NIST Cybersecurity Framework Core:
Informative Reference Standards

CCS CSC

(Council on CyberSecurity Top 20 Critical Security Controls)

4/1/14

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 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.

How to Implement This Control

ID #	Description	Category
CSC 1-1	Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	Quick win
CSC 1-2	Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.	Quick win
CSC 1-3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected	Quick win

	to the network.	
CSC 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.	Visibility/ Attribution
CSC 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.	Configuration/ Hygiene
CSC 1-6	Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.	Configuration/ Hygiene
CSC 1-7	Utilize client certificates to validate and authenticate systems prior to connecting to the private network.	Advanced

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 the business 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 looking 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 churn significantly. 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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take to detect new devices added to the organization's network (time in minutes)?
2. How long does it take the scanners to alert the organization's administrators that an unauthorized device is on the network (time in minutes)?
3. How long does it take to isolate/remove unauthorized devices from the organization's network (time in minutes)?
4. Are the scanners able to identify the location, department, and other critical details about the unauthorized system that is detected (yes or no)?

CSC 1 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

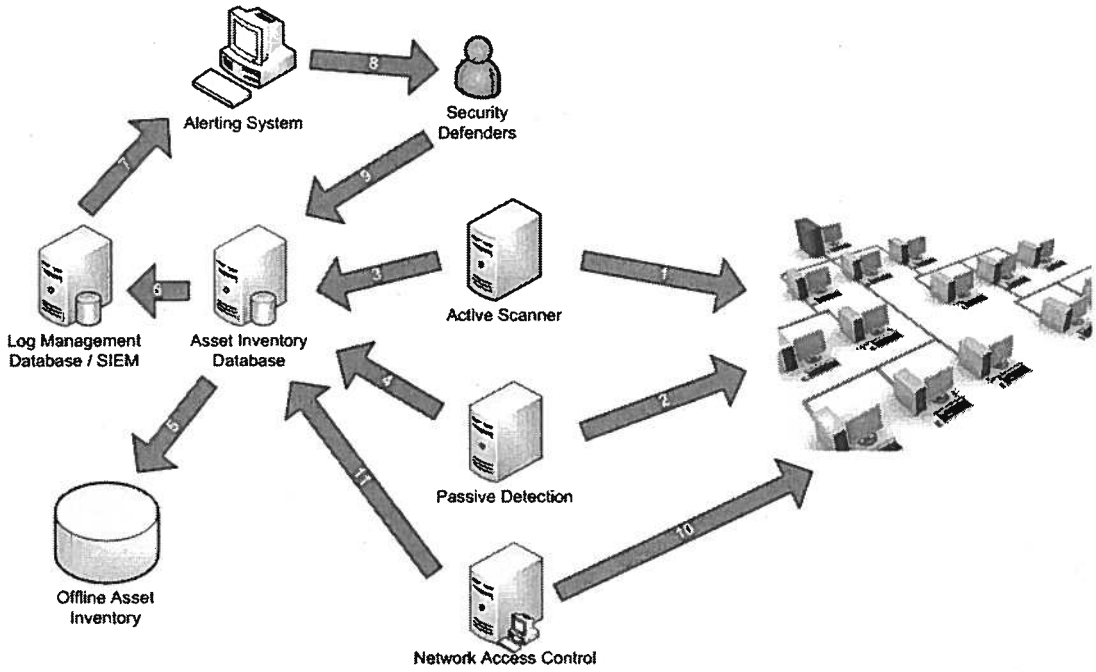
1. How many unauthorized devices are presently on the organization's network (by business unit)?
2. How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?
3. What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) to authenticate to the organization's network (by business unit)?
4. What is the percentage of systems on the organization's network that are not utilizing Network Access Control (NAC) with client certificates to authenticate to the organization's network (by business unit)?

CSC 1 Effectiveness Test

To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network, including a selection of subnets associated with demilitarized zones (DMZs), workstations, and servers. Two of the systems must be included in the asset inventory database, while the other systems are not. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team must verify that the system provides details of the location of all the test machines connected to the network. For those test machines included in the asset inventory, the team must also verify that the system provides information about the asset owner.

CSC 1 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining hardware devices on the organization's network. These systems should be able to identify if new systems are introduced into the environment that have not been authorized by enterprise personnel. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Active device scanner scans network systems

Step 2: Passive device scanner captures system information

Step 3: Active scanner reports to inventory database

Step 4: Passive scanner reports to inventory database

Step 5: Inventory database stored offline

Step 6: Inventory database initiates alert system

Step 7: Alert system notifies security defenders

Step 8: Security defenders monitor and secure inventory database

Step 9: Security defenders update secure inventory database

Step 10: Network access control continuously monitors network

Step 11: Network access control checks and provides updates to the asset inventory database.

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.

How to Implement This Control

ID #	Description	Category
CSC 2-1	Deploy application whitelisting technology 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	*Quick win (One of the "First Five")*

	of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (isolating the custom software in a virtual operating system that does not retain infections.).	
CSC 2-2	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.	Quick win
CSC 2-3	Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).	Quick win
CSC 2-4	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. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.	Visibility/ Attribution
CSC 2-5	The software inventory systems must be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location.	Visibility/ Attribution
CSC 2-6	Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked.	Configuration/ Hygiene
CSC 2-7	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.	Advanced
CSC 2-8	Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.	Advanced
CSC 2-9	Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.	Advanced

CSC 2 Procedures and Tools

Whitelisting can be implemented using commercial whitelisting tools 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 of programs allowed to run 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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take to detect new software installed on systems in the organization (time in minutes)?
2. How long does it take the scanners to alert the organization's administrators that an unauthorized software application is on a system (time in minutes)?
3. How long does it take to alert that a new software application has been discovered (time in minutes)?
4. Are the scanners able to identify the location, department, and other critical details about the unauthorized software that is detected (yes or no)?

CSC 2 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. How many unauthorized software applications are presently located on business systems within the organization (by business unit)?
2. How long, on average, does it take to remove unauthorized applications from business systems within the organization (by business unit)?
3. What is the percentage of the organization's business systems that are not running software whitelisting software that blocks unauthorized software applications (by business unit)?
4. How many software applications have been recently blocked from executing by the organization's software whitelisting software (by business unit)?

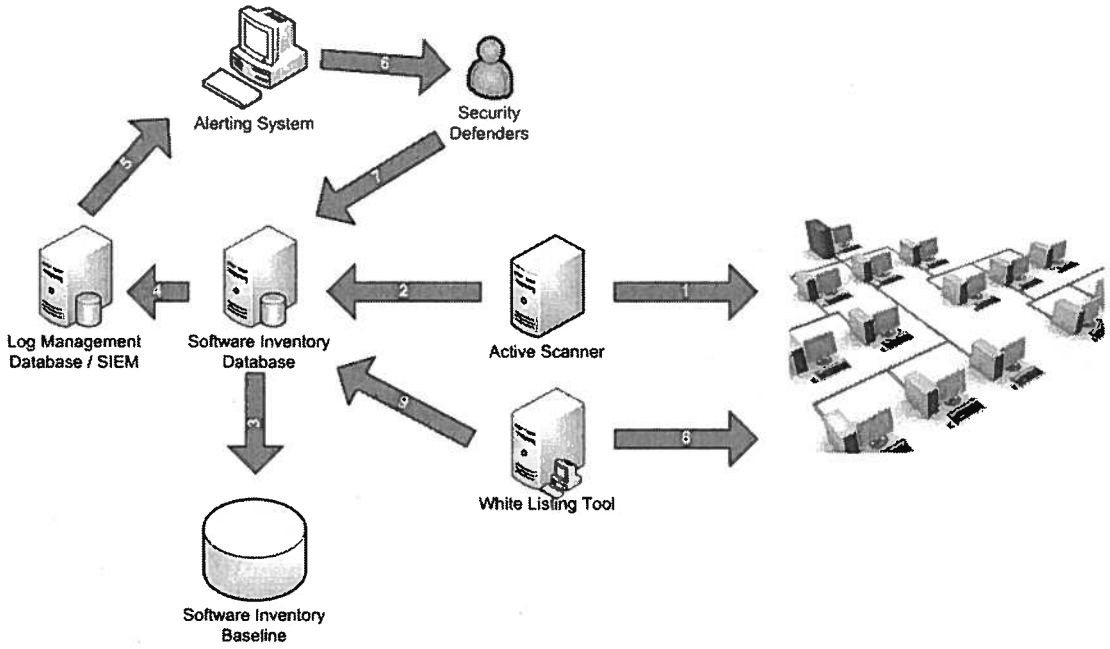
CSC 2 Effectiveness Test

To evaluate the implementation of Control 2 on a periodic basis, the evaluation team must move a benign software test program that is not included in the authorized software list to 10 systems on the network. Two of the systems must be included in the asset inventory database, while the other systems do not need to be included. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the new software within 24 hours. The team must also verify that the alert or e-mail is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team must verify that the system provides details of the location of each machine with this new test software, including information about the asset owner. The evaluation team must then verify that the software is blocked by attempting to execute it and verifying that the software is not allowed to run.

