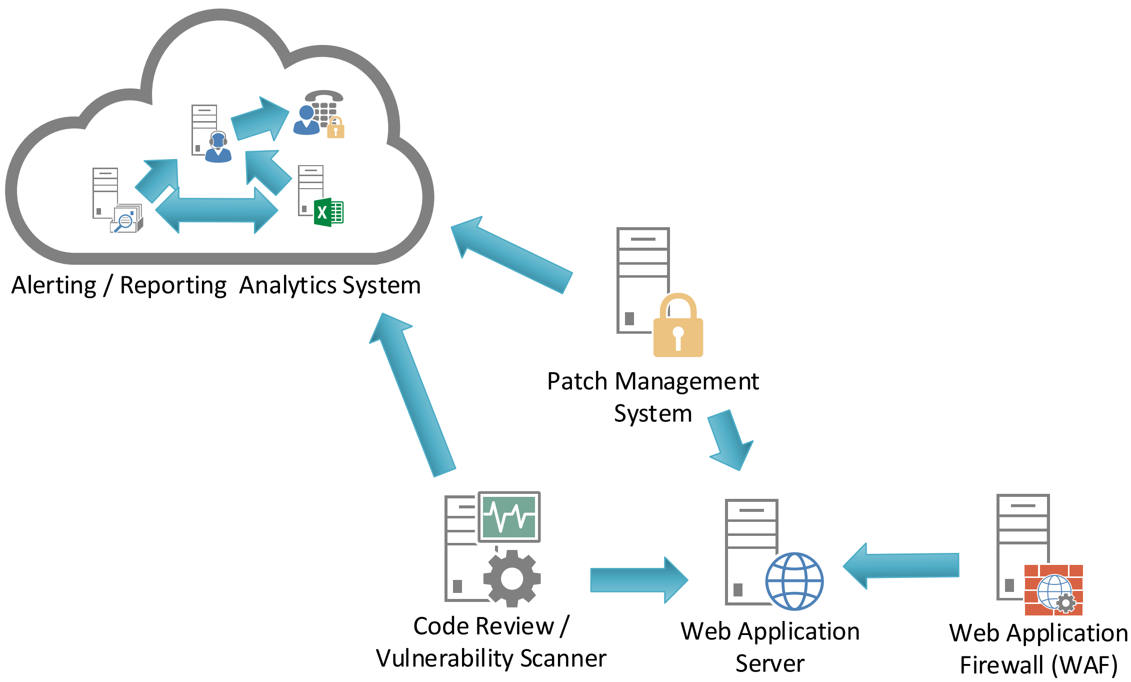
Family	CSC	Control Description	Foun-dational	Advanced
Application	**18.3**	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	**Y**	
Application	**18.4**	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.	**Y**	
Application	**18.5**	Do not display system error messages to end-users (output sanitization).	**Y**	
Application	**18.6**	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.	**Y**	
Application	**18.7**	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	**Y**	
Application	**18.8**	Ensure that all software development personnel receive training in writing secure code for their specific development environment.	**Y**	
Application	**18.9**	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.	**Y**	

CSC 18 Procedures and Tools

The security of applications (in-house developed or acquired) is a complex activity requiring a complete program encompassing enterprise-wide policy, technology, and the role of people. These are often broadly defined or required by formal Risk Management Frameworks and processes.

A comprehensive treatment of this topic is beyond the scope of the Critical Security Controls. However, the actions in CSC 6 provide specific, high-priority steps that can improve Application Software Security. In addition, we recommend use of the many excellent comprehensive resources dedicated to this topic. Examples include: the DHS "Build Security In" Program < buildsecurityin.us-cert.gov >, and The Open Web Application Security Project (OWASP) < www.owasp.org >.

CSC 18 System Entity Relationship Diagram



CSC 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Why Is This Control Critical?

Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not "if" but "when."

When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place.

CSC 19: Incident Response and Management				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**19.1**	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.	**Y**	
Application	**19.2**	Assign job titles and duties for handling computer and network incidents to specific individuals.	**Y**	
Application	**19.3**	Define management personnel who will support the incident handling process by acting in key decision-making roles.	**Y**	
Application	**19.4**	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.	**Y**	

