This is a GIAC Gold Template

Using the Center for Internet Security (CIS) Benchmarks to support an Information Security Management System

GIAC (G2700) Gold Certification

Author: Robert Mavretich, bmav@rocketmail.com

Advisor: Robert VandenBrink

Accepted: October 18, 2012

Abstract

Within any organization, securing information assets appropriately is a very important part of the Information Security Management System (ISMS) puzzle. Unfortunately, many organizations leave the configuration of those assets up to the preferences of a very small, autonomous group of folks. Using the Windows 7 platform as an example, we will walk through a few of the secure configuration items of this operating system, highlighting ways to increase awareness and participation so that all groups can have a stake in the direction of securing their information assets through a common set of industry acceptable standards.

1. Introduction

Humans are quite a fickle bunch. We learn our daily tasks and responsibilities in varying ways and pass on that knowledge in an increasingly different world than the one we learned it in. By the time we re-visit the task or responsibility itself, the ways in which we perform that task may have become obsolete or simply incomplete. Technological advances have only sped up this process and even though our jobs (and lives) were supposed to become easier as a result, it has actually complicated it. In fact, "over the last 20 years, there has been immense growth in the number of computing and network services, enabling transactions to be undertaken by the smallest business across a global marketplace" (Hayes, Shore & Jakeman, 2012).

As a result of this, "in some parts of the world, organizations prefer to do business with other companies that adhere to well defined international standards" (Hoelzer, 2012). That is an understatement if you consider the wide-ranging regulations and compliance programs that have directed organizations in the recent past (PCI, SOX, HIPPA, etc.). As a result of wide scale information security breaches and service interruptions over the last decade, organizations have tried to become much more careful in the solutioning of connectivity to unknown organizations and their public internet-facing presence for the purpose of commerce. This starts at a fundamental level, with the configuration of your network devices. While you may have a relatively stable and defined exterior network border, the interior of your organization can sometimes resemble the Wild West! "Many of the shortcomings in technology…were recognized many years ago, but nationally, commercially, and personally sensitive systems continue to be installed and operated with these shortcomings" (Hayes, Shore & Jakeman, 2012).

Information technology standards have been a popular way to help provide simple uniformity across a large population of assets such as desktops, laptops, servers, multi-function devices, firewalls, routers – you name it! "Vendors continually release tactical patches and upgrades to fix problems, but hackers with knowledge, skills and capability have developed and release exploits and easy-to-use tools to enable even the least technical users to become adversaries" (Hayes, Shore & Jakeman, 2012). Notice how the graphic below conspicuously calls out seemingly everyone *except* the casual non-corporate user, who is usually the most dangerous because they unwittingly act as an intermediary for the perpetrators listed below.