On systems where blocking is not allowed or blocking functionality is not available, the team must verify that the execution of unauthorized software is detected and results in a notification to alert the security team that unauthorized software is being used.

CSC 2 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining software installed on the organization's network systems. These systems should be able to identify if new software is introduced to the environment that has not been authorized by enterprise personnel. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Active device scanner

Step 2: Active scanner reports to inventory database

Step 3: Inventory database compares to inventory baseline

Step 4: Inventory database initiates alerting system

Step 5: Alert system notifies security defenders

Step 6: Security defenders monitor and secure inventory database

Step 7: Security defenders update software inventory database

Step 8: Whitelisting tool continuously monitors all systems on the network

Step 9: Whitelisting checks and makes updates to the software inventory database.

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. 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.

How to Implement This Control

ID #	Description	Category
CSC 3-1	Establish and ensure the use of standard secure configurations of your operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening typically includes: removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, configuring non-executable stacks and heaps, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and use of host-based firewalls. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	*Quick win (One of the "First Five")*
CSC 3-2	Implement automated patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, update to the	*Quick win (One of the "First Five")*

	latest version of application software. Remove outdated, older, and unused software from the system.	
CSC 3-3	Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges.	*Quick win (One of the "First Five")*
CSC 3-4	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.	*Quick win*
CSC 3-5	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.	*Quick win*
CSC 3-6	Negotiate contracts to buy systems configured securely out of the box using standardized images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.	*Visibility/ Attribution*
CSC 3-7	Do 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 or IPSEC.	*Configuration/ Hygiene*
CSC 3-8	Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. All alterations to such files should be automatically reported security personnel. The reporting system should have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations. For investigative support, the reporting system should be able to show the history of configuration changes over time and identify who made the change (including the original logged-	*Configuration/ Hygiene*

	in account in the event of a user ID switch, such as with the `su` or `sudo` command). These integrity checks should also 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; as well as detecting 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).	
CSC 3-9	Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing using features such as those included with tools compliant with Security Content Automation Protocol (SCAP), 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.	*Advanced*
CSC 3-10	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.	*Configuration/ Hygiene*

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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take to detect configuration changes to a network system (time in minutes)?
2. How long does it take the scanners to alert the organization's administrators that an unauthorized configuration change has occurred (time in minutes)?
3. How long does it take to block/quarantine unauthorized changes on network systems (time in minutes)?
4. Are the scanners able to identify the location, department, and other critical details about the systems where unauthorized changes occurred (yes or no)?
5. Are the scanners able to trigger different notifications / workflows based on the severity of the configuration variance detected?

For all of the above, consider that system priority, service level commitments, system role, and other factors may drive varying objectives for scan frequency and alert time frames on different systems. Ensure that the rationale for these classifications is clear, consistent, documented, and consistently applied. Verify that target detection and notification results are aligned with service level commitments and policies for each class of system.

CSC 3 Automation Metrics

In order to automate the collection of relevant data from these systems, the organization should gather the following information with automated technical sensors:

1. What is the percentage of business systems that are not currently configured with a security configuration that matches the organization's approved configuration standard (by business unit)?
2. What is the percentage of business systems whose security configuration is not enforced by the organization's technical configuration management applications (by business unit)?
3. What is the percentage of business systems that are not up to date with the latest available operating system software security patches (by business unit)?
4. What is the percentage of business systems that are not up to date with the latest available business software application security patches (by business unit)?
5. What is the percentage of business systems not protected by file integrity assessment software applications (by business unit)?
6. What is the percentage of unauthorized or undocumented changes with security impact (by business unit)?

CSC 3 Effectiveness Test

To evaluate the implementation of Control 3 on a periodic basis, an evaluation team must move a benign test system that does not contain the official hardened image, but that does contain additional services, ports, and configuration file changes, onto the network. This must be performed on 10 different random segments using either real or virtual systems. The evaluation team must then verify that the systems generate an alert regarding the changes to the software within the target service window, or within 24 hours – whichever is less. It is important that the evaluation team verify that all unauthorized changes have been detected. The team must also verify that the alert or e-mail is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team must verify that the system provides details of the location of each machine with the unauthorized changes, including information about the asset owner.

The evaluation team must also introduce undocumented / out-of-band configuration settings and binaries using real or virtual systems on 10 random segments. The test should include making a non-persistent change, in which a change is introduced to the primary program location (/bin, Program Files, etc.), left in place for 30-60 minutes, then reverted to the original configuration.

The evaluation team must verify that all configuration changes and binaries are detected, and that there is a record of the non-persistent changes mentioned above. The detection data should include the nature of the change made (addition, removal, alteration, owner, permissions, contents, etc.), as well as the user account that made the change.

The evaluation team must also verify that unauthorized software is blocked by attempting to execute it and verifying that it is not allowed to run. On systems where blocking is not allowed or blocking functionality is not available, the team must verify that the execution of unauthorized software is detected and results in a notification to alert the security team that unauthorized software is being used.

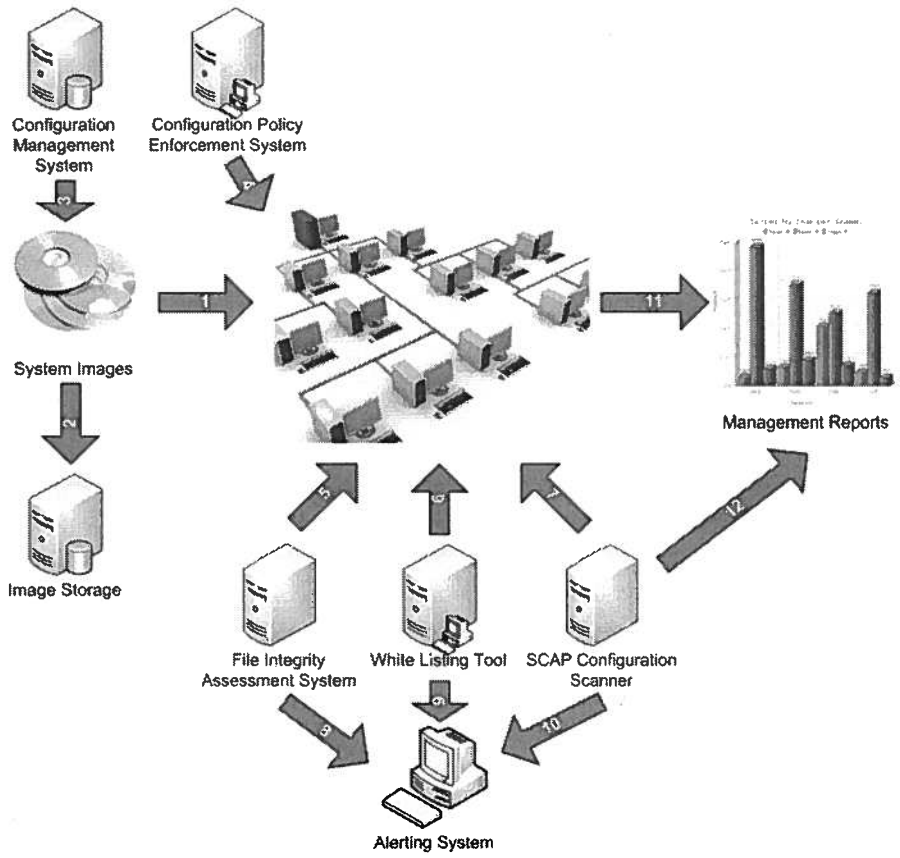
In addition to these tests, the following tests must be performed:

1. File integrity checking tools must be run on a regular basis. Any changes to critical operating system, services, and configuration files must be checked on an hourly basis. Any changes must be detected and either blocked or trigger an alert that follows the above notification process.

2. Detection software must detect the disabling of system logging, as well as the truncation, modification or deletion of log files. Note that growth of logs should not trigger notifications, but suspicious changes associated with malicious activities should; examples include deletion or truncation of logs, modification of past log events, owner or permission changes, etc. Any inappropriate changes to logs must trigger an alert that follows the above notification process.
3. System scanning tools that check for software version, patch levels, and configuration files must be run on a daily basis. Any changes must be detected and either blocked or trigger an alert that follows the above notification process.