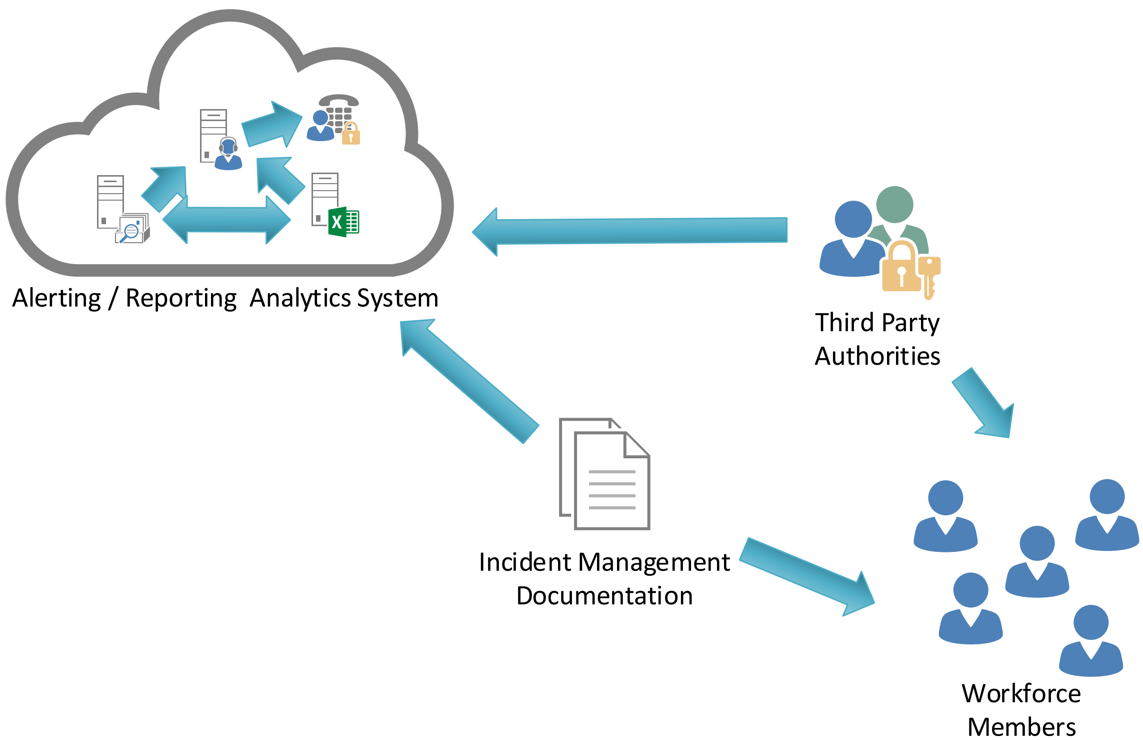
Family	CSC	Control Description	Foun-dational	Advanced
Application	**19.5**	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).	**Y**	
Application	**19.6**	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	**Y**	
Application	**19.7**	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.	**Y**	

CSC 19 Procedures and Tools

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents.

A full treatment of this topic is beyond the scope of the Critical Security Controls. However, the actions in CSC 18 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive incident and response plan.

CSC 19 System Entity Relationship Diagram



CSC 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Why Is This Control Critical?

Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include: the time window between announcement of a vulnerability, the availability of a vendor patch, and actual installation on every machine; well-intentioned policies which have no enforcement mechanism (especially those intended to restrict risky human actions); failure to apply good configurations and other practices to the entire enterprise, or to machines that come in-and-out of the network; and failure to understand the interaction among multiple defensive tools, or with normal system operations that have security implications.

In addition, successful defense requires a comprehensive program of technical defenses, good policy and governance, and appropriate action by people. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness.

Penetration testing starts from the identification and assessment of vulnerabilities that can be identified in the enterprise. It complements this by designing and executing tests that demonstrate specifically how an adversary can either subvert the organization's security goals (e.g., the protection of specific Intellectual Property) or achieve specific adversarial objectives (e.g., establishment of a covert Command and Control infrastructure). The result provides deeper insight, through demonstration, into the business risks of various vulnerabilities.

Red Team exercises take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future implementation.

CSC 20: Penetration Tests and Red Team Exercises				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**20.1**	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.	**Y**	
Application	**20.2**	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	**Y**	
Application	**20.3**	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	**Y**	
Application	**20.4**	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.	**Y**	
Application	**20.5**	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.	**Y**	
Application	**20.6**	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	**Y**	
Application	**20.7**	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.		**Y**

Family	CSC	Control Description	Foun-dational	Advanced
Application	**20.8**	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.		**Y**