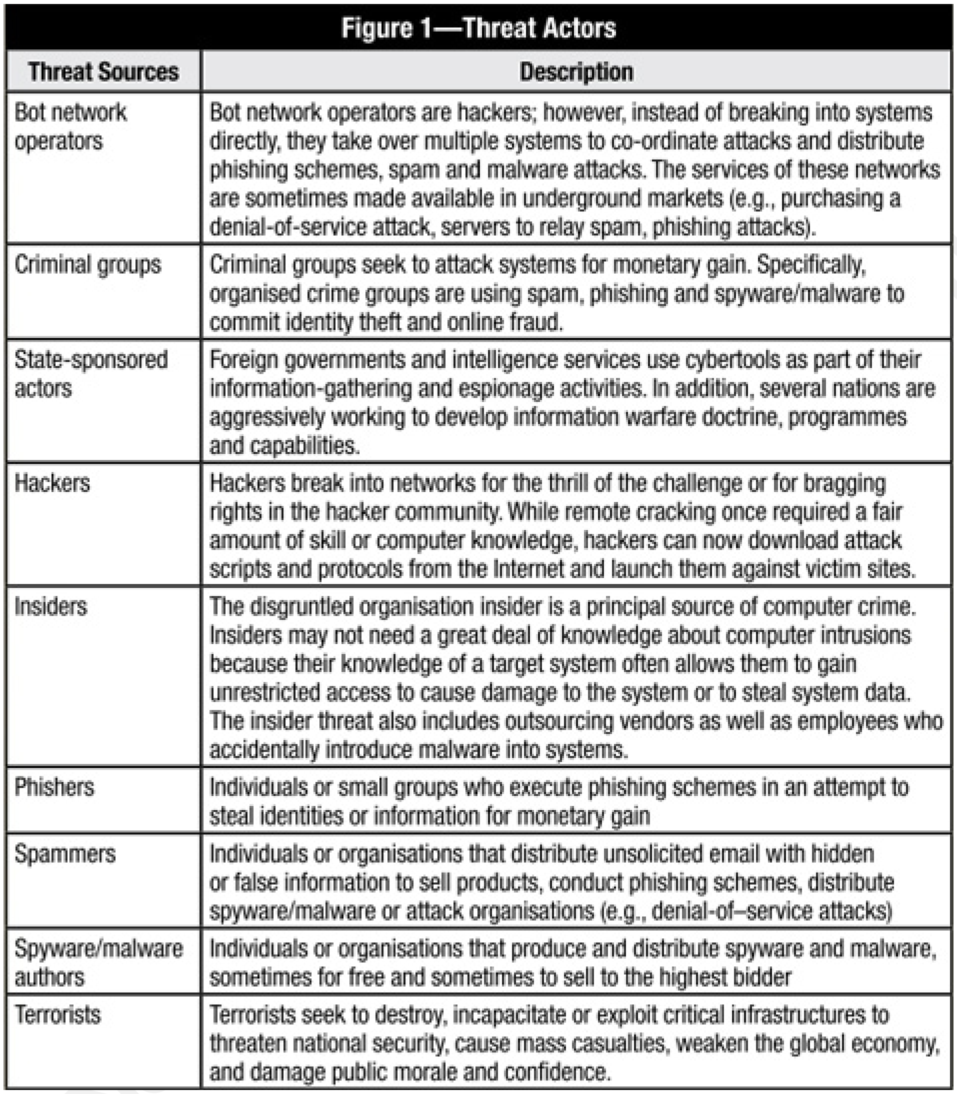


Figure 1—Threat Actors

Threat Sources	Description
Bot network operators	Bot network operators are hackers; however, instead of breaking into systems directly, they take over multiple systems to co-ordinate attacks and distribute phishing schemes, spam and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organised crime groups are using spam, phishing and spyware/malware to commit identity theft and online fraud.
State-sponsored actors	Foreign governments and intelligence services use cybertools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programmes and capabilities.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites.
Insiders	The disgruntled organisation insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals or small groups who execute phishing schemes in an attempt to steal identities or information for monetary gain
Spammers	Individuals or organisations that distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware or attack organisations (e.g., denial-of–service attacks)
Spyware/malware authors	Individuals or organisations that produce and distribute spyware and malware, sometimes for free and sometimes to sell to the highest bidder
Terrorists	Terrorists seek to destroy, incapacitate or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the global economy, and damage public morale and confidence.

Picture Credit (Hayes, Shore & Jakeman, 2012)

An independent organization that constantly reviews configuration settings across multiple vendors, supported by a brain trust of IT professionals, was long overdue. “Researchers have long studied the sheer cost-effectiveness of planning for and preventing defects upfront rather than finding and fixing them later” (Sethi & Foroughi, 2012). One good example of this collaboration and mitigation is the Center for Internet Security (CIS). All CIS references will be in bold and italicized to avoid confusion.

“CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (‘Products’) as a public service to Internet users worldwide. Recommendations contained in the Products (‘Recommendations’) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs. This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel, who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Windows 7” (‘Cis windows 7,’ 2012). While it doesn’t state the obvious here, even home users can utilize these standards on their personal Windows-based platform(s) at home. CIS even provides for other operating systems, databases, etc.

Another great thing about the CIS standards is that “they don't perform any actual testing and also don't dictate how the tests are supposed to be done. …the fact that CIS does not mandate how a test is performed…means you can use scanning, a credentialed audit, an agent, a reference gold image or magic” (Gula, 2011). As this is a SANS Gold level paper, the use of magic simply cannot be supported here.

There are a few housekeeping items about the CIS standards that will help guide users throughout the benchmark - the definition of “security profiles.”

*“**Enterprise***

Settings in this level are designed for systems operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are ‘Windows XP SP3 or later’ and ‘Windows Server 2003 SP2 or later.’ In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.

Specialized Security – Limited Functionality (SSLF)

Settings in this level are designed for systems in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Not Defined

These items do not impact a system’s score as the Benchmark does not recommend a specific value for this setting and profile combination.

Not Configured

The default behavior of Windows is commonly a secure behavior. For several settings, Windows allows the administrator to reinforce the default behavior by enabling or disabling a setting. Given this, for the Enterprise profiles, several settings are recommended Not Configured as the default behavior is secure. For the SSLF profiles, the Benchmark recommends that the default behavior be reinforced via GPO. An Enterprise profile system that is configured in accordance with the SSLF profile recommendation is not deemed out of conformance with this Benchmark” (‘Cis windows 7,’ 2012).

2. A Review of Select CIS Standards for Windows 7 Configuration

Within most organizations, there is an IT group responsible for the configuration and maintenance of various corporate assets such as servers and workstations/laptops. Many organizations customize their “baseline image” for each platform (desktop/laptop/server) so that every time they need to rebuild an asset, they have incorporated the previous patches and don’t have to wait while multiple patches install as pre-requisites to the newest ones not incorporated in the baseline image, taking a painful amount of time in most situations.

Patch levels can be accounted for in this image building process through tools such as Symantec’s Ghost product and Microsoft’s own native toolset. You can also affect the level of protection on the asset by setting the configuration settings on audit, security and application capabilities. “The vast majority of cyber attacks exploit known vulnerabilities for which a patch or security configuration control is available. 80-100% of known vulnerabilities are blocked by implementing the CIS consensus benchmark configuration controls and applying available patches” (Carrington, 2006).

While this paper is by no means completely inclusive (the CIS standard itself is almost 200 pages of recommendations) it will highlight a number of security settings that may get overlooked in the effort to get the asset into production status.

By utilizing the already battle-tested CIS standards, you will incorporate an immense amount of support into your Information Security Management System (ISMS), as it can help to raise awareness and a call to action for tasks that may seem mundane to some, but are recognized as critically important when doing a post-mortem of a breach incident.

Some folks may question the use the CIS standard to contribute to forming an audit standard. While certainly not the only option, it does itself go through a process whereby multiple authorities on the subject matter can contribute, ratify, and publish the standards. This is very similar to the iterative process espoused within ISO 27001, making these two very complementary.

While ISO 27001 provides for a higher level of guidance, the CIS standards provide for the granular level that will keep your technical folks happy. Not only will they have specific guidance for the platforms in your organization that they can implement “check-list” style, they will also have the opportunity to contribute their own opinions, lessons learned, and generally keep their interest in continuing to participate in the process. So while folks may question the means (and a lot of different things go through “review” process to decide if they’re still needed or relevant), they certainly shouldn’t question the end result – especially if you are able to implement these standards and show their value to the organization.

Now let's look at a few of the Windows 7 settings within the CIS standard for this platform. The ones highlighted here were chosen because of their applicability in a wide number of organizations. Even if they are not yet implemented, they surely will be soon as technology moves all platforms forward (smaller companies are likely to start using virtualization for example).***"Account Policies***

1.1.1 ***Enforce password history***

Description:

This control defines the number of unique passwords a user must leverage before a previously used password can be reused. For all profiles, the recommended state for this setting is 24 or more passwords remembered.