CSC 3 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur. As with any configurations, all changes must be approved and managed by a change control process.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the devices, software, and entities used to manage and implement consistent configuration settings to workstations, laptops, and servers on the network. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Secured system images applied to computer systems

Step 2: Secured system images stored in a secure manner

Step 3: Configuration management system validates and checks system images

Step 4: Configuration policy enforcement system actively scans production systems for misconfigurations or deviations from baselines

Step 5: File integrity assessment systems monitor critical system binaries and data sets

Step 6: Whitelisting tool monitors systems configurations and software

Step 7: SCAP configuration scanner validates configurations

Step 8: File integrity assessment system sends deviations to alerting system

Step 9: Whitelisting tool sends deviations to alerting system

Step 10: SCAP configuration scanner sends deviations to alerting system

Step 11 and 12: Management reports document configuration status.

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 new vulnerabilities are reported by researchers, 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.

How to Implement This Control

ID #	Description	Category
CSC 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).	*Quick win (Supports the "First Five")*
CSC 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 themselves is logged. Second, personnel should be able to correlate attack	*Quick win*

	detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	
CSC 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.	*Quick win*
CSC 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.	*Quick win*
CSC 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.	*Visibility/ Attribution*
CSC 4-6	Carefully monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the timeframes of legitimate scans.	*Visibility/ Attribution*
CSC 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.	*Configuration/ Hygiene*
CSC 4-8	Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization. Alternative countermeasures should be considered if patches are not available.	*Configuration/ Hygiene*
CSC 4-9	Evaluate critical patches in a test environment before pushing them into production on enterprise systems. If such patches break critical business applications on test machines, the	*Configuration/ Hygiene*

	organization must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality.	
CSC 4-10	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.	*Configuration/ Hygiene*

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 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take vulnerability scanning systems, if they detect unauthorized devices on the network, to generate an alert (time in minutes)?
2. How long after a scan successfully completes does it take to generate an alert indicating that it completed (time in minutes)?
3. If a scan does not complete, how long does it take to generate an alert that the scan failed to run (time in minutes)?
4. How long does it take automated patch management tools to alert or send e-mail to administrative personnel regarding the successful installation of new patches (time in minutes)?

For all of the above, consider that system priority, service level commitments, system role, and other factors may drive varying objectives for scan frequency and alert time frames on different systems. Ensure that the rationale for these classifications is clear, consistent, documented, and consistently applied. Verify that target detection and notification results are aligned with service level commitments and policies for each class of system.

CSC 4 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

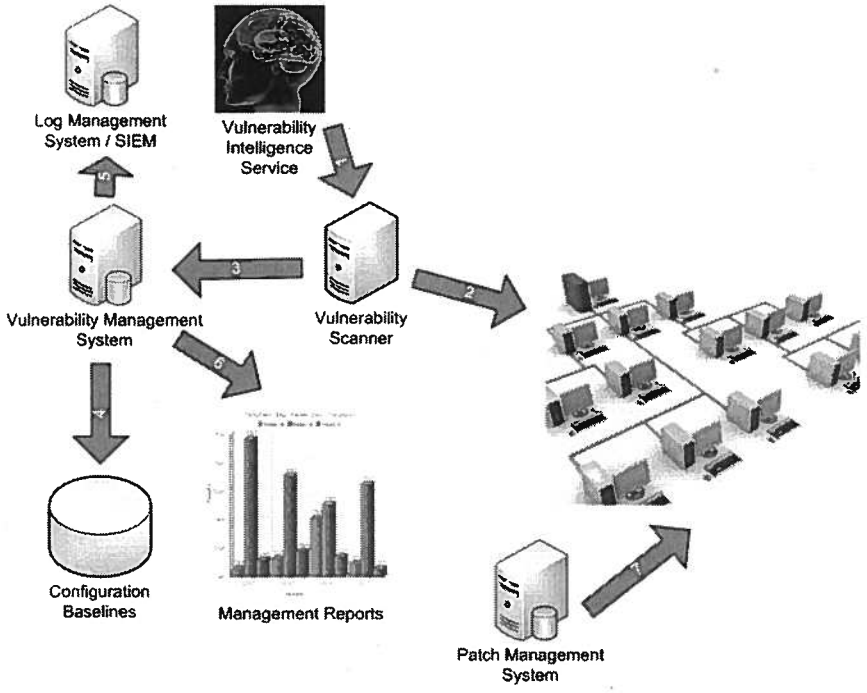
1. What is the percentage of the organization's business systems that have not recently been scanned by the organization's approved, SCAP compliant, vulnerability management system (by business unit)?
2. What is the average SCAP vulnerability score of each of the organization's business systems (by business unit)?
3. What is the total SCAP vulnerability score of each of the organization's business systems (by business unit)?
4. How long does it take, on average, to completely deploy operating system software updates to a business system (by business unit)?
5. How long does it take, on average, to completely deploy application software updates to a business system (by business unit)?

CSC 4 Effectiveness Test

To evaluate the implementation of Control 4 on a periodic basis, the evaluation team must verify that scanning tools have successfully completed their weekly or daily scans for the previous 30 cycles of scanning by reviewing archived alerts and reports to ensure that the scan was completed. If a scan could not be completed in that timeframe, the evaluation team must verify that an alert or e-mail was generated indicating that the scan did not finish.

CSC 4 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, the vulnerability scanners, management system, patch management systems, and configuration baselines all work together to address an organization's vulnerability management and remediation strategy. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Vulnerability intelligence service provides inputs to vulnerability scanner

Step 2: Vulnerability scanners scan production systems

Step 3: Vulnerability scanners report detected vulnerabilities to a vulnerability management system (VMS)

Step 4: The VMS compares production systems to configuration baselines

Step 5: The VMS sends information to log management correlation system

Step 6: The VMS produces reports for management

Step 7: A patch management system applies software updates to production systems.

CSC 5: 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, e-mail attachments, web pages, cloud services, user actions, and removable media. Modern malware can be designed to avoid defenses, or to attack or disable them.

How to Implement This Control

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.

ID #	Description	Category
CSC 5-1	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.	*Quick win*
CSC 5-2	Employ anti-malware software that offers a remote, cloud-based 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.	*Quick win*
CSC 5-3	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,.	*Quick win*
CSC 5-4	Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	*Quick win*
CSC 5-5	Scan and block all e-mail attachments entering the	*Quick win*

	organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.	
CSC 5-6	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.	*Quick win*
CSC 5-7	Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.	*Quick win*
CSC 5-8	Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection.	*Visibility/ Attribution*
CSC 5-9	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.	*Visibility/ Attribution*
CSC 5-10	Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running on corporate systems that do not appear to be recognized by the enterprise's anti-malware software. Samples should be provided to the security vendor for "out-of-band" signature creation and later deployed to the enterprise by system administrators.	*Advanced*
CSC 5-11	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.	*Advanced*

CSC 5 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 5 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take the system to identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system (time in minutes)?
2. How long does it take the system to send e-mail notification to a list of enterprise personnel via their centralized anti-malware console or event log system after malicious code has been identified (time in minutes)?
3. Does the system have the ability to block installation, prevent execution, or quarantine malicious software (yes or no)?
4. Does the system have the ability to identify the business unit in the organization where the malicious software was identified (yes or no)?
5. How long does it take the organization to completely remove the malicious code from the system after it has been identified (time in minutes)?

CSC 5 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. How many instances of malicious code have been detected within a period of time by host based anti-malware systems (by business unit)?
2. How many instances of malicious code that were detected within a period of time were automatically remediated by the organization's host based anti-malware systems (by business unit)?
3. How many instances of malicious code have been detected within a period of time by network based anti-malware systems (by business unit)?
4. How many instances of malicious code that were detected within a period of time were automatically remediated by the organization's network based anti-malware systems (by business unit)?
5. Percentage of applications on a system that are not utilizing application sandboxing products (by business unit)?
6. Percentage of systems with anti-malware systems deployed, enabled, and up-to-date (by business unit)?