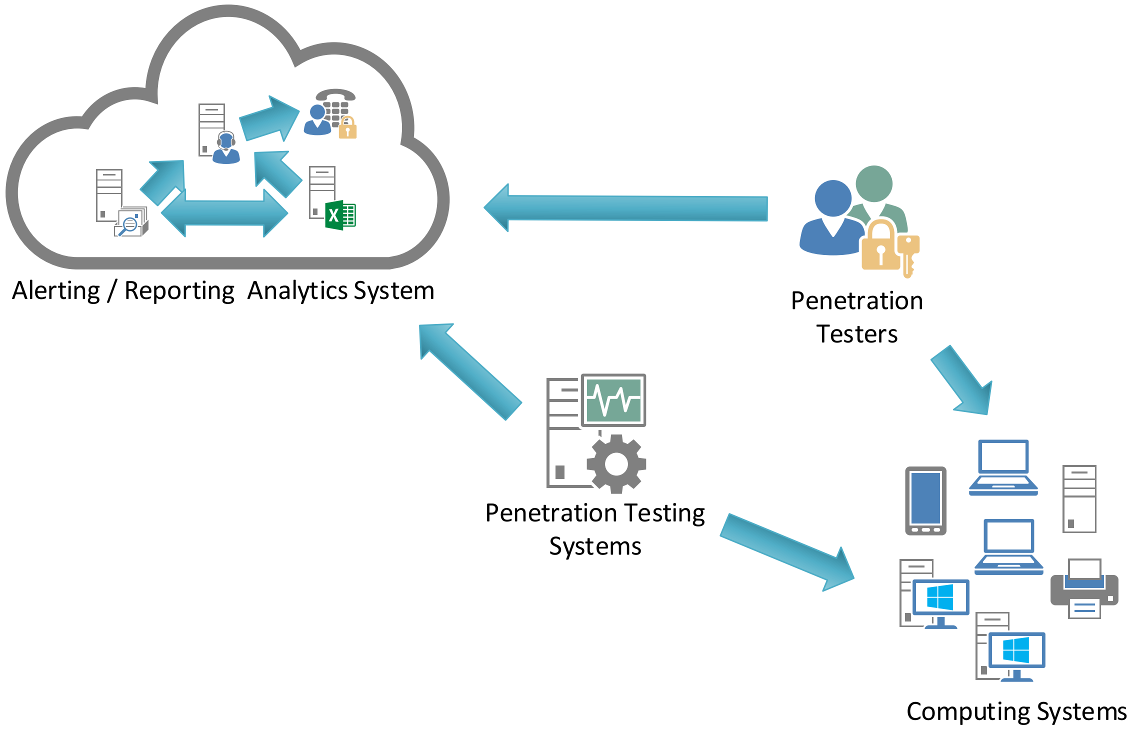
CSC 20 Procedures and Tools

Penetration testing and Red Teaming only provide significant value when basic defensive measures have already been put into place, and when they are performed as part of a comprehensive, ongoing program of security management and improvement. These are often specified and required by formal Risk Management Frameworks and processes.

Each organization should define a clear scope and rules of engagement for penetration testing and Red Team analyses. The scope of such projects should include, at a minimum, systems with the organization's highest value information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration tests and Red Team analyses should describe, at a minimum, times of day for testing, duration of tests, and the overall test approach.

A full treatment of this topic is beyond the scope of the CIS Critical Security Controls. However, the actions in CSC 20 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive penetration testing and Red Team program.

CSC 20 Entity Relationship Diagram



Appendix A: Evolving An Attack Model for the CIS Critical Security Controls.

Background

Since their inception, the CIS Critical Security Controls ("the Controls") have had a basic tenet of *"Offense Informs Defense"*. That is, knowledge of actual attacks that have compromised systems (the Bad Guys' "offense") is the key factor to inform and determine the value of defensive actions. You may not be able to afford to do everything you want or need to do and so cyber defense must be driven by prioritization – what should I do first to get the most value from my defensive resources? We believe that **value** is best determined by the attacker – what are they doing to us now, and what are the most useful, scalable actions we can take to stop them?

The Controls reflect and knowledge of actual attacks and effective defenses gathered from experts from every part of the ecosystem across many sectors. To do this, a team reviewed and analyzed attack data from many of the leading vendor threat reports to ensure the Controls adequately aligned with the most prevalent threats. We call this process a **"Community Attack Model"** for the CIS Critical Security Controls – the gathering of relevant real-life information about attacks and putting them into context so they can be easily and reliably mapped to defensive action. "Community" refers to the breadth of the participants and information sources, and also to the shared labor that operates this process. But we also emphasize that these are the threats that the entire Community faces – the documented, specific successes of the Attackers. Any one specific category of attack might not have hit you today, but it could just as easily do so tomorrow.

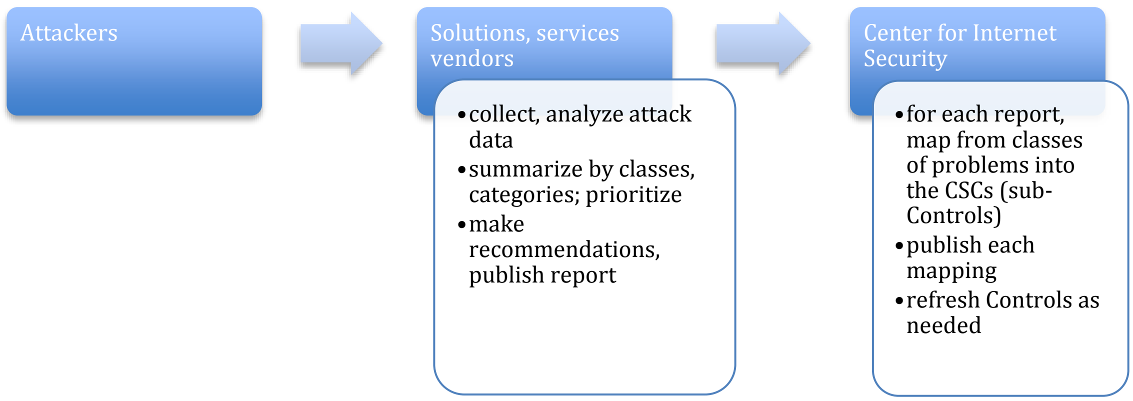
A Community Approach to Understanding Attacks and Threats

The Community Attack Model began by validating and enriching mapping from a well-documented and authoritative source of "real life" data – the Verizon Data Breach Investigations Report (2013, 2014, 2015). After the Verizon team did their primary analysis, a volunteer panel formed by the Center for Internet Security worked with them to map the most important categories of attacks seen in the prior year's data directly in the Controls (at a sub-Control) level, and this map became a key part of the Verizon DBIR Recommendations. More recently, we completed similar mappings using annual reports working with Symantec Internet Security Report 2015 and HP Cyber Risk Report 2015. This approach allows readers of these data-driven annual reports to easily and consistently map into the Controls.

