Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

CASE STUDY ON IMPROVING THE SECURITY OF A FIRM I A LEGACY APPLICATION SETTING

This paper documents the steps that were taken by me to increase the security within my firm's computer network system, a system that includes Windows XP workstations and Windows 2000 Server systems. The implementation process includes enhancements to internal firm policies and procedures as a result of and in response to an updated firm risk assessment. Recent legislative activities in the State of California regarding the privacy of names and social security numbers maintained within network computer systems dictated...

Copyright SANS Institute

Author Retains Full Rights

AD

CASE STUDY ON IMPROVING THE SECURITY OF A FIRM IN A LEGACY APPLICATION SETTING

By

Susan E. Bradley, CPA, CITP, MCP

GSEC Practical Assignment
Version 1.4b

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

CASE STUDY ON IMPROVING THE SECURITY OF A FIRM IN A LEGACY APPLICATION SETTING

TABLE OF CONTENTS

ABSTRACT 2
BEFORE PROCEDURES 2-8
- Current practice regarding Legacy Applications..... 2
- Security Implications of each level 3
- Additional analysis of current security practices..... 4
- Review of current employee manual 4
- Recent legislative actions and revised risk analysis..... 5
- Analysis of risk categories and factors 5
- Assigning value to the assets..... 5
- Physical damage and malfunctions..... 6
- Attacks 6
- Estimation of potential loss from the risk or threat 7
- Estimate the possible frequency of the threat occurring..... 7
- Calculation of the cost of the risk..... 8

DURING PROCEDURES 8-16
- Review of sources of documents regarding Windows XP Security..... 8
- Recommended changes and testing..... 9
- Use of Registry key changes 14
- Adjusting Firewalls for Egress filtering and notification..... 15
- Changes to employee manual..... 16

AFTER PROCEDURES 16-17
- Additional remedial recommended procedures..... 16

REFERENCES 18-19
BIBLIOGRAPHY 20
APPENDIX A - Graphical views of Microsoft Baseline Security Advisor prior to corrective actions on a Testing platform: 21-24
APPENDIX B - Graphical views of corrective actions taken on a Testing platform: 25-29
APPENDIX C Revised sections of the Employee Manual with direct implications to my firm's information technology..... 30-37

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

CASE STUDY ON IMPROVING THE SECURITY OF A FIRM IN A LEGACY APPLICATION SETTING

ABSTRACT:

This paper documents the steps that were taken by me to increase the security within my firm's computer network system, a system that includes Windows XP workstations and Windows 2000 Server systems. The implementation process includes enhancements to internal firm policies and procedures as a result of and in response to an updated firm risk assessment. Recent legislative activities in the State of California regarding the privacy of names and social security numbers maintained within network computer systems dictated a self-imposed review of our current security practices.

The network in my firm was previously set up when "legacy" business applications required and needed more access to the registry of the attached workstations. As is the case, typical business applications that are written for a specific industry are trailing in their use and application of securely written code. These types of applications are typically referred to as "legacy applications", that is, written for the Win95/98 code base when access to the Windows registry was freely allowed by those Operating systems. Current operating systems and business programs are designed to be connected to networks with restrictions to this access.

State and national legislative bodies are becoming increasingly aware of the impact of technology in business practices. Recent laws enacted by the State of California have imposed a need to review the current security practices in my firm. Businesses should periodically review their security practices to ensure that they are in compliance with governing bodies having jurisdiction in their industries. In addition, business practices should be reviewed on a regular basis to ensure that the applications running within the network systems allow for increased security and that the network policies and procedures are updated.

BEFORE PROCEDURES

Current practice regarding Legacy Applications

Currently, I am the Chief Information Officer, network administrator, and computer troubleshooter for the computer network at my office. My firm is a Certified Public Accounting office requiring support for legacy applications within its network. The legacy application that is featured in this case study is one that is a typical accounting program used by numerous small to medium sized businesses. This product, called **Quickbooks**[i], is a single or multi-user accounting package that can be installed in a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

small network environment. The installation instructions as provided by the Vendor, clearly state that in order to properly operate the program, the "permissions level" of the workstation must be changed to allow the user to be "Standard user or higher".[ii] The instructions provided by the Vendor detail the steps necessary to raise the level of the local user. Those steps are as follows:

"To resolve this issue in Windows 2000 or Windows XP, set up each user of this computer with group memberships of Standard user or Other: Administrator permission level. To accomplish this:

1. *Log on to the system as a local administrator.*
2. *On the taskbar, click the **Start** button, choose **Settings**, and then choose **Control Panel**. (For Windows XP: Click the **Start** button and choose **Control Panel**.)*
3. *Double-click **Users and Passwords**. (For Windows XP: Click **User Accounts**.)*
4. *Under **Users for this computer**: is the user listed?*
    a. *If the user is listed, click **Properties**. Skip to Step 5.*
    b. *If the user is not listed, click **Add**, enter the user's login and network domain, and then click **Next**.*
5. *You are now at the **Access Level/Group Membership** assignment window. Choose either **Standard** or **Other: Administrator**.*
6. *Click **Finish** or **OK"**.*[iii]

These actions elevate the user on the workstation to either a "Power User" level or "Local Administrator" level. When the user has local "Power User" ability, he or she is allowed to "customize time, display settings, printers, and shares on the computer".[iv] When users are added to the "Local Administrator" group, they are allowed to perform any function on that local computer. They are allowed to install hardware drivers, services, configure audit policies, and other critical functions,[v] the assignment of these privileges normally are unacceptable to unauthorized and/or untrained computer users in a domain environment.

Security implications of each level

"Power users" are allowed to customize shares on a computer. Unprotected Shared Folders are specifically identified by the SANS organization as a security weakness in a December 2002 handout, "The Top Ten Windows Vulnerabilities"[vi] in the section discussing Unprotected Shared Folders. As discussed in the handout, both Sircam virus [*CERT Advisory 2001-22*[vii]] and Nimda worm [*CERT Advisory 2001-26*[viii]] spread rapidly across networks by using unprotected network shares.

"Local Administrator" users present an even larger security implication in a network setting. These users are given full access to the registry of their systems. Identified as number nine in the Top Ten Handout[ix], "improper permissions or security settings can permit remote registry access". Making users "Local Administrators" degrades protection of the registry of the system. The practice I have followed up to this point in my network has been to set the user to be a "Local Administrator" of the computer to allow the legacy application to work properly and obtain regular program updates from the vendor. Given the current state of Viruses, Trojans and other malware, my use of "Local Administrator" violates the principle of "least privilege". I historically have had to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

install computers with "local administrative" privileges in order to have legacy computer applications function properly in my firm. I am no longer willing to continue to operate in this manner.

Additional analysis of current security practices

Workstations in my network are connected to a Windows 2000 server that currently is using as its means of protection, several layers of firewall protection. The first is a Microsoft product called Internet Acceleration and Security Server [ISA Server]. This has been set up without egress filtering to allow certain legacy applications to connect to the Internet for updates following directions outlined in a Microsoft Knowledge base article allowing third party access[x]. A second layer of protection is provided by a Netopia router using Network address translation with firewall capabilities. I have purposely outsourced the web site to a third party web hosting service. Both the Netopia firewall and the ISA server have specific rules in place to block access to inbound port 80 and 443, thereby reducing a potential vulnerability in the network. A scan of open network ports indicates a very closed network, with very few ports registering as open. Furthermore, I have not allowed any wireless access to be set up on the network. Currently only I and another person use remote connectivity on nonstandard ports and these logins and logouts are monitored.

The outward facing Network server has two network cards with only tcp/ip protocol enabled on the external network card. **File and Printer Sharing** and **Client for Microsoft Networks** are disabled and thus ensuring that NetBIOS attacks and/or spam using the internal Microsoft messaging service cannot enter the network.

There are two modems in my network; one is located within my workstation to allow for legacy connectivity with my clients that still use a modem. This modem has been set to allow no dial in access. The second modem is connected to a server and that is currently turned off as it is no longer used for remote dial in. All prior connectivity to that modem has been disabled to ensure that it cannot be used for access.

All computers in the network have **NTFS** file systems in use. The **Encrypting File System** has not been regularly used; however recent legislative actions applicable to businesses with computerized data that is defined as private, dictate that I will be evaluating the use of encryption for private client data on a more regular and extensive basis. Each workstation has the boxes "hide file extensions for known file types" and "show hidden files and folders" adjusted to ensure that files with "double file extensions" are seen.

It is the policy of my firm to send any confidential, private emails using encrypted email. Furthermore, any word documents or excel documents are first converted to Adobe PDF format to ensure that they cannot be changed after transmission.

Review of current employee manual

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As a result of my SANS training, steps are being taken to review the employee manual in place at my firm. Increased emphasis on ensuring the privacy and protection of client data will be incorporated in the manual. As it now exists, the manual makes no mention of password policy, remote access, or requiring that employees maintain antivirus and firewalls on home computer systems.

Recent legislative actions and revised risk analysis

In September of 2002, the State of California passed a law [Senate Bill 1386][xi] requiring that

> "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

This law goes into effect in June of 2003. Data contained in several applications on the server include Names and Social Security numbers which are defined as personal information by the State of California. The data is not encrypted by these applications, thus any unauthorized breach of my network would have to be disclosed to clients of the firm. Given the level of trust and confidence emphasized by the CPA profession, I have determined that a revised risk analysis needs to be performed with this legislative information in mind.