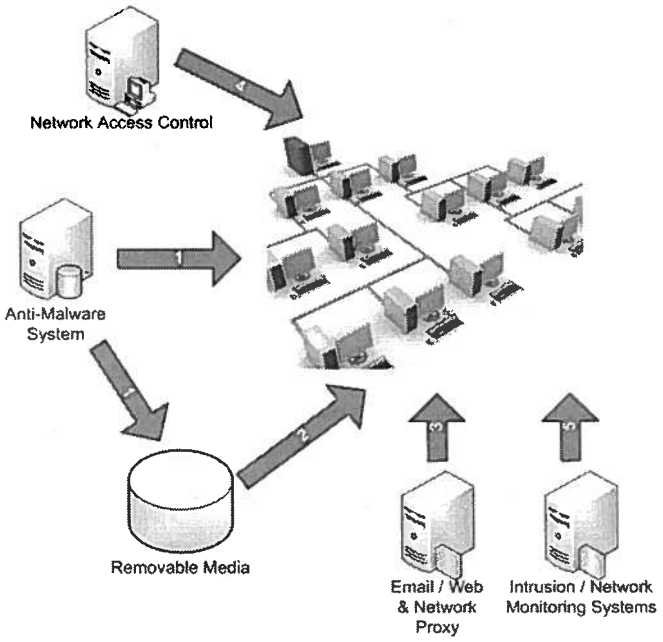
CSC 5 Effectiveness Test

To evaluate the implementation of Control 5 on a periodic basis, the evaluation team must move a benign software test program that appears to be malware (such as an EICAR file or benign hacker tools), but that is not included in the official authorized software list, to 10 systems on the network via a network share. The selection of these systems must be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the benign malware within one hour. The team must also verify that the alert or e-mail indicating that the software has been blocked or quarantined is received within one hour. The evaluation team must verify that the system provides details of the location of each machine with this new test file, including information about the asset owner. The team must then verify that the file is blocked by attempting to execute or open it and verifying that it is not allowed to be accessed.

Once this test has been performed transferring the files to organization systems via removable media, the same test must be repeated, but this time transferring the benign malware to 10 systems via e-mail instead. The organization must expect the same notification results as noted with the removable media test.

CSC 5 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining anti-malware systems and threat vectors such as removable media. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Anti-malware systems analyze production systems and removable media

Step 2: Removable media is analyzed when connected to production systems

Step 3: Email/web and network proxy devices analyze all incoming and outgoing traffic

Step 4: Network access control monitors all systems connected to the network

Step 5: Intrusion/network monitoring systems perform continuous monitoring looking for signs of malware.

CSC 7: 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.

How to Implement This Control

ID #	Description	Category
CSC 7-1	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.	*Quick win*
CSC 7-2	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.	*Quick win*
CSC 7-3	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.	*Visibility/ Attribution*
CSC 7-4	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.	*Configuration/ Hygiene*
CSC 7-5	For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible	*Configuration/ Hygiene*

	firmware interface), with password protections to lower the possibility that the user will override such configurations.	
CSC 7-6	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.	*Configuration/ Hygiene*
CSC 7-7	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.	*Configuration/ Hygiene*
CSC 7-8	Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.	*Configuration/ Hygiene*
CSC 7-9	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.	*Configuration/ Hygiene*
CSC 7-10	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.	*Configuration/ Hygiene*

CSC 7 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 7 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Are systems capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to their networks (yes or no)?
2. How long does it take to generate alerts about unauthorized wireless devices that are detected (time in minutes)?
3. How long does it take for unauthorized wireless devices to be blocked from connecting or isolated from the network (time in minutes)?
4. Are additional alerts generated every 24 hours after the initial alert until the system is isolated or removed from the network (yes or no)?
5. Is the system able to identify the location, department, and other details of where authorized and unauthorized wireless devices are plugged into the network (yes or no)?

CSC 7 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. How many rogue wireless access points have been discovered recently in the organization (by business unit)? This should include non-persistent, temporary and transient access points.
2. What is the average time that it takes to remove rogue access points from the organization's network (by business unit)?
3. How many wireless access points or clients have been discovered using an unauthorized wireless configuration recently in the organization (by business unit)?

CSC 7 Effectiveness Test

To evaluate the implementation of Control 7 on a periodic basis, the evaluation team must configure 10 unauthorized but hardened wireless clients and wireless access points to the organization's network and attempt to connect them to its wireless networks. In the case of wireless access points, these access points must not be directly connected to the organization's trusted network. Instead, they must simply be configured to act as a wireless gateway without physically connecting to a wired network interface. In the case of scanning for wireless access points from a wired interface, the connected access point must have the wireless radio disabled for the duration of the test. These systems must be configured to test each of the following scenarios:

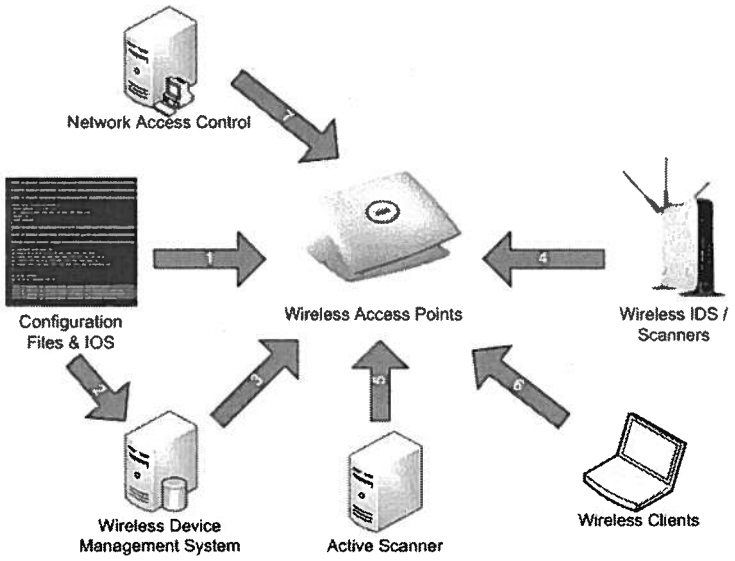
- A wireless client with an unauthorized service set identifier configured on it.
- A wireless client with improper encryption configured.
- A wireless client with improper authentication configured.

- A wireless access point with improper encryption configured.
- A wireless access point with improper authentication configured.
- A completely rogue wireless access point using an unauthorized configuration.

When any of the above-noted systems attempt to connect to the wireless network, an alert must be generated and enterprise staff must respond to the alerts to isolate the detected device or remove the device from the network.

CSC 7 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the configuration and management of wireless devices, wireless IDS/scanners, wireless device management systems, and vulnerability scanners. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Hardened configurations applied to wireless devices

Step 2: Hardened configurations managed by a configuration management system

Step 3: Configuration management system manages the configurations on wireless devices

Step 4: Wireless IDS monitor usage of wireless communications

Step 5: Vulnerability scanners scan wireless devices for potential vulnerabilities

Step 6: Wireless clients utilize wireless infrastructure systems in a secure manner.

CSC 8: 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.

How to Implement This Control

ID #	Description	Category
CSC 8-1	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.	*Quick win*
CSC 8-2	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	*Quick win*
CSC 8-3	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.	*Configuration/ Hygiene*
CSC 8-4 *(NEW)*	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.	

CSC 8 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 which is believed to predate the original infection.

CSC 8 Effectiveness Metrics

- Percentage of systems with current backups within their target frequency (targets can vary by system role, type, and criticality)

CSC 8 Automation Metrics

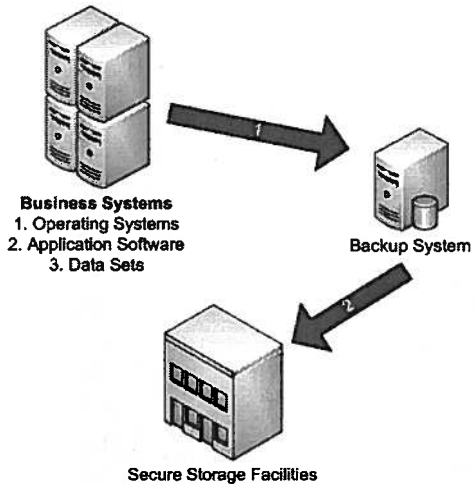
None

CSC 8 Effectiveness Test

The evaluation team should identify 5 systems in the environment and restore to a test system (physical or virtual) using the most recent backup. Verify that the system has been restored properly by comparing the restore results to the original system.

CSC 8 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining an organization's capability to restore systems in the event that data need to be restored because of a data loss or breach of a system. While backups are certainly an important part of this process, the ability to restore data is the critical component. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Production business systems backed up on a regular basis to authorized organizational backup systems

Step 2: Backups created are stored offline at secure storage facilities.