A couple of key points to note about this workflow.

- The mapping is from the vendor's category or summary level of attacks – not from data about every individual attack.

- The data is created by the vendor's business model (e.g., incident response, managed security, anti-malware sensors, threat intelligence), and so each represents an incomplete but well-documented sampling of the ecosystem.
- The categories used by the vendors are typically in narrative form, and not presented in any standard form or taxonomy. Recommendations are also typically in narrative form, not tied to any specific defensive framework. Therefore, mapping from any one vendor's report to the Controls requires some discussion and analytic judgment.



The use of this attack information and the selection of appropriate defensive action can be seen as part of a broader **"Foundational Risk Assessment"** of understanding vulnerabilities, the threats and the resulting consequences – one that can be used by an individual enterprise as a starting point for immediate, high-value action, and can also provide a basis for common action across an entire community.

Building An Operational Attack Model

As the community around the Controls has grown in size and diversity, and as the environment has grown more complex, we must evolve this Model to be more scalable, repeatable, adaptable to different communities, and more consistent with formal security frameworks – all without disrupting the spirit of cooperation and common good that has brought us this far.

Whether you approach this problem as an individual enterprise or as a community of enterprises, you must create and operate an ongoing, repeatable process to find relevant new information about Attackers, assess the implications for your environment, make key decisions, and then take action. Doing so will help determine your best investments both tactically and strategically.

A useful model will have a number of essential attributes.

- It should be driven by data from authoritative, publicly available sources, but also be able to make use of specialized (e.g., uniquely applicable to a sector) or restricted (e.g., encumbered by classification or agreement) knowledge.
- It should have a well-defined process to translate from attacks to action (controls) in a way that supports prioritization and is consistent with formal Risk Management Frameworks.
- It should have an on-going “refresh” cycle that allows validation of prior defensive choices, as well as assessment of new information.
- It should be low cost, and preferably shared cost across a community.
- It should be openly demonstrable to others and negotiable (since your risk is always shared with others).

So the evolution of the CIS Critical Security Controls will follow the above guidelines to continually enrich and refresh the Controls. It will expand the number and variety of threat reports, develop a standard categorization or taxonomy of attacks to map to other frameworks and will take advantage of existing avenues for information sharing, such as using the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Appendix B: Attack Types

Historically, the following Attack Types were the primary ones considered when developing the Critical Security Controls. The types were also mapped back into the Controls as part of the discussion to ensure good coverage by the Controls. This approach has been phased out in favor of the CIS Community Attack Model.

Attack Summary
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.
Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness.
Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools.
Attackers scan for remotely accessible services on target systems that are often unneeded for business activities, but provide an avenue of attack and compromise of the organization.
Attackers exploit weak application software, particularly web applications, through attack vectors such as SQL injection, cross-site scripting, and similar tools.
Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information.
Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness.
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.

Attackers trick a user with an administrator-level account into opening a phishing-style email with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges.
Attackers exploit boundary systems on Internet-accessible DMZ networks, and then pivot to gain deeper access on internal networks.
Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions.
Attackers operate undetected for extended periods of time on compromised systems because of a lack of logging and log review.
Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information.
Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees.
Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which is then used to propagate to other victim machines across an enterprise.
Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization.
Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information.
Attackers operate undiscovered in organizations without effective incident-response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state.

Appendix C: The NIST Framework for Improving Critical Infrastructure Cybersecurity

Since its release in February 2014, The NIST *Framework for Improving Critical Infrastructure Cybersecurity* has become a major part of the national conversation about cybersecurity for the critical infrastructure (and beyond), and we believe it represents an important step towards large-scale and specific improvements in security for the United States and internationally. The Center for Internet Security was an active participant in the development of the Framework, and the CIS Critical Security Controls are called out as one of the "Informative References" that can be used to drive specific implementation.

The Framework is true to its name – "a set of principles, ideas, etc. that you use when you are forming your decisions and judgments" (from the MacMillan Dictionary) – and it provides a way to organize, conduct, and drive the conversation about security goals and improvements, for individual enterprises and across communities of enterprises. But it does not include any specific risk management process, or specify any priority of action. Those "decisions and judgments" are left to the adopter to manage for their specific situation and context.

We believe that for the vast majority of enterprises, the best approach to solving these problems is to tackle them as a community – not enterprise-by-enterprise. This is the essence of the CIS non-profit community model, and is embodied in projects like the CIS Critical Security Controls, the CIS Security Configuration Benchmarks, and the National Cyber Hygiene Campaign. We need to band together to identify key actions, create information, share tools, and remove barriers so that we can all succeed.

In that spirit the Center for Internet Security will continue to support the evolution of the Framework, and also help our community leverage the content, processes, and priorities of the CIS Critical Security Controls as an action mechanism in alignment with the NIST Cybersecurity Framework.

Below is an example of the working aids that CIS maintains to help our community leverage the Framework. This chart shows the mapping from the Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.

	Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V6.0)	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC 1: Inventory of Authorized and Unauthorized Devices	AM				
CSC 2: Inventory of Authorized and Unauthorized Software	AM				

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core				
	Identify	Protect	Detect	Respond	Recover
CSC 3: Secure Configuration of End user devices		IP			
CSC 4: Continuous Vulnerability Assessment and Remediation	RA		CM	MI	
CSC 5: Controlled Use of Administrative Privileges		AC			
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
CSC 7: Email and Web Browser Protections		PT			
CSC 8: Malware Defense		PT	CM		
CSC 9: Limitation and Control of Network Ports, Protocols, and Service		IP			
CSC 10: Data Recovery Capability					RP
CSC 11: Secure Configuration of Network Devices		IP			
CSC 12: Boundary Defense			DP		
CSC 13: Data Protection		DS			
CSC 14: Controlled Access Based on Need to Know		AC			
CSC 15: Wireless Access Control		AC			
CSC 16: Account Monitoring and Control		AC	CM		
CSC 17: Security Skills Assessment and Appropriate Training		AT			
CSC 18: Application Software Security		IP			
CSC 19: Incident Response and Management			AE	RP	
CSC 20: Penetration Tests and Red Team Exercises				IM	IM

Appendix D: The National Cyber Hygiene Campaign

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementation of the CIS Critical Security Controls. Although the Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer.

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using "known good" configurations? (CSC 3)
- Are we continuously looking for and managing "known bad" software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in "plain language" by the Top 5 Priorities of the Campaign: **"Count, Configure, Control Patch, Repeat".** To support the Campaign, volunteers have created documentation and "toolkits" to guide implementation.

Although the language is simple and catchy, behind the scenes each of these questions is associated with a primary Control that provides an action plan. The Campaign is also designed to be in alignment with the first 5 of the CIS Critical Security Controls, the Australian Signals Directorate's (ASD) "Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation (CDM) Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

The National Campaign for Cyber Hygiene has been jointly adopted by the Center for Internet Security (home of the Multi-State Information Sharing and Analysis Center) and the National Governor's Association Homeland Security Advisory Council (GHSAC) as a foundational cybersecurity program across many State, Local, Tribal, and Territorial governments and offers toolkits and resources for any public or private organization.

For more information, go to www.cisecurity.org.

Appendix E: Critical Governance Controls and the CIS Critical Security Controls

Cybersecurity governance is a key responsibility of the board of directors and senior executives, and it must be an integral part of overall enterprise governance. Because of its dynamic nature, cybersecurity governance must also be aligned with an *operational* cybersecurity framework.

To exercise effective governance, executives must have a clear understanding of what to expect from their information security program. They need to know how to direct the implementation, evaluate their own status with regard to existing security programs, and determine the strategy and objectives of an effective security program.

How the CIS Critical Security Controls Can Help

The Controls are actionable, automated activities that detect and prevent attacks against your network and most important data. They support enterprise security governance programs by bridging the gap from an executive view of business risk to a technical view of specific actions and operational controls to manage those risks. Key executive concerns about information security risks can be translated into specific programs for security improvement, and also into day-to-day security tasks for front-line personnel. This allows better alignment top-to-bottom of corporate risk management. Also, since the Controls are created and supported by a large independent community of practitioners and vendors, they provide a specific, supported, and open baseline for measurement and negotiation about security improvement – one that is demonstrably in alignment with essentially all formal regulatory, governance, and oversight frameworks.

From Governance to the CIS Critical Security Controls

To help improve your company's ability to manage information risks, here are some sample steps to help you align corporate governance concerns with the implementation of security controls. These examples identify the primary, but not the only, CIS Critical Security Controls which should be implemented.

Governance item #1: *Identify your most important information assets and the impact on your business or mission if they were to be compromised.*

> Information is the lifeblood of every modern enterprise, and the movement, storage, and control of that information is inextricably bound to the use of Information Technology. Therefore the following CIS Critical Security Controls are the primary means to track and control the system components that manage the flow, presentation, and use of information.
>
> **CSC 1—Inventory of Authorized and Unauthorized Devices**
>
> **CSC 2—Inventory of Authorized and Unauthorized and Software**

Governance Item #2: *Manage the known cyber vulnerabilities of your information and make sure the necessary security policies are in place to manage the risk.*

At a minimum, you should be able to identify and manage the large volume of *known* flaws and vulnerabilities found in Information Technology and processes. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported.

CSC 3: Secure Configurations of Hardware and Software

CSC 4: Continuous Vulnerability Assessment and Remediation

Governance Item #3: *Clearly identify the key threats to your information and assess the weaknesses in your defense.*

Threats to your information, systems, and processes evolve constantly. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported.

CSC 8: Malware Defenses

CSC 20: Penetration Tests and Red Team Exercises

Governance Item #4: *Confirm and control who has access to the most important information.*

Ensuring that the right people have access to corporate data and ensuring privileges are managed accurately can reduce the impact of unauthorized access, both from internal threats and external. The following CIS Critical Security Controls are the primary means to establish a baseline of responsible practices to identify needs and manage access.

CSC 5: Controlled Use of Administrative Privileges

CSC 14: Controlled Access Based on the Need to Know

A fundamental goal of information security is to reduce adverse impacts on the organization to an acceptable level of risk. Therefore, a crucial metric comprises the adverse impacts of information security incidents experienced by the company. An effective security program will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time.