Rationale:

Enforcing a sufficiently long password history will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential. For example, if an attacker compromises a given credential that is then expired, this control prevents the user from reusing that same compromised credential.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value:

24 passwords remembered" ('Cis windows 7,' 2012)

This should align with default domain policy, and with regard to multiple domains, it should align across all security domains. Workstation password history should match the domain password history in order to simplify things.

There will no doubt be certain situations whereby this cannot be truly replicated across multiple domains, and that should be accounted for in a variance to your standards document and housed in a centralized area such as a SharePoint, to be reviewed at a regular interval to determine if this control can be implemented at a future date.

1.1.2 "*Maximum Password Age*

Description:

This control defines how many days a user can use the same password before it expires. For all profiles, the recommended state for this setting is 90 days or less.

Rationale:

Enforcing a reasonably short password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.

Default Value: 42 days" ('Cis windows 7,' 2012)

While the default value for this control is 42 days, most organizations will likely have it set to 90 days to satisfy Payment Card Industry (PCI) compliance as described above. Even if you are not an organization who is beholden to the Payment Card Industry Data Security Standard (PCI-DSS) it may be advisable if you intend to someday jump into the foray of accepting credit card payments.

It is hard to imagine any company in this present time that does not accept credit cards, although very small businesses might fill this space. By taking these steps in advance, the organization may make itself a more attractive partner or take-over target to larger companies.

1.1.4 “***Minimum password length***

Description:
This control defines the minimum number of characters a user password must contain. It is recommended that this setting be configured as described below:

For the SSLF profile(s), the recommended value is 12 or more characters.

For the Enterprise profile(s), the recommended value is 8 or more characters.

Rationale:
Enforcing a minimum password length helps protect against brute force and dictionary attacks, and increases the efficacy of password-based authentication systems.
Remediation:
To establish the recommended configuration via GPO, set the following to the value above:
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length
Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed.
Default Value: Zero characters” (‘Cis windows 7,’ 2012)

Despite the ease with which nefarious individuals can take advantage of low hanging fruit such as weak passwords, it is very common to find default configurations such as the above – zero characters! This is unfortunate, but designed to be user friendly. In the Special Security – Limited Functionality setting recommendation above it does note that is a suggested 12 characters.

To support this argument, consider the following: “The 12-character era of online security is upon us, according to a report published this week by the Georgia Institute of Technology. The researchers used clusters of graphics cards to crack eight-character passwords in less than two hours. But when the researchers applied that same processing power to 12-character passwords, they found it would take 17,134 years to make them snap" (Sutter, 2010).

This quote originated in 2010, by a very reputable university. Fast-forward a meager two years and the conversation and the math, changes dramatically. "There needs to be some kind of Moore's law analog to capture the tremendous advances in the speed of password cracking operations. Just within the last five years, there's been an explosion in innovation in this ancient art, as researchers have realized that they can harness specialized silicon and cloud based computing pools to quickly and efficiently break passwords" (Roberts, 2012).

Admittedly, breaking passwords online and offline are different beasts, but the concept itself is both instructive and scary to Information Security professionals. The lesson here is that despite the default setting, you should really consider the Special Security – Limited Functionality setting recommendation.

“1.3 ***Detailed Audit Policy***

1.3.8 Audit Policy: Object Access: File System

Description:

This control defines whether an audit entry is created when file objects are accessed. It is recommended that this setting be configured as described below:

> ***For the SSLF desktop and SSLF laptop profile(s), the recommended value is Failure.***
>
> ***For the Enterprise desktop and Enterprise laptop profile(s), the recommended value is No auditing.***

Rationale:

Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies - Local Group Policy Object\Object Access\Audit File System\Audit Policy: Object Access: File System

Perform the following to establish recommended configuration state via auditpol.exe.

auditpol /set /subcategory:"File System" [/success:<enable|disable> /failure:<enable|disable>]

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

auditpol /get /subcategory:"File System"

Default Value: No auditing” (‘Cis windows 7,’ 2012)

This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all.

Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. (http://technet.microsoft.com/en-us/library/cc776774%28WS.10%29.aspx)

For corporations that operate customer facing assets such as web servers with back-end databases, kiosks, point-of-sale (POS) devices, etc., it will commonly export the logs of these assets through a File Integrity Monitoring/Security Event Incident Monitoring solution for correlation and investigation to determine patterns of unauthorized activity. This eliminates the possibility of the local log storage being overwhelmed, and failing to maintain useful information that can be used to mitigate potential abuse of the asset and the underlying data.

"1.6 ***Windows Update***

1.6.1 Configure automatic updates

Description:

This control defines whether Windows will receive security updates from Windows Update or WSUS. For all profiles, the recommended state for this setting is Enabled: 3 - Auto download and notify for install.

Rationale:

Establishing automated means to deploy and apply system updates will help ensure the system always has the most recent critical operating system updates and service packs installed. It is recommended that organizations align this option with their patch policy. For more information on patch management, see http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v AUOptions reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v NoAutoUpdate

Default Value: Download the updates automatically and notify when they are ready to be installed" ('Cis windows 7,' 2012)

Although the recommendation for this is Enabled: 3 – Auto-download and notify for install, most companies have an over-arching management tool that incorporates update management to both Microsoft and non-Microsoft software. Examples include: Symantec Endpoint Management, IBM's Tivoli, HP's Radia, etc.

By preventing the automatic download, your development and server/client groups can determine whether or not they need the patch (the patch may not be applicable in your environment) or it should be accepted as a risk to **not** implement. Discussion could raise the concern that would cause harm to the organization (especially those with a large amount of customized or home-grown applications) by unexpected freezing or crashing operating system responses at the most inopportune of times.

Every company should have an established process whereby the amount of time to download, validate, and deploy is appropriate, based on the severity of the deficiency the update is to solve for.

“1.6.3 No auto-restart with logged on users for scheduled automatic updates installations

Description:

This control defines whether Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. For all profiles, the recommended state for this setting is Disabled.