CSC 9: 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: the actions of end users (who can fall prey to social engineering schemes such as phishing); IT operations (who may not recognize the security implications of IT artifacts and logs); security analysts (who struggle to keep up with an explosion of new information); system developers and programmers (who don't understand the opportunity to resolve root cause vulnerabilities early in the system life-cycle); 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 begin to address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

How to Implement This Control

ID #	Description	Category
CSC 9-1	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.	*Quick win*
CSC 9-2	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	*Quick win*

	to train, use training conferences or online training to fill the gaps.	
CSC 9-3	Implement an online security awareness program that (1) focuses only 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, and (5) is reliably monitored for employee completion.	*Quick win*
CSC 9-4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail 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.	*Visibility/ Hygiene*
CSC 9-5	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 skills mastery.	*Configuration/ Hygiene*

CSC 9 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, and specific (for example, using a S.M.A.R.T. metrics program). 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 list prepared by the Council on CyberSecurity (which builds upon 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. The Council has validated this list as consistent with the broader NIST National Initiative on Cybersecurity

Education (NICE) framework, and with the needs of many enterprises in government and industry. Training for these mission critical roles should be supplemented with foundational security training for all users.

< www.counciloncybersecurity.org/practice-areas/people >.

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 actions in CSC 9 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive security training program.

Control 9 Effectiveness Metrics

1. Participation rate for online training courses – percentage of staff completing security training (by business unit)
2. Average scores of online tests, compared to baseline (previous tests, industry data if available, etc.) by business unit
3. Average scores of periodic tests (e.g. click rates for test phishing emails) by business unit
4. Individual scores on skill assessment tests for individual mission critical roles by business unit
5. Retention (or job opening fill rate) of mission critical roles (org/unit metric)

CSC 9 Automation Metrics

None

CSC 9 Effectiveness Test

None

CSC 10: 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.

How to Implement This Control

ID #	Description	Category
CSC 10-1	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.	*Quick win*
CSC 10-2	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	*Configuration/ Hygiene*

	that business need, and an expected duration of the need.	
CSC 10-3	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be automatically reported to security personnel.	*Configuration/ Hygiene*
CSC 10-4	Manage network devices using two-factor authentication and encrypted sessions.	*Configuration/ Hygiene*
CSC 10-5	Install the latest stable version of any security-related updates.	*Configuration/ Hygiene*
CSC 10-6	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.	Advanced

CSC 10 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 10 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. How long does it take to detect configuration changes to a network system (time in minutes)?
2. How long does it take the scanners to alert the organization's administrators that an unauthorized configuration change has occurred (time in minutes)?
3. How long does it take to block/quarantine unauthorized changes on network systems (time in minutes)?
4. Are the scanners able to identify the location, department, and other critical details about the systems where unauthorized changes occurred (yes or no)?

CSC 10 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. What is the percentage of network devices that are not currently configured with a security configuration that matches the organization's approved configuration standard (by business unit)?
2. What is the percentage of network devices whose security configuration is not enforced by the organization's technical configuration management applications (by business unit)?
3. What is the percentage of network devices that are not up to date with the latest available operating system software security patches (by business unit)?
4. What is the percentage of network devices do not require two-factor authentication to administer the device (by business unit)?

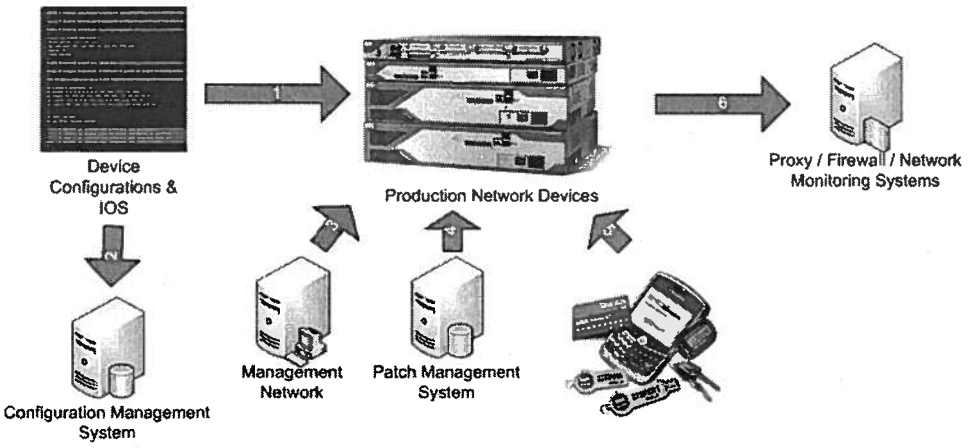
CSC 10 Effectiveness Test

To evaluate the implementation of Control 10 on a periodic basis, an evaluation team must make a change to each type of network device plugged into the network. At a minimum, routers, switches, and firewalls need to be tested. If they exist, IPS, IDS, and other network devices must be included. Backups must be made prior to making any changes to critical network devices. It is critical that changes not impact or weaken the security of the device. Acceptable changes include but are not limited to making a comment or adding a duplicate entry in the configuration. The change must be performed twice for each critical device. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the changes to the device within 24 hours. It is important that the evaluation team verify that all unauthorized changes have been detected, the account making the changes has been recorded, and the changes have resulted in an alert or e-mail notification. The evaluation team must verify that the system provides details of the location of each device, including information about the asset owner. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation, with notification about unauthorized configuration changes in network devices sent within two minutes.

If appropriate, an additional test must be performed on a daily basis to ensure that other protocols such as IPv6 are being filtered properly.

Control 10 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case we are examining the network devices, test lab network devices, configuration systems, and configuration management devices. The following list of the steps in the diagram above shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Hardened device configurations applied to production devices

Step 2: Hardened device configuration stored in a secure configuration management system

Step 3: Management network system validates configurations on production network devices

Step 4: Patch management system applies tested software updates to production network devices

Step 5: Two-factor authentication system required for administrative access to production devices

Step 6: Proxy/firewall/network monitoring systems analyze all connections to production network devices.

CSC 12: 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 e-mail 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 e-mail. An administrator inadvertently opens an e-mail 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.

How to Implement This Control

ID #	Description	Category
CSC 12-1	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.	*Quick win (One of the "First Five")*
CSC 12-2	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.	*Quick win*
CSC 12-3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters	*Quick win*

	intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	
CSC 12-4	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.	*Quick win*
CSC 12-5	Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	*Quick win*
CSC 12-6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800-132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges.	*Quick win*
CSC 12-7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients especially must be configured to never run as administrator.	*Quick win*
CSC 12-8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non-administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows "administrator" or UNIX "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	*Quick win*
CSC 12-9	Configure operating systems so that passwords cannot be re-used within a timeframe of six months.	*Quick win*
CSC 12-10	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.	*Visibility/ Attribution*
CSC 12-11 *(NEW)*	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	*Visibility/ Attribution*
CSC 12-12	Use multifactor authentication for all administrative	*Configuration/*

	access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	*Hygiene*
CSC 12-13 *(NEW)*	When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	*Configuration/ Hygiene*
CSC 12-14	Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, 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. Users would use their own administrative accounts and enter a password each time that is different than their user account.	*Configuration/ Hygiene*

CSC 12 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 e-mail reading, security personnel should periodically gather a list of running processes to determine whether any browsers or e-mail readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, e-mail 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.

Control 12 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Does the system report on log-in to administrative accounts?
2. Does the system report on the elevation to administrative access, to include traceability to the user account that performed the elevation?
3. Does the system provide an inventory of all administrative accounts?
4. Does the system report on the addition of new administrative accounts?
5. Does the system allow limitations to be placed on the use of administrative accounts, to include not allowing web browsers and email clients to run as administrator?
6. Does the system prevent administrative accounts from logging into machines, either locally or remotely, instead requiring elevation of privileges once logged in with a user account?
7. Does the system require strong passwords for all administrative accounts and does the system require update of administrator passwords on a regular basis?
8. Does the system audit all attempts to gain access to password files within the system?
9. Does the system comply with password policies detailed in the control (yes or no)?
10. How long does it take for administrators to be notified about user accounts being added to super user groups (time in minutes)?
11. Are additional alerts generated every 24 hours until the user account has been removed from or authorized to be a part of the super user group (yes or no)?

CSC 12 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. How many unauthorized elevated operating system accounts (local administrator/root) are currently configured on the organization's systems (by business unit)?
2. How many unauthorized elevated application accounts are currently configured on the organization's systems (by business unit)?
3. What percentage of the organization's elevated accounts do not currently adhere to the organization's password standard (by business unit)?
4. What percentage of the organization's elevated accounts do not require two-factor authentication (by business unit)?
5. How many attempts to upgrade an account to administrative privileges have been detected on the organization's systems recently (by business unit)?
6. How many attempts to gain access to password files within the system have

been detected on the organization's systems recently (by business unit)?