Developing an Overall Governance Strategy

While the CIS Critical Security Controls provide an effective way to plan, prioritize, and implement primarily *technical* controls for cyberdefense, they are best used as part of a holistic information governance program – one that also addresses policies, standards, and guidelines that support technical implementations. For example, conducting an inventory of devices on your network is an important technical best practice, but an organization must also define and publish policies and processes that clearly communicate to employees the purpose of these controls, what is expected of them and the role they play in protecting the company's interests.

The following topics provide a useful framework for developing your overall governance strategy. Based on our experience, these are prioritized based on their impact in building and supporting an effective information assurance program.

Executive Sponsorship: Develop information assurance charters with roles and responsibilities, steering committees, and board of director briefings to establish support and leadership from executives.

Information Assurance Program Management: Define management and resource allocation controls, such as budgeting, and prioritization to govern information assurance programs under executive sponsorship.

Information Assurance Policies and Standards Management: Define and document policies and standards to provide detailed guidance regarding how security controls will be completed to promote consistency in defense.

Data Classification: Identify, prioritize and label data assets, including analog or physical assets.

Risk Management: Identify thoughtful and purposeful defense strategies based on priority decisions on how best to defend valuable data assets.

Compliance and Legal Management: Address compliance requirements based on the regulatory and contractual requirements placed on your organization.

Security Awareness and Education: Establish education plans for all workforce members to ensure that they have the necessary skills to protect information assets as a part of their responsibilities.

Audit and Assessment Management: Conduct audits and assessments to ensure that information assurance efforts are consistent with the standards you have defined and to assist in your efforts to manage risk.

Personnel and Human Resources Management: Specify personnel and human resources controls to manage the way people interact with data assets. People, as well as technology controls, are critical for the defense of information assets.

Budgets and Resource Management: Allocate appropriate resources in order to be effective at defense. Information assurance architectures are vital for defense, but without budgets and resources, such plans will never be effective.

Physical Security: Protect the equipment, buildings, and locations where data assets are stored to provide a foundation for the logical security of data assets.

Incident Response Management: Specify the planned management of how you will respond in the face of potentially adverse events. This acts as a component of business continuity and disaster management.

Business Continuity and Disaster Recovery Management: Specify resiliency controls to help mitigate potential losses due to potential disruptions to business operations.

Procurement and Vendor Management: Partner with business associates in defending their data assets. The Controls define how an organization aligns with third parties and vendors to protect their data assets.

Change and Configuration Management: Assess, accept or deny, and log changes to systems, especially configuration changes in a systematic formal manner in order to defend the organization's information assets.

Organizations are encouraged (and many are required) to implement these governance controls in parallel with the technical controls defined elsewhere in this document. Both technical and governance related controls should be considered equally important pillars in the architecture of an organization's defense.

Appendix F: Toward A Privacy Impact Assessment (PIA) for the CIS Critical Security Controls

Introduction

An effective posture of enterprise cybersecurity need not, and, indeed, should not compromise individual privacy. Many laws, regulations, guidelines, and recommendations exist to safeguard privacy, and enterprises will, in many cases, adapt their existing policies on privacy as they apply the Controls.

At a minimum, use of the Controls should conform to the general principles embodied in the *Fair Information Practice principles* (FIPs) [2] and in *Privacy by Design.*[3] All enterprises that apply the Controls should undertake – and make available to stakeholders – privacy impact assessments of relevant systems to ensure that appropriate protections are in place as the Controls are implemented. Every enterprise should also regularly review these assessments as material changes to its cybersecurity posture are adopted. The aim is to assess and mitigate the major potential privacy risks associated with implementing specific Controls as well as evaluate the overall impact of the Controls on individual privacy.

To assist enterprises in efforts to conduct a privacy impact assessment when implementing the Controls and to contribute to the establishment of a more general reference standard for privacy and the Controls, CIS will convene technical and privacy experts to review each Control and offer recommendations for best practice.

The following framework will help guide this effort and provide a possible outline for a Privacy Impact Assessment.

Privacy Impact Assessment of the CIS Critical Security Controls

I. Overview

Outline the purpose of each Control and provide justification for any actual or potential intersection with privacy-sensitive information.

- Where possible, identify how technologies, procedures, and data flows are used to implement the Control. Provide a brief description of how the Control generally

[2] See http://www.dhs.gov/publication/fair-information-practice-principles-fipps, and http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[3] See https://www.privacybydesign.ca. The approach discussed in this Annex draws heavily on public sector approaches in the United States, but can be adapted for any jurisdiction.

collects and stores information. Identify the type of data collected by the Control and the kinds of information that can be derived from this data. In discussing how the Control might collect and use PII, include a typical transaction that details the life cycle of that PII from collection to disposal.

- Describe the measures necessary to protect privacy data and mitigate any risks of unauthorized access or inadvertent disclosure of the data. The aim here is not to list every possible risk to privacy, but rather, to provide a holistic view of the risks to privacy that could arise from implementation of the Control.
- Describe any potential ad-hoc or routine information sharing that will result from the implementation of the Control both within the enterprise and with external sharing partners. Also describe how such external sharing is compatible with the original collection of the information, and what agreements would need to be in place to support this sharing.