Rationale:

Enforcing and restricting access to this control is important because if computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

reg query HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v NoAutoRebootWithLoggedOnUsers

Default Value: Enabled” (‘Cis windows 7,’ 2012)

In both of the above control settings, it is assumed that the corporation does not allow end users to be able to affect the download and installation of Windows updates. While that may be true, the end user *does* have the ability to decide whether or not they shut their computers down for the evening.

Not too long ago, users were instructed by companies to just “lock” their computers at the end of the day to ensure that patches could be pushed to the workstations after hours. Many users also left the monitors on, leading to a somewhat comical shadow image being burned into many CRT monitor screens; even when turned off you could see the silhouette of the Novell or Windows login logos!

“Disable” is definitely the best setting here to ensure your assets are appropriately processing the patches they need a reboot to complete, in order to harden themselves against vulnerabilities. Don’t take chances by leaving the patching process beholden to user preferences.

“1.9 ***Security Options***

1.9.16 Domain member: Disable machine account password changes Description:

This control defines whether a domain member can periodically change its computer account password. For all profiles, the recommended state for this setting is Disabled.

Rationale:

By disabling this policy setting on all domain controllers, domain members will be able to periodically change their computer account passwords, which in-turn reduces their susceptibility to attacks.

Remediation:

To establish the recommended configuration via GPO, set the following to the value prescribed above:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes

Audit:

Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:

reg query HKLM\System\CurrentControlSet\Services\Netlogon\Parameters /v disablepasswordchange

Default Value: Disabled” (‘Cis windows 7,’ 2012)

Although the recommendation is spot on here, some exceptions to this will be required. For example, VM-based test systems are often "snapshotted" and then reverted back to known good. This could result in a VM having an expired password after restoration. In this situation, newer administrators or non-technical folks may cause undue concern and confusion over this.

"1.9.20 Interactive logon: Number of previous logons to cache (in case domain controller is not available)

> ***Description:***
> ***This control defines whether a user can log on to a Windows domain using cached account information. When a workstation belongs to a domain, users can log on to it using domain credentials. The domain credentials can be cached in the local workstation's Security Accounts Manager (SAM) database. On next logon, should no domain controller be available, the user can still log on locally by authenticating against the cached account information. When logging on using cached credentials, some account properties will not be enforced, since the domain controller maintains responsibility for enforcing account policy. The local SAM database does not "own" the account, so cached account passwords do not expire, and domain accounts can not be locked out when the domain is unavailable.***
> ***When establishing corporate policy for cached accounts, consider the remote user. They commonly log on with cached credentials from a laptop. To access corporate resources, the user establishes a Virtual Private Network (VPN) connection to the corporate network. Since logon occurs before the domain is available—the VPN has not yet been established—the user will never be prompted to change the password on the cached account. This setting only affects workstations joined to a domain, and only impacts interactive logons with domain accounts. The workstation will not cache non-interactive log on information. Change this setting to zero to disable the caching of domain accounts in the local SAM database. It is recommended that this setting be configured as described below:***
>
> > ***For the Enterprise desktop, Enterprise laptop and SSLF laptop profile(s), the recommended value is 2 logons.***

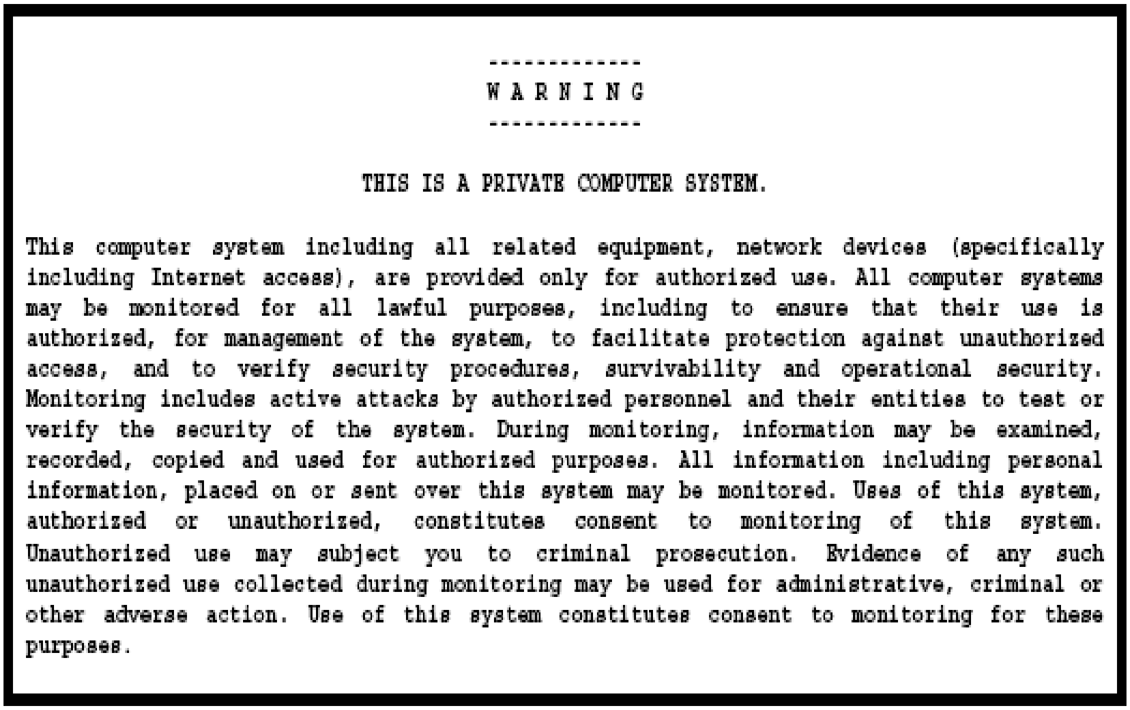
> ***For the SSLF desktop profile(s), the recommended value is 0 logons.***
>
> ***Rationale:***
> ***Setting the number of cached logon to the appropriate level for the system's profile will remove an avenue for an attacker to further compromise the environment by deriving credentials from the cache while allows logons should the domain become unavailable.***
> ***Remediation:***
> ***To establish the recommended configuration via GPO, set the following to the value prescribed above:***
> ***Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)***
> ***Audit:***
> ***Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:***
> ***reg query HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon /v cachedlogonscount***
> ***Default Value: 10 logons"*** ('Cis windows 7,' 2012)

This recommended value of 2 logons is most likely accurate for most organizations. The default value of 10 logons may be too high, but situations whereby certain groups are sharing laptops (like the on-call groups that rotate a laptop and on-call pager (smartphone) or "go" teams called to action during an incident.