Control 12 Effectiveness Test

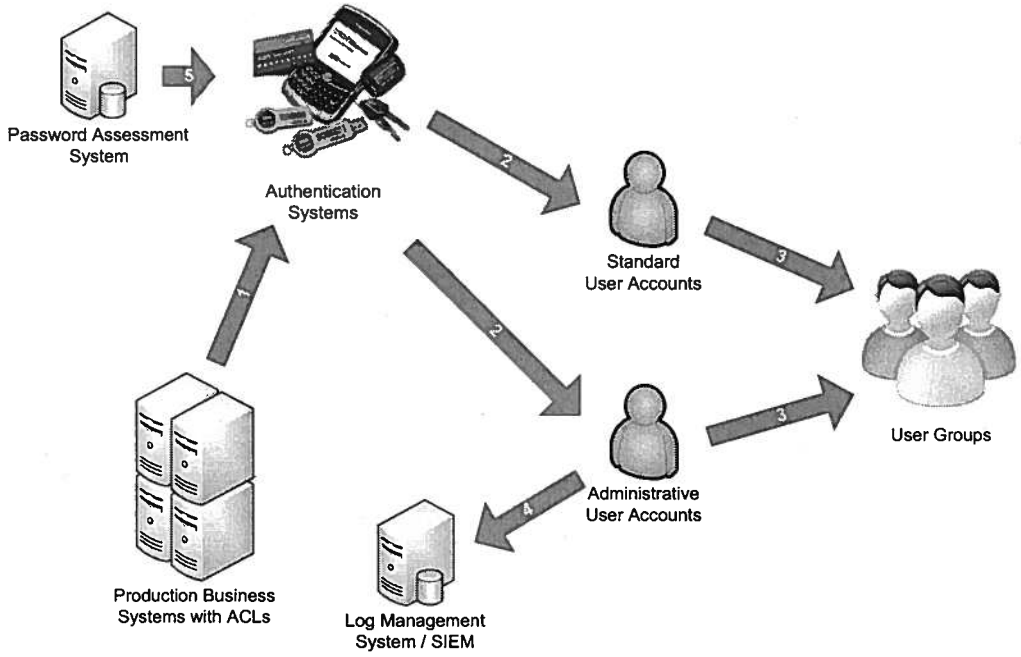
To evaluate the implementation of Control 12 on a periodic basis, the evaluation team must attempt a variety of techniques to gain access and exploit administrative accounts within the system. Each of the following tests must be performed at least three times:

- Attempt to gain access to a cross section of devices within the system, using default administrative passwords.
- Attempt to log-in remotely to machines using administrative accounts directly. Verify that this is disallowed by policy.
- Attempt to log-in directly to a workstation or server with root or administrator accounts. Verify that this is disallowed by policy.
- Attempt to gain access to password files within the system using unauthorized accounts. Verify that access is disallowed and that attempts are logged and reported.
- Attempt to elevate to a privileged account on the system. Verify that the administrator password is required to perform the elevation and that the elevation is logged and reported by the system. Verify that traceability within the audit logs is provided to detail the user account that performed the elevation.
- Attempt to configure weak administrator passwords that are non-compliant with established policy. Verify that the system does not allow weak passwords to be used.
- Attempt to re-use an administrator password that was previously used for the account. Verify that the system requires unique new passwords during each update.

Each of these tests must be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of administrator controls.

CSC 12 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the components of user account provisioning and user authentication. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Production systems use proper authentication systems

Step 2: Standard and administrative user accounts use proper authentication systems

Step 3: Standard and administrative user accounts properly managed via group memberships

Step 4: Administrative access to systems properly logged via log management systems

Step 5: Password assessment system validates the strength of the authentication systems.

CSC 14: 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 though the evidence of the attack has been recorded in unexamined log files.

How to Implement This Control

ID #	Description	Category
CSC 14-1	Include at least two synchronized time sources (i.e., Network Time Protocol – NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent, and are set to UTC (Coordinate Universal Time).	*Quick win*
CSC 14-2	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.	*Quick win*

CSC 14-3	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.	*Quick win*
CSC 14-4	Develop a log retention policy to make sure that the logs are kept for a sufficient period of time. Organizations are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes an organization to detect an attack so they can accurately determine what occurred.	*Quick win*
CSC 14-5	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.	*Quick win*
CSC 14-6	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.	*Visibility/ Attribution*
CSC 14-7	For all servers, ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from the hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.	*Visibility/ Attribution*
CSC 14-8	Deploy a SIEM (Security Incident 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.	*Visibility/ Attribution*
CSC 14-9	Monitor for service creation events and enable process tracking logs. On Windows systems, many attackers use PsExec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely. Process tracking is valuable for incident handling.	*Advanced*

CSC 14-10 *(NEW)*	Ensure that the log collection system does not lose events during peak activity, and that the system detects and alerts if event loss occurs (such as when volume exceeds the capacity of a log collection system). This includes ensuring that the log collection system can accommodate intermittent or restricted-bandwidth connectivity through the use of handshaking / flow control.	*Advanced*

CSC 14 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 14 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Does each system log appropriately to a central log management system (yes or no)?
2. Does each log event generated include a date, timestamp, source address, destination address and other details about the packet (yes or no)?
3. If a system fails to log properly, how long does it take for an alert about the failure to be sent (time in minutes)?

4. If a system fails to log properly, how long does it take for enterprise personnel to receive the alert about the failure (time in minutes)?

CSC 14 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

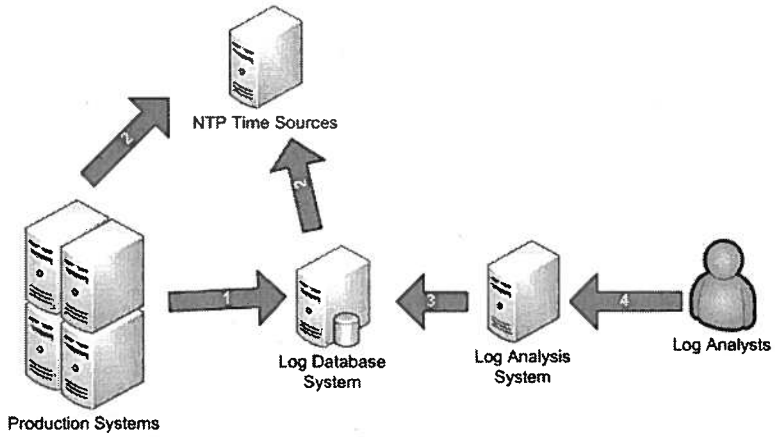
1. What percentage of the organization's systems do not currently have comprehensive logging enabled in accordance with the organization's standard (by business unit)?
2. What percentage of the organization's systems are not currently configured to centralize their logs to a central log management system (by business unit)?
3. How many anomalies / events of interest have been discovered in the organization's logs recently (by business unit)?

CSC 14 Effectiveness Test

To evaluate the implementation of Control 14 on a periodic basis, an evaluation team must review the security logs of various network devices, servers, and hosts. At a minimum the following devices must be tested: two routers, two firewalls, two switches, 10 servers, and 10 client systems. The testing team should use traffic-generating tools to send packets through the systems under analysis to verify that the traffic is logged. This analysis is done by creating controlled, benign events and determining if the information is properly recorded in the logs with key information, including a date, timestamp, source address, destination address, and other details about the packet. The evaluation team must verify that the system generates audit logs and, if not, an alert or e-mail notice regarding the failed logging must be sent within 24 hours. It is important that the team verify that all activity has been detected. The evaluation team must verify that the system provides details of the location of each machine, including information about the asset owner.

CSC 14 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining audit logs, the central log database system, the central time system, and log analysts. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Production systems generate logs and send them to a centrally managed log database system

Step 2: Production systems and log database system pulls synchronize time with central time management systems

Step 3: Logs analyzed by a log analysis system

Step 4: Log analysts examine data generated by log analysis system.

CSC 15: 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.

How to Implement This Control

ID #	Description	Category
CSC 15-1	Locate any sensitive information on separated VLANS with firewall filtering. All communication of sensitive information over less-trusted networks should be encrypted.	*Quick win*
CSC 15-3	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.	*Visibility/ Attribution*
CSC 15-4	Segment the network based on the trust levels of the information stored on the servers. Whenever information flows over a network with a lower trust level, the information should be encrypted.	*Configuration/ Hygiene*
CSC 15-5	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.	*Advanced*

CSC 15 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 15 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Can the system detect all attempts by users to access files on local systems or network-accessible file shares without the appropriate privileges (yes or no)?
2. How long does it take the system to generate an alert or e-mail for administrative personnel of a user inappropriately accessing the file shares (time in minutes)?