II. Authorities

Identify the legal authorities or enterprise policies that would permit or, conversely, limit or prohibit the collection or use of information by the Control.

- List the statutory and regulatory authorities that would govern operation of the Control, including the authorities to collect the information identified above. Explain how the statutory and regulatory authorities permit or would limit collection and use of the information or govern geographic storage requirements. If the Control would conceivably collect Personally Identifiable Information (PII), also identify the specific statutory authority that would permit such collection.
- Would the responsible office of an enterprise be able to rely on authorities of another parent organization, subsidiary, partner or agency?
- Might the information collected by the Control be received from a foreign user, organization or government? If so, do any international agreement, contract, privacy policy or memorandum of understanding exist to support or otherwise govern this collection?

III. Characterizing Control-Related Information

Identify the type of data the Control collects, uses, disseminates, or maintains.

- For each Control, identify both the categories of technology sources, logs, or individuals from whom information would be collected, and, for each category, list any potential PII, that might be gathered, used, or stored to support the Control.
  - Relevant information here includes (but is not limited to): name; date of birth; mailing address; telephone numbers; social security number; e-mail address; mother's maiden name; medical records locators; bank account numbers; health plan beneficiaries; any other account numbers; certificates or other license numbers; vehicle identifiers, including license plates;

marriage records; civil or criminal history information; medical records; device identifiers and serial numbers; education records; biometric identifiers; photographic facial images; or any other unique identifying number or characteristic.

- If the output of the Control, or system on which it operates, creates new information from data collected (for example, a scoring, analysis, or report), this might this new information have privacy implications? If so, perform the same above analysis on the newly created information.
- If the Control uses information from commercial sources or publicly available data to enrich other data collected, explain how this information might be used.
    - Commercial data includes information from data aggregators (such as Lexis Nexis, threat feeds, or malware databases), or from social networking sources where the information was originally collected by a private organization.
    - Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.
    - Identify scenarios with this enriched data might derive data that could have privacy implications. If so, perform the same above analysis on the newly created information.
- Identify and discuss the privacy risks for Control information and explain how they are mitigated. Specific risks may be inherent in the sources or methods of collection.
- Consider the following Fair Information Practice principles (FIPs):
    - *Principle of Purpose Specification:* Explain how the collection of PII by the Control links to the cybersecurity needs of the enterprise.
    - *Principle of Minimization:* Is the PII data directly relevant and necessary to accomplish the specific purposes of the Control?
    - *Principle of Individual Participation:* Does the Control, to the extent possible and practical, collect PII directly from individuals?

IV. Uses of Control-Related Information

Describe the Control's use of PII or privacy protected data. Describe how and why the Control uses this data.

- List likely uses of the information collected or maintained, both internal and external to the enterprise. Explain how and why different data elements will be used. If Social Security numbers are collected for any reason, for example, describe why such collection is necessary and how such information would be used. Describe types of procedures and protections to be in place to ensure that information is handled appropriately, and policies that need to be in place to provide user notification.
- Does the Control make use of technology to conduct electronic searches, queries, or analyses in a database to discover or locate a predictive pattern or an anomaly? If

so, describe what results would be achieved and if there would be possibility of privacy implications.

- Some Controls require the processing of large amounts of information in response to user inquiry or programmed functions. The Controls may help identify data that were previously not identifiable and may generate the need for additional research by analysts or other employees. Some Controls are designed to perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.
- Discuss the results generated by the uses described above, including link analysis, scoring, or other analyses. These results may be generated electronically by the information system, or manually through review by an analyst. Would these results potentially have privacy implications?
- Are there other offices or departments within or connected to the enterprise that would receive any data generated? Would there be privacy implications to their use or collection of this data?
- Consider the following FIPs:
    - *Principle of Transparency:* Is the PIA and related policies clear about the uses of information generated by the Control?
    - *Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the Control?

V. Security

Complete a security plan for the information system(s) supporting the Control.

- Is there appropriate guidance when implementing the Control to ensure that appropriate physical, personnel, IT, and other safeguards are in place to protect privacy protected data flowing to and generated from the Control?
- Consider the following Fair Information Practice principle:
    - *Principle of Security*: Is the security appropriate and proportionate to the protected data?

VI. Notice

Identify if any notice to individuals must be put in place regarding implementation of the Control, PII collected, the right to consent to uses of information, and the right to decline to provide information (if practicable).

- Define how the enterprise might require notice to individuals prior to the collection of information.
- Enterprises often provide written or oral notice to employees, customers, shareholders, and other stakeholders before they collect information from individuals. In the U.S. government, that notice may include a posted privacy policy, a Privacy Act statement, a Privacy Impact Assessment, or a Statement of Records

Notice (SORN) published in the *U.S. Federal Register*. For private companies, collecting information from consumers, publicly available privacy policies are used. Describe what notice might be relevant to individuals whose information might be collected by the Control.