> ***"1.9.24 Interactive logon: Message text for users attempting to log on***
>
> ***Description:***
> ***This control defines a text message that displays to users when they log on. For all profiles, the recommended state for this setting is the text blessed by your organization.***
> ***Rationale:***

> ***Enforcing this control may be important in limiting the potential for unauthorized users attempting to gain access to perform an attack on the system by notifying them of the consequences of their misconduct.***
> ***Remediation:***
> ***To establish the recommended configuration via GPO, set the following to the value prescribed above:***
> ***Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on***
> ***Audit:***
> ***Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. Alternatively, execute the following to determine if the system is configured as recommended:***
> ***reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v LegalNoticeText***
> ***Default Value:***
> ***Not defined"*** ('Cis windows 7,' 2012)

This particular setting should not be overlooked! It provides fair warning to those individuals who may at a later time say that they didn't realize that they were exceeding their authority because the asset lacked a warning banner similar to the one below. You should work very closely with Legal on the wording to ensure that the use of the system clearly implies consent with whatever requirements are stated within the text.



```
                         -------------
                         W A R N I N G
                         -------------

                 THIS IS A PRIVATE COMPUTER SYSTEM.

This computer system including all related equipment, network devices (specifically
including Internet access), are provided only for authorized use. All computer systems
may be monitored for all lawful purposes, including to ensure that their use is
authorized, for management of the system, to facilitate protection against unauthorized
access, and to verify security procedures, survivability and operational security.
Monitoring includes active attacks by authorized personnel and their entities to test or
verify the security of the system. During monitoring, information may be examined,
recorded, copied and used for authorized purposes. All information including personal
information, placed on or sent over this system may be monitored. Uses of this system,
authorized or unauthorized, constitutes consent to monitoring of this system.
Unauthorized use may subject you to criminal prosecution. Evidence of any such
unauthorized use collected during monitoring may be used for administrative, criminal or
other adverse action. Use of this system constitutes consent to monitoring for these
purposes.
```

Photo Credit (Radvanovsky, 2004)

2.1. Incorporating the right stakeholders to review CIS Standards

"Humans are bad at estimating risk. When we are not in control we over-estimate (shark attack at the beach), when we are in control we underestimate (vending machine falls on you as you rock it to get your money back)" (Spitzner, 2012). Utilizing the CIS standards will allow you to gather input from a wide range of folks in your organization to come up with a "Goldilocks" strategy…not over-estimate or underestimate of what needs to be done, but "just right."

Our IT folks and a large portion of our end users "already know how to use technology; we just need to change their behavior so they can use it safely. Awareness is just another control to reduce risk…" (Spitzner, 2012). While it is admittedly hard to change their behavior, providing them with standardized platforms hardened by the CIS standards, you are in effect changing behaviors by not allowing some things to happen that might otherwise if certain configurations are left in their "default" setting.

"Management buy-in is a very important part of the implementation equation.

Why should management care? An easy and quick way to let management know the benefits are a slide deck that should go into high level detail about the following topics: 1. CIS standard implementation will help reduce risk, 2. Remain compliant with regulatory and industry mandates (PCI for example) , and 3. Reduce costs. To get the budget you need to drive this initiative, you have to identify the need" (Spitzner, 2012).

"Standards will usually specify what must be done. In an information security framework…a standard is a list of what must be done. In a sense, you could think of this in terms of being required to meet a certain standard before a building inspector will issue you a building permit or certificate of occupancy. Rather than allow administrators or users to turn on and plug in new systems, require that they go through an accreditation process, after which they are issued an electronic building permit. This accreditation process becomes your standard" (Hoelzer, 2012).

Once you have decided to align your organization with a certain CIS standard, it is important that you find these "building inspectors" within your organization and socialize the proposed settings to ensure cooperation and buy-in.

Putting these requirements (in the form of the CIS standards for Windows 7 in this case example) into the project requirements *early* will be met with less resistance than if you try to inject them when the project is close to completion. In this way, you are also doing it for them (this is a very good tool in becoming extremely popular with your stakeholders!).

And additional benefit is that "knowing security controls up front allows development teams to build cost estimates and prioritize security issues alongside other priorities at project or iteration inception. Upfront discussion and risk acceptance have the benefit of side-stepping disagreements later in a development cycle and avoiding a culture of development vs. security" (Sethi & Foroughi, 2012).

"While the components of information security, i.e. requirements definition, strategy and policies, technology, process, and people…are common to all organizations, like snowflakes, no two implementations are identical. The parameters that make a difference include organizational requirements, culture, the level of resources available and employee engagement. The consequence of this is that what may be 'good enough' for one organization may be totally inadequate for another" (Gelbstein, 2012).

There may also be situations in your organization in which the settings may have to differ materially from division to division, making this iterative process even more important. The stakeholders may change as well, making constant communication (possibly quarterly meetings convened at the Information Security Officer level with representatives from each division) and identification of key individuals a necessary component of success.

"Some people…begin to balk when they discover that 27002 very strongly recommend the creation of a number of committees, all working under the guidance of the Information Security Officer and the steering committee. If you consider the committees that are recommended, you realize that they are placed at key control junctures for business and security objectives, which is only appropriate.