CSC 15 Automation Metrics

In order to automate the collection of relevant data from these systems, organizations should gather the following information with automated technical sensors:

1. What percentage of the organization's data sets have not been classified in accordance with the organization's data classification standards (by business unit)?

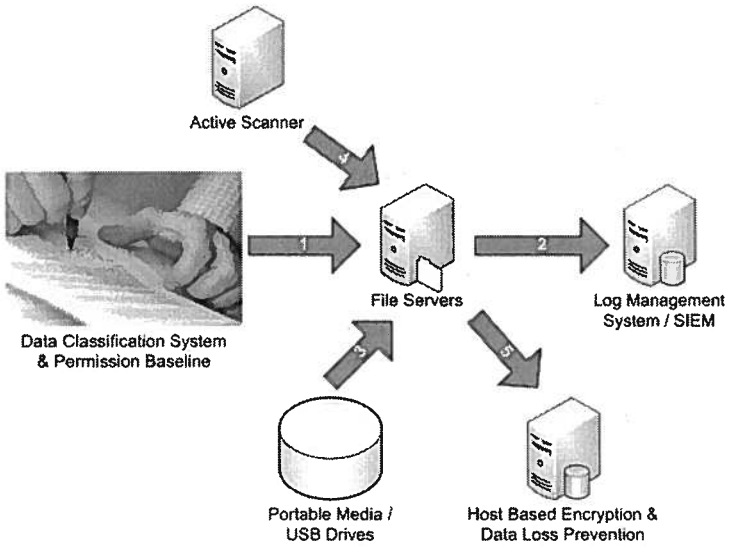
2. What percentage of sensitive data sets are not configured to require logging of access to the data set (by business unit)?
3. What percentage of the organization's business systems are not utilizing host based Data Loss Prevention (DLP) software applications (by business unit)?

CSC 15 Effectiveness Test

To evaluate the implementation of Control 15 on a periodic basis, the evaluation team must create two test accounts each on 10 representative systems in the enterprise: five server machines and five client systems. For each system evaluated, one account must have limited privileges, while the other must have privileges necessary to create files on the systems. The evaluation team must then verify that the non-privileged account is unable to access the files created for the other account on the system. The team must also verify that an alert or e-mail is generated based on the attempted unsuccessful access within 24 hours. Upon completion of the test, these accounts must be removed.

CSC 15 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, the data classification system and permission baseline is the blueprint for how authentication and access of data is controlled. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also

delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: An appropriate data classification system and permissions baseline applied to production data systems

Step 2: Access appropriately logged to a log management system

Step 3: Proper access control applied to portable media/USB drives

Step 4: Active scanner validates, checks access, and checks data classification

Step 5: Host-based encryption and data-loss prevention validates and checks all access requests.

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.

How to Implement This Control

ID #	Description	Category
CSC 16-1	Review all system accounts and disable any account that cannot be associated with a business process and owner.	*Quick win*
CSC 16-2	Ensure that all accounts have an expiration date associated with the account.	*Quick win*
CSC 16-3	Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.	*Quick win*
CSC 16-4	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.	*Quick win*
CSC 16-5	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	*Quick win*
CSC 16-6 *(NEW)*	Configure screen locks on systems to limit access to unattended workstations.	*Quick win*
CSC 16-7	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	*Quick win*

	for system recovery or continuity operations).	
CSC 16-8	Require that all non-administrator accounts have strong passwords that contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password. These values can be adjusted based on the specific business needs of the organization.	*Quick win*
CSC 16-9	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.	*Quick win*
CSC 16-10	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 active employees or contractors.	*Visibility/ Attribution*
CSC 16-11	Monitor attempts to access deactivated accounts through audit logging.	*Visibility/ Attribution*
CSC 16-12 *(NEW)*	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.	*Configuration/ Hygiene*
CSC 16-13	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.	*Configuration/ Hygiene*
CSC 16-14 *(NEW)*	Require multi-factor authentication for accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using Smart cards with certificates, One Time Password (OTP) tokens, or biometrics.	*Advanced*
CSC 16-15 *(NEW)*	For authenticated access to web services within an enterprise, ensure that account usernames and passwords are passed over an encrypted channel and associated password hash files are stored securely if a centralized service is not employed.	*Advanced*
CSC 16-16 *(NEW)*	Configure all systems to use encrypted channels for the transmission of passwords over a network.	*Advanced*
CSC 16-17 *(NEW)*	Verify that all password files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password	*Advanced*

	files in the system.	

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.

Control 16 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Does the system audit and report on valid and invalid log-ins to user accounts?
2. Does the system audit and report on valid and invalid log-ins to network and security device user accounts?
3. Does the system lock users out after five (5) invalid attempts?
4. Do user account passwords expire at least every 90 days?
5. Does the system report on dormant accounts that have not been used for a configurable period of time?
6. How long does it take to send an alert or e-mail to administrative personnel that the comparison report has been created (time in minutes)?

Control 16 Automation Metrics

In order to automate the monitoring and control of user accounts, organizations should gather the following information with automated technical sensors:

1. How many invalid attempts to access user accounts have been detected within a period of time?
2. How many accounts have been locked out within a period of time?
3. How many attempts to gain access to password files in the system have been

detected within a period of time?

4. Perform authorized password cracking against password files and identify the number of administrator account passwords that are cracked during the attempt. Remediate any compromised passwords immediately.
5. Is an automated list of user accounts on the system created daily & compared to a baseline (yes or no)?
6. How long does it take to send an alert or e-mail to administrative personnel that the comparison report has been created (time in minutes)?

CSC 16 Effectiveness Test

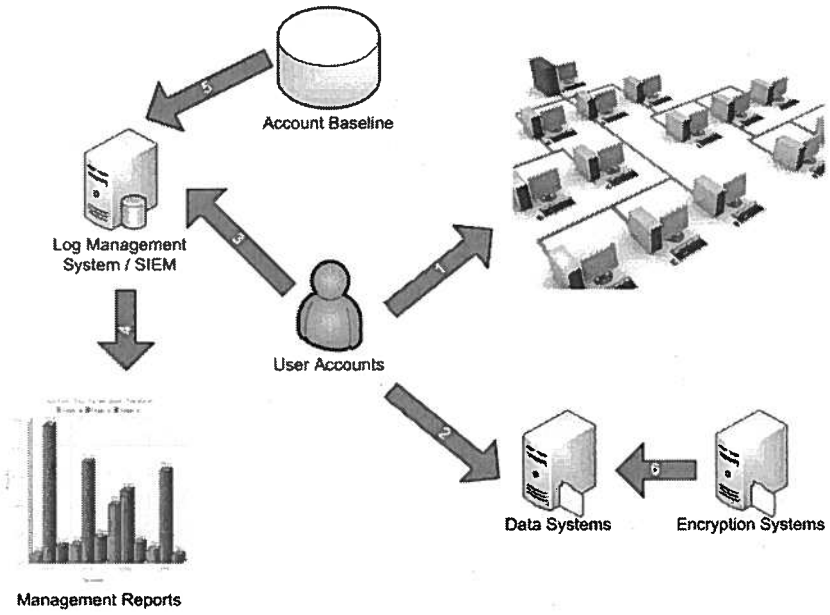
To evaluate the implementation of Control 16 on a periodic basis, the evaluation team must attempt a variety of techniques to gain access to user accounts within the system. Each of the following tests must be performed at least three times:

1. Attempt to configure weak user account passwords that are non-compliant with established policy. Verify that the system does not allow weak passwords to be used.
2. Attempt to re-use a user account password that was previously used for the account. Verify that the system requires unique new passwords during each update.
3. Attempt to capture passwords by monitoring network traffic to server resources. Remediate any instances where passwords are transmitted in clear text.
4. Attempt to gain access to password files stored on the system. If successful, identify whether passwords are cryptographically secured.

Each of these tests must be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of user account controls.

CSC 16 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining user accounts and how they interact with the data systems and the log management systems. Another key component of these systems is the reports generated for management of user accounts.

The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. It also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: User accounts are properly managed on production systems

Step 2: User accounts are assigned proper permissions to production data sets

Step 3: User account access is logged to log management system

Step 4: Log management systems generate user account and access reports for management

Step 5: Account baseline information is sent to log management system

Step 6: Critical information is properly protected and encrypted for each user account.

CSC 17: 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 for organizations 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.