- If notice might not, or cannot be provided, define if one is required or how it can be mitigated. For certain law enforcement operations, notice may not be appropriate – enterprises would then explain how providing direct notice to the individual at the time of collection would undermine a law enforcement mission.
- Discuss how the notice provided corresponds to the purpose of the Control and the declared uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how implementation of the Control mitigates the risks associated with potentially insufficient notice and opportunity to decline or consent.
- Consider the following FIPs:
  - *Principle of Transparency*: Will this Control allow sufficient notice to be provided to individuals?
  - *Principle of Use Limitation:* Is the information used only for the purpose for which notice was provided either directly to individuals or through a public notice? What procedures can be put in place to ensure that information is used only for the purpose articulated in the notice?
  - *Principle of Individual Participation*: Will the enterprise be required to provide notice to individuals regarding redress, including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

VII. Data Retention

Will there be a requirement to develop a records retention policy, subject to approval by the appropriate enterprise authorities (e.g., management, Board), to govern information gathered and generated by the Control?

- Consider the following FIPs below to assist in providing a response:
  - *Principle of Minimization:* Does the Control have the capacity to use only the information necessary for declared purposes? Would the Control be able to manage PII retained only for as long as necessary and relevant to fulfill the specified purposes?
  - *Principle of Data Quality and Integrity:* Does the PIA describe policies and procedures required by an organization for how PII is purged once it is determined to be no longer relevant and necessary?

VIII. Information Sharing

Describe the scope of the information sharing within and external to the enterprise that could be required to support the Control. External sharing encompasses sharing with other *businesses, vendors, private sector groups, or federal, state, local, tribal, and territorial government, as well as with governments or official agencies of other countries.*

- For state or local government agencies, or private sector organizations list the general types that might be applicable for the Control, rather than the specific names.
- Describe any agreements that might be required for an organization to conduct information sharing as part of normal enterprise operations.
- Discuss the privacy risks associated with the sharing of information outside of the enterprise. How can those risks be mitigated?
- Discuss how the sharing of information is compatible with the stated purpose and use of the original collection for the Control.

IX. Redress

Enterprises should have in place procedures for individuals to seek redress if they believe their PII may have been improperly or inadvertently disclosed or misused through implementation of the Controls. These procedures may include allowing them to file complaints about what data is collected or how it's used.

- Consider the following issue that falls under the FIP principle of *Individual Participation*:
    - Can a mechanism be applied by which an individual can prevent PII obtained for one purpose from being used for other purposes without the individual's knowledge?

X. Auditing and Accountability

Describe what technical and policy based safeguards and security measures might be needed to support the Control. Include an examination of technical and policy safeguards, such as information sharing protocols, special access restrictions, and other controls.

- Discuss whether the Control allows for self-audits, permits third party audits, or allows real time or forensic reviews by appropriate oversight agencies.
- Do the IT systems supporting the Control have automated tools to indicate when information is possibly being misused?
- Describe what requirements for privacy training should be provided to users either generally or specifically relevant to the Control, including information handling procedures and sensitivity of information. Discuss how individuals who have access to PII collected or generated by the Control should be trained to appropriately handle that information.
- Discuss the types of processes and procedures necessary to review and approve information sharing agreements, new uses of Control information, and new access to Control information by other parties.

Appendix G: Categorization for the CIS Critical Security Controls

Introduction

When we created Version 6 of the CIS Controls, one of the notable changes was deletion of the "categories" for each sub-Control (*Quick Win, Visibility and Attribution, Improved Security Configuration and Hygiene, and Advanced).* These had proved to be problematic for several reasons, and a number of people found them to be more inconsistent than useful.

But other adopters told us they missed the categories and found them helpful in prioritizing their Controls implementation plans, especially in presenting those plans to management, so we went back to take another look at them. In addition, people asked for more help in identifying sub-controls that were truly "advanced" and would require substantial investment of time and resources.

This document presents a simpler categorization scheme for each sub-control, along with some explanatory information to separate actions that we consider "Foundational" from those that are "Advanced".

Description

In Version 5 of the CIS Controls, each sub-category was identified in one of the following categories:

- ***Quick wins*** that provide significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide such substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.
- ***Visibility and attribution measures*** to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.
- ***Improved information security configuration and hygiene*** to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- ***Advanced sub-controls*** that use new technologies or procedures that provide maximum security but are harder to deploy or more expensive or require more highly skilled staff than commoditized security solutions.

For Version 6.1, we made this simpler and moved to a 2-category system. As a starting point, we worked from the original Version 5 categories since most of the sub-controls carried over in some form.

- ***Foundational:*** These provide essential improvements to the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack. They reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- ***Advanced:*** These are sub-controls that use new technologies or procedures for maximum security, but are harder to deploy or more expensive or require more highly skilled staff than commoditized security solutions.

However a number of adopters noted that some of the individual sub-controls contain wording, phrases, or an interpretation that did not fall neatly into either category. So for each of those, we identified a primary category (Foundational or Advanced, shown as "Y" in one column of the charts); and then we added text to clarify and separate out the other aspect of the sub-control.

For example, we might identify a given sub-control as Foundational, but those seeking to build upon the sub-control for an Advanced security program now have some guidance. This is not a particularly elegant solution, but we wanted to provide useful guidance without a significant rewrite of the sub-controls. Enterprises adopting the Controls do something like this anyway – interpret each of the sub-controls in the context of their specific situation, technical base, and risk management – in order to create a roadmap of phased implementation.