So this means that the committee should be composed of:

Management members who are committed to the policy process

Process owners who have proven themselves to be effective process mangers/owners

Auditors who have been able to keep pace with changes in the organization and report on risk effectively

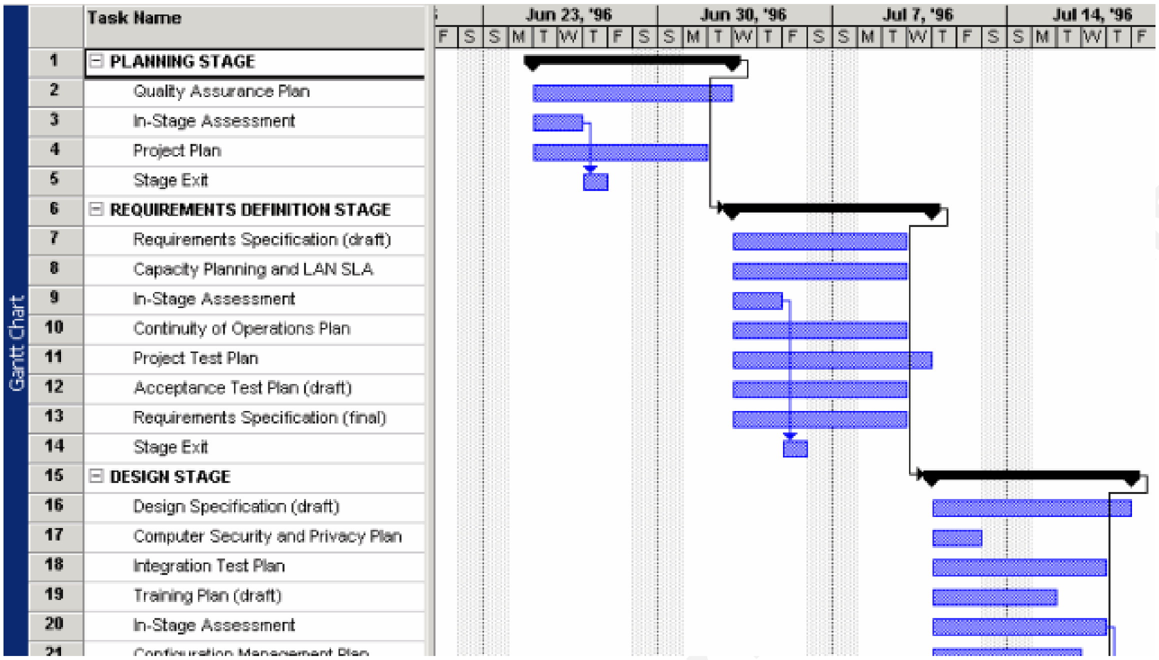
> The Information Security Officer, who will be a ‘member’ of each committee, but who may not attend every meeting. The committees report to the Information Security Officer.
>
> Legal department representatives who are current on appropriate business case law and state/federal requirements” (Hoelzer, 2012).

It is also advisable when choosing participants that they are interested in participating in the initiative. Many good intentioned projects are scuttled by poor participation due to lack of interest, time, or a multitude of other excuses!

A good way to motivate these folks (because some will likely be “volunteered” for these committee reviews) is to keep reminding them of the fact that they will be guiding principles that will not only create a secure posture for the company, but will make their jobs easier as well.

“When the committees are formed and given tasks, it is very important to give them reasonable deadlines at the same time. From an effective project management standpoint, you may even want to lay out a series of milestones for the committee so that they know where they are going” (Hoelzer, 2012).

Having a project manager (PM) in charge of the initiative can lessen the burden on the more technical folks, who in the absence of a project manager are going to likely be charged with making this happen. A good project manager will come up with a project plan (like the one below) that will give everyone estimated dates and tasks, so that there is a clear reminder of the end goal, as well as check points to ensure that the overall goal will be met.



	Task Name
1	⊟ PLANNING STAGE
2	Quality Assurance Plan
3	In-Stage Assessment
4	Project Plan
5	Stage Exit
6	⊟ REQUIREMENTS DEFINITION STAGE
7	Requirements Specification (draft)
8	Capacity Planning and LAN SLA
9	In-Stage Assessment
10	Continuity of Operations Plan
11	Project Test Plan
12	Acceptance Test Plan (draft)
13	Requirements Specification (final)
14	Stage Exit
15	⊟ DESIGN STAGE
16	Design Specification (draft)
17	Computer Security and Privacy Plan
18	Integration Test Plan
19	Training Plan (draft)
20	In-Stage Assessment
21	Configuration Management Plan

Photo Credit (Atwood, 2006)

Productivity suites such as Microsoft's Outlook can provide a great opportunity to gently "remind" people of due dates regarding their tasks. Keeping already busy people on point for your initiative is half the battle!

"One of the early lessons practitioners learn is that their activities are invisible until something goes wrong, at which time the reaction is swift and often hard. Engaging in dialog with executives, senior managers and other parts of the business—including procurement and legal counsel—to understand their perceptions and requirements is highly recommended. It must be recognized that these groups have their own accountabilities and pressures to deal with, that their time is valuable (and not to be wasted), and that information security may not appear on their lists of priorities. Therefore, good preparation and soft skills have become prerequisites for such dialog to be meaningful" (Gelbstein, 2012).

2.1.1. Publishing accepted standards for your organization

"Our next step is to put our training and security awareness programs into place. There would actually have been some training already occurring, but here we're talking about the long term, ongoing training and security awareness programs. Even in the ongoing scenario, various groups of individuals within our organization will have different needs in terms of training and awareness" (Hoelzer, 2012).

The implementation of the CIS standards for select platforms doesn't necessarily imply that it must become part of your information security awareness training that is released to your entire population as part of recurring training. Rather, it should find a home next to things like secure coding training (developer), and hazardous materials handling (shop or bio-lab worker). It may be a good idea to task your training department with the implementation of these various tracks of compliance training, and have them centralize the information to ensure it stays current and always available to your desired population.