How to Implement This Control

ID #	Description	Category
CSC 17-1	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	*Quick win*
CSC 17-2 *(NEW)*	Verify that cryptographic devices and software are configured to use publicly-vetted algorithms.	*Quick win*
CSC 17-3 *(NEW)*	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls	*Quick win*
CSC 17-4 *(NEW)*	Review cloud provider security practices for data protection.	*Quick Win*
CSC 17-5	Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., 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.	*Visibility/ Attribution*
CSC 17-6	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and 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.	*Visibility/ Attribution*
CSC 17-7	Move data between networks using secure,	*Configuration/*

	authenticated, and encrypted mechanisms.	*Hygiene*
CSC 17-8	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.	*Configuration/ Hygiene*
CSC 17-9	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.	*Configuration/ Hygiene*
CSC 17-10 *(NEW)*	Only allow approved Certificate Authorities (CAs) to issue certificates within the enterprise; Review and verify each CAs Certificate Practices Statement (CPS) and Certificate Policy (CP).	*Configuration/ Hygiene*
CSC 17-11 *(NEW)*	Perform an annual review of algorithms and key lengths in use for protection of sensitive data.	*Configuration/ Hygiene*
CSC 17-12	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.	*Advanced*
CSC 17-13	Block access to known file transfer and e-mail exfiltration websites.	*Advanced*
CSC 17-14 *(NEW)*	Define roles and responsibilities related to management of encryption keys within the enterprise; define processes for lifecycle.	*Advanced*
CSC 17-15 *(NEW)*	Where applicable, implement Hardware Security Modules (HSMs) for protection of private keys (e.g., for sub CAs) or Key Encryption Keys.	*Advanced*

CSC 17 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 lifecycle 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 17 Effectiveness Metrics

In order to test the effectiveness of the automated implementation of this control, organizations should measure the following:

1. Does the system identify and report on unauthorized data being exfiltrated, whether via network file transfers or removable media?
2. Does the system identify the attachment of unencrypted USB tokens and require encryption of tokens?
3. Does the system store cryptographic key material securely?
4. Does the system use only NIST approved encryption algorithms?
5. Within one hour of a data exfiltration event or attempt, enterprise administrative personnel must be alerted by the appropriate monitoring system.
6. Do alerts notifying of data exfiltration also note the system and location where the event or attempt occurred?
7. Are the systems able to identify the location, department, and other critical details about where the sensitive data originated from (yes or no)?
8. How long does it take before a data leakage risk has been remediated from the time it was detected (time in minutes)?

CSC 17 Automation Metrics

In order to automate the protection of data using cryptography and DLP functions, organizations should gather the following information with automated technical sensors:

1. How many unauthorized data exfiltration attempts have been detected within a period of time by DLP software?
2. How many plaintext instances of sensitive data have been detected within a period by automated scanning software?
3. How many attempts to access known file transfer and e-mail exfiltration websites have been detected within a period of time?

CSC 17 Effectiveness Test

To evaluate the implementation of Control 17 on a periodic basis, the evaluation team must attempt to move test data sets that trigger DLP systems but do not contain sensitive data outside of the trusted computing environment via both network file

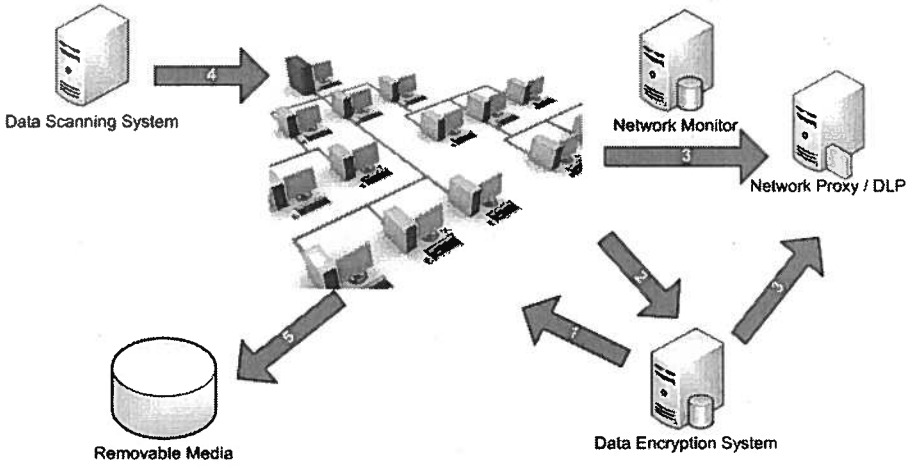
transfers and removable media. Each of the following tests must be performed at least three times:

- Attempt to transfer large data sets across network boundaries from an internal system.
- Attempt to transfer plaintext test data sets of personally identifiable information (that trigger DLP systems but do not contain sensitive data) across network boundaries from an internal system (using multiple keywords specific to the business).
- Attempt to transfer encrypted test data sets across network boundaries from an internal system to identify if the exfiltration is reported.
- Attempt to maintain a persistent network connection for at least 10 hours across network boundaries between an internal and external system, even though little data may be exchanged.
- Attempt to maintain a network connection across network boundaries using an anomalous service port number between an internal and external system.
- Insert a USB token into an organization system and attempt to transfer example test data to the USB device.

Each of these tests must be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of the monitoring systems. Once each of these events has occurred, the time it takes for enterprise staff to respond to the event must be recorded.

CSC 17 Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the flow of information in and out of the organization in an attempt to limit potential data loss via network or removable media sources. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. It also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Data encryption system ensures that appropriate hard disks are encrypted

Step 2: Sensitive network traffic encrypted

Step 3: Data connections monitored at the network's perimeter by monitoring systems

Step 4: Stored data scanned to identify where sensitive information is stored

Step 5: Offline media encrypted.

CSC 18: 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.

How to Implement This Control

ID #	Description	Category
CSC 18-1	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.	*Quick win*
CSC 18-2	Assign job titles and duties for handling computer and network incidents to specific individuals.	*Quick win*
CSC 18-3	Define management personnel who will support the incident handling process by acting in key decision-making roles.	*Quick win*
CSC 18-4	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	*Quick win*

	organization in computer incidents.	
CSC 18-5	Assemble and maintain information on third-party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).	*Quick win*
CSC 18-6	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.	*Quick win*
CSC 18-7	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.	*Configuration/ Hygiene*

CSC 18 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 18 Effectiveness Metrics

None

CSC 18 Automation Metrics

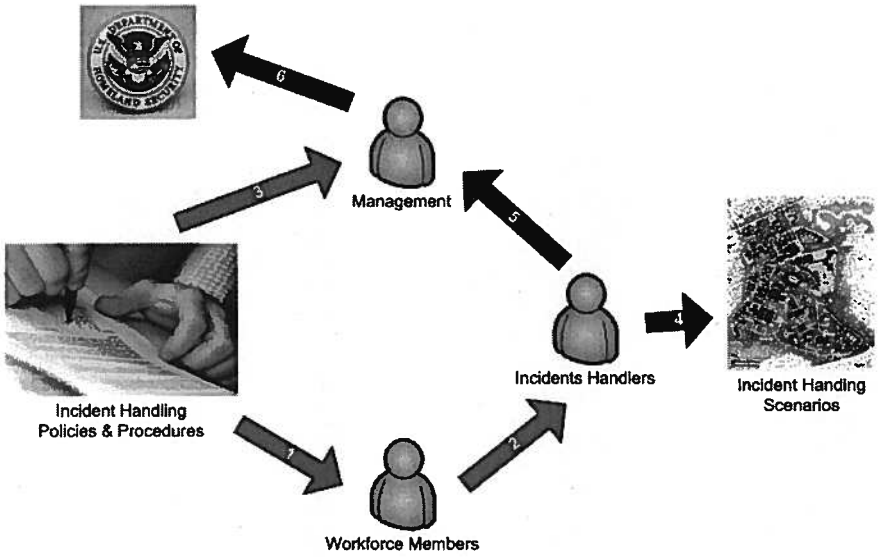
None

CSC 18 Effectiveness Test

None

Control 18 System Entity Relationship Diagram

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the incident handling process and how prepared organizations are in the event that an incident occurs. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Incident handling policies and procedures educate workforce members as to their responsibilities during an incident

Step 2: Some workforce members designated as incident handlers

Step 3: Incident handling policies and procedures educate management as to their responsibilities during an incident

Step 4: Incident handlers participate in incident handling scenario tests

Step 5: Incident handlers report incidents to management

Step 6: The organization's management reports incidents to outside law enforcement and the appropriate computer emergency response team, if necessary.