Analysis of risk categories and factors

My firm is highly dependent upon information assets. On a daily basis, computers are used to calculate and accumulate financial data for our clients. These assets include server hardware, Windows 2000 based server software, workstations running Windows XP, Hewlett Packard printers, cabling, etc. While paper documentation of transactions are generated, the costs that would be incurred to recover the data would seriously inhibit the firm's ability to generate net operational cash flows, thus the need to maintain integrity of the data is of utmost priority.

Assigning value to the assets

The costs to replace the hard assets [computers, printers, and other technology infrastructure including wiring] would not be of a material amount to the firm when compared to the impact on the credibility and confidence in the firm if we were required to notify clients of an inadvertent computer breach. My perception is that the value of the firm's reputation, given our stature in the community, would be likened to the calculated value of a business. Using typical business valuation methodology, this amount would be in the range of one to one and one-half times annual revenues of the firm. My firm has a reputation of being a technology leader and therefore, I as well as

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

others in my firm, feel that any such notification to its clients, as a result of a computer breach, which includes business professionals is simply not acceptable.

Physical damage and malfunctions

My firm's current focus is to emphasize risks due to damage and/or losses. The servers are configured with a hardware raid 5 configuration with SCSI drives. I consider this configuration as a "server best practice", no matter how small or how large a network is. Particular attention has been given to ensuring data can be accessed at all times. My firm performs a full nightly backup of the entire server drive including system state. Using a third party backup product, Ultrabac©, a report is emailed to me at my workstation, and the backup report is reviewed for success or failure. Once a week a tape is taken offsite with the prior backup brought back to the firm. An additional "data only" backup is performed using "robocopy" a Windows NT© utility and nightly files that have changed are copied using this utility to a workstation that is set to automatically perform this task at 4:00 a.m. Again, I review the report of this action to ensure it's success.

ERD disks are kept in a fireproof safe and are updated after changes to the system. Each workstation and server has, attached to it, an uninterruptible power supply ensuring that data loss is kept to a minimum. I am in the process of identifying machines at possible risk to vandalism and theft. Currently I lock up all movable computers [laptops] and I am in the process of physically securing those desktop computers in more open areas with Kensington© locks attached to the Flat screens and computers. The server is physically secured to the wall in a separate room and has a locked floppy drive. Given the unique nature of my business, I feel that the cost of these physical locks [approximately $29.95 US each] is certainly not cost prohibitive to be attached to all computers compared to security breaches and lost productivity that would result if the machines were stolen. Locks for each workstation have been ordered and will be installed upon receipt.

The building has an alarm and full sprinkler system. All backup tapes are kept in a locked, fire resistant, water resistant safe. Backup tapes are taken offsite to my home. The current tape rotation system is to take each Friday's tape offsite. The previous Friday's tape is then brought back to the office for reuse. Tapes are generally replaced with new tapes once a year.

All laptops are equipped with firewalls and antivirus software, and all attached workstations are protected with a real-time desktop antivirus that is updated on a regular basis by the server. End users are prohibited from turning off any antivirus by

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the use of an administration password that is only known to me and the backup network administrator.

Attacks

I have a practice of using a program from Shavlik©, Hfnetckpro[xii] to scan each workstation for missing and needed patches. If patches are required, I make it a policy to update the workstations each Friday at lunchtime. While many security authors recommend a schedule whereby patches are installed near the middle of the week, due to the fact that my workstations are all relatively new operating systems [all Windows XP on service pack one], and due to the user workloads, I prefer to apply the patches on Friday. The server[s] are also scanned at the same time and patches are applied after hours also on Friday. The servers are up to date on security patches. [Windows 2000 service pack 3, Exchange service pack 3, Internet Acceleration and Security service pack 1]. All workstations are running Windows XP with service pack 1, and Office XP [with Outlook XP] on service pack 2.

It is a monthly practice of mine to ensure that the condition of open and closed ports on the server has not changed as a result of security patches or other maintenance during the month. Thus Foundstone's Superscan tool[xiii] is used on a regular basis to ensure that nothing has changed on the external connections to the network.

The firm has a low employee turnover, but employees who have left have their accounts disabled but maintained on the system for six months. SNMP services are not used inside the Network and all network attached HP printers have the community name of "Public" removed from their SNMP settings.

Estimation of potential loss from the risk or threat

While my level of security patches has the workstations "patched" as best as they can be at this time, given the potential loss of trust of clients should an unauthorized breach occur, I am certain that continuing the practice of "Local Administrator" to support older applications is no longer acceptable. I have built at home, a test server, set up in the same manner as my firm [Local Administrator rights on the workstation] and recently had an incident whereby I inadvertently installed "Gator"[xiv] on my workstation without the realization of its install. My intention is to restrict the use of "Local Administrator" on all network workstations and to no longer operate in this manner.