Once the realm of only large companies, a Learning Management System (LMS) can be leveraged to perform initial notification, tracking, and even issue completion certificates when completed. These shouldn't be the system of record for your standards, but should reference them appropriately. For the CIS Windows 7 standards, the appropriate place to house these documents would be an IT intranet page that is accessible to the entire company for utilization. When asked about requirements in the early stages of a project, the link could be provided directly to the participants ensuring that they are not sent a soon to be outdated document, but in fact a living link.

Your corporate communications department can be a great asset to leverage. They can assist in getting the word out to the organization that these committees have done a great job in solidifying standards that will secure the enterprise, and provide steady guidance to future business initiatives that will rely heavily on the technology you are hardening. It may be advisable to utilize the corporate recognition platform to thank your participants as well to encourage future team work and "esprit de corp."

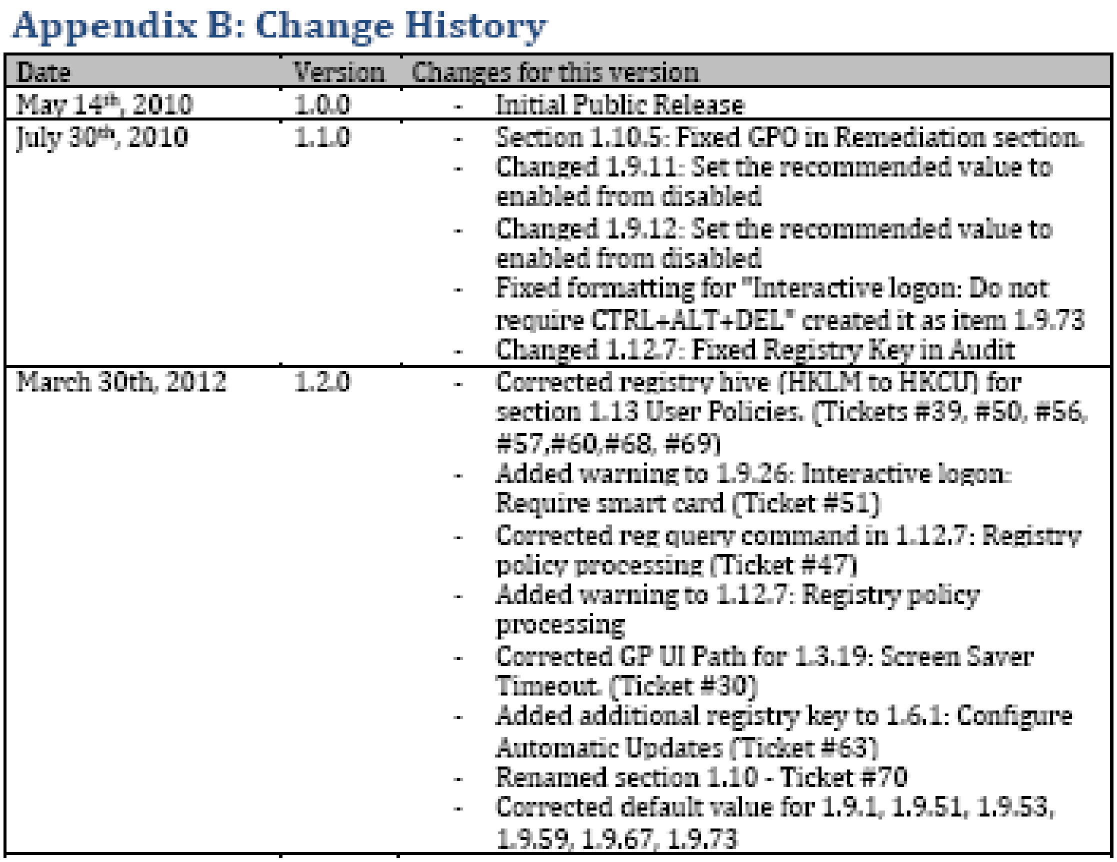
While it is said to "beware Greeks bearing gifts" in reference to the infamous Trojan Horse, you should take care to always show appreciation to your participants in the form of some small token (just not a horse), even if it's a simple certificate with your company logo stating your appreciation for their contribution.

Once the agreed upon standards have been released and published to your organization, you now need to ensure that they stay relevant in order to maintain the support of your population. "We now begin to monitor and review the ISMS continually. This is actually one of the greatest values of 27001 since it forces us to be pro-active in monitoring and correcting our organization over time. For instance, here are some of our monitoring tools: System administrators, security administrators, auditors, human resources, incident response teams…All of these contribute information regulary that can be used to derive the overall health of the ISMS and determine if there are problems or flaws developing" (Hoelzer, 2012).

When you are monitoring your ISMS, the CIS standards should be reviewed as well, as they are a living body a work that is constantly being updated by the larger information technology professional community, based on emerging thinking and application of existing technology. There may be certain settings that were deemed acceptable as "Default" that are no longer acceptable. This is why it is critically important to maintain constant contact with your stakeholders and communicate often what you are doing so that no one is surprised if and when the standard should change. In situations whereby the settings may be impediments to further progress, the review can take place in an ad-hoc fashion, but reviews this way should be an exception.

"As new risks are identified, they can be addressed by adding new pieces to the ISMS. If our business requirements or objectives change, they can be modified in the ISMS and the ISMS can adapt to the new requirements over time" (Hoelzer, 2012). This thinking can also be applied to the CIS standards that you have incorporated into your organization. Rather than taking on each standard in an ad-hoc fashion, they should follow a regular pattern so that your stakeholders can get used to the schedule of review. Suggested review periods should not exceed one year to ensure you are using relevant guidance that will not be obsolete very quickly (admittedly, in Information Technology everything seems to become obsolete very quickly as Moore's Law continues it disruptive progress!).

The group responsible for the maintenance of these standards and the incorporation of the CIS standards as well, should also be mindful of including a change history much like the one below. It provides a running log of changes (both technical and grammatical) and acts as a "running rationale" in order to give context, so that decisions that may have seemed perfectly logical at one point can change as necessary to newer thinking and guidance. It's very important to stay relevant!



Appendix B: Change History

Date	Version	Changes for this version
May 14th, 2010	1.0.0	- Initial Public Release
July 30th, 2010	1.1.0	- Section 1.10.5: Fixed GPO in Remediation section. - Changed 1.9.11: Set the recommended value to enabled from disabled - Changed 1.9.12: Set the recommended value to enabled from disabled - Fixed formatting for "Interactive logon: Do not require CTRL+ALT+DEL" created it as item 1.9.73 - Changed 1.12.7: Fixed Registry Key in Audit
March 30th, 2012	1.2.0	- Corrected registry hive (HKLM to HKCU) for section 1.13 User Policies. (Tickets #39, #50, #56, #57,#60,#68, #69) - Added warning to 1.9.26: Interactive logon: Require smart card (Ticket #51) - Corrected reg query command in 1.12.7: Registry policy processing (Ticket #47) - Added warning to 1.12.7: Registry policy processing - Corrected GP UI Path for 1.3.19: Screen Saver Timeout. (Ticket #30) - Added additional registry key to 1.6.1: Configure Automatic Updates (Ticket #63) - Renamed section 1.10 - Ticket #70 - Corrected default value for 1.9.1, 1.9.51, 1.9.53, 1.9.59, 1.9.67, 1.9.73

Photo Credit ('Cis windows 7,' 2012)

3. Conclusion

As the CIS standard for Windows 7 has shown a pragmatic approach to the configuration of the assets it will live on, so should you when incorporating them into your environment. In review, the steps you should take on behalf of your organization are as follows:

1. Provide a recommendation to your Information Security Officer to obtain the authority to carry forward the implementation of the CIS standards in support of your ISO 27001-based Information Security Management System

2. Review the selected CIS standard as a stand-alone document to familiarize yourself with the details and rationale.
3. Compare and contrast each setting in the standard with your current corporate setting.
4. Request participation from various stakeholders in your organization utilizing communication chains that may already exist through your Information Security Officer. If there is currently no structure for this purpose, take this opportunity to develop one and then cultivate and maintain it.
5. Utilizing a dedicated project manager, create an over-arching project plan to review the specific CIS standards applicable in your environment.
6. Review with the stakeholders selected settings that may have a negative impact. Such examples include, but are not limited to training situations, on-call situations, etc., where many people may have short term access or access to non-production data. Use these situations to guide an appropriate exception to the CIS standard and denote it as a corporate standard.

7. Utilize your corporate communications division to help announce and socialize the “new” (new to your company at least) standards amongst everyone.

8. For specific groups like developers, target this knowledge transfer through a Learning Management System (LMS) to ensure that the standards are incorporated into their build processes as they go forward.
9. Determine a set schedule whereby the CIS standards that are applicable and implemented in your environment, continue to be reviewed on a regular schedule not to exceed once per year. While trying to maintain the same stakeholders, account for turnover and changes within the organization, and leverage your Information Security Officer for assistance with this.
10. Stay vigilant! Only by continuing this iterative process will you advance your Information Security Management System to new, more secure heights!

4. References

Books

Strunk, William Jr. & White, E. B. . *The Elements of Style*. New York, NY: Longman

Hoelzer, D. (2012). *Introduction to ISO/IEC 2700: Policy, ISMS, and Awareness*. (V2012_0228 ed., Vol. 411.1). Baltimore: The SANS Institute.

Hoelzer, D. (2012). *SANS 27000 Controls and Process Improvement II*. (V2012_0228 ed., Vol. 411.3). Baltimore: The SANS Institute.

Hoelzer, D. (2012). *SANS 27000 Controls and Process Improvement III*. V2012_0228 ed., Vol. 411.4). Baltimore: The SANS Institute.

Hoelzer, D. (2012). *ISO 27000 Implementation.* (V2012_0228 ed., Vol. 411.6). Baltimore: The SANS Institute.

Magazines

Ross, S. (2012). Information security matters: The cost of cyberattacks. *ISACA Journal*, *6*, 4.

Gelbstein, E. (2012). Demonstrating due diligence in the management of information security. *ISACA Journal*, *6*, 17-20.

Sethi, R., & Foroughi, E. (2012). Preventative technical controls for application security. *ISACA Journal*, *6*, 26-28.

Hayes, S., Shore, M., & Jakeman, M. (2012). The changing face of cybersecurity. *ISACA Journal*, *6*, 29-36.

Web

Warlick, David (2004). Son of citation machine. Retrieved February 17, 2009, from Son of citation machine Web site: http://www.citationmachine.net

Cis windows 7 benchmark v1.2.0. (2012, March 30). Retrieved from https://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.windows7.120

Gula, R. (2011, November 2). [Web log message]. Retrieved from http://blog.tenablesecurity.com/2011/06/comparing-the-pci-cis-and-fdcc-certification-standards.html

Carrington, A. (2006, October). *Auditing and hardening unix*. Retrieved from http://www.bedrocksecurity.com/ISC2_Seminar_Oct_05_-_Auditing_and_Hardening_Unix.pdf

Asadoorian, P. (2009, November 22). [Web log message]. Retrieved from http://blog.tenablesecurity.com/2009/04/auditing-linux-apache-mysql-against-cis-benchmarks.html

Atwood, J. (2006, November 14). [Web log message]. Retrieved from http://www.codinghorror.com/blog/2006/11/microsoft

Sutter, J. (2010, 08 20). *How to create a 'super password'*. Retrieved from http://www.cnn.com/2010/TECH/innovation/08/20/super.passwords/

Radvanovsky, B. (2004, 05). *Whitepaper: Login warning banners*. Retrieved from http://unixworks.net/papers/wp-007.pdf

Roberts, P. (2012, 12). *New 25 gpu monster devours passwords in seconds*. Retrieved from http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds/

Spitzer, L. (2012, 10). *Why security awareness matters - 1st in series*. Retrieved from https://www.sans.org/webcasts/access-elm.php