Estimate the possible frequency of the threat occurring

On a regular basis, viruses, worms and other malware are released on the Internet. While my firm utilizes a server based antivirus that checks every hour on the hour for updates, scans email entering the system, scans the server, and provides real time file monitoring on each workstation, the potential for loss still exists. I currently subscribe to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

newsletters on the potentials for loss to ensure that I am aware of the issues. In order to stay informed, I subscribe to the following:

- Security bulletins from Microsoft.com [http://www.microsoft.com/security][xv]
- NT Bugtraq newsletters [http://www.ntbugtraq.com/]
- Daily news updates in the IT industry [Russ Levine's Newsbits http://www.newsbits.net]
- Virus information from Trend [http://www.antivirus.com]
- SANS weekly newsletters [http://server2.sans.org/sansnews]
- Review of port trends by reviewing the top ten ports as identified by the Internet Storm Center [http://isc.incidents.org/]

Employees of the firm are made aware of these risks during regular staff.

Calculation of the cost of the risk

As a result of my SANS training, I am even more convinced that my current practice of using a setting of "Local Administrator" and not using egress filtering on my firewall are extremely risky and potentially too costly for my firm to absorb should a breach occur. More importantly, these practices are not acceptable to me given the change in industry regulations. I also feel that the risks and "costs" of my settings include some potential to damage the reputation of the firm.

The value of the fixed assets is approximately $300,000. For these assets, the current exposure factor given current practices is computed as 1.00 given that all of the firm's computers share data with a centralized server. Thus if one machine is affected, it could spread quickly to the entire network. The threat of viruses and malware and possible Trojan horses being installed in the system is closer to an annualized rate of occurrence of 1.0, given the due diligence of the network administrator [me] and judicious use of security patches, antivirus, and employee awareness, in my case an exposure factor value of .25 was set. Thus the Annualized loss expectancy is calculated at $75,000. I determined that countermeasures and activities herein described in this paper could easily be recommended and implemented to mitigate the potential risks.

DURING PROCEDURES

Review of sources of documents regarding Windows XP Security

While Windows XP is a relatively new platform, there are various sources of credible literature containing guidance as to how to better secure the Windows XP platform. The National Security Agency [NSA] has recently released a document that contains a security template [WinXP_workstation.inf file] as well as a document discussing recommended security settings. [xvi] As per NSA recommendations, I have "clean

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

installed" all Windows XP workstations and have not "upgrade installed". In addition, all workstations are NTFS formatted. The latest service packs have been installed on the system and monitored on a weekly basis.

As noted in the NSA documentation, Windows XP includes additional security features not found in Windows 2000 and have been noted:[xvii]

- Everyone Group Membership does not include anonymous user (null connection)
- Only the administrative user that creates an object becomes the sole owner of the object
- Power users and Administrators groups are the only users able to install local printers
- Local accounts that do not have passwords can only be used to log in locally and cannot log in across the domain [network]

Recommended changes and testing

Upon reviewing the recommended guidelines I have made the following changes to the settings to the test XP workstation at my home.[xviii] The settings were also compared to recommendations from the Microsoft Baseline Security Advisor tool.[xix] [Details of the recommendations from the Microsoft Baseline Security Advisor tool have been included in Appendix A] At this time the Center for Internet Security[xx] has not yet released their own version of their baseline tool for Windows XP workstations. Therefore testing on my home test Windows XP workstation was done using the MBSA tool. With the exception of the item mentioned in step 4, all items have been tested on my home Windows XP workstation and have been applied to all of the workstations at my office.

1. As recommended by the NSA guidelines, I renamed the Administrator account but retained the settings. The User "Administrator" was changed and the description of the Administrator account was removed. This is recommended for "security through obscurity".
2. I reviewed the settings and ensured that the Guest account was disabled. [Upon reviewing the settings, the guest account had previously been disabled by the operating system].
3. As recommended I changed the password policies. While Group policy settings can be adjusted for passwords, upon my review, I determined that the best course of action would be to statically assign complex passwords every 90 days. (In applying this recommendation at my firm, I felt that due to the relatively new use of this security recommendation being made as well as the various ages and computer literacy of the users, this policy provides the necessary security yet still allows Administrative control over the setting of the passwords.
4. I use Shavlik HfnetckPro tool for patch deployment throughout my firm's network. I have contacted Shavlik to update to this or another product that will provide

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Office suite scanning as well as Operating system scanning.[xxi] (This product is currently only running on my network system at the office due to the fact that I am only licensed for its use at my firm and to purchase a version for home testing would be cost prohibitive.)

5. As suggested, the Group Policy security template of the local policies section was adjusted to enable auditing on each workstation. [Please see appendix B, Figure 1] The following recommended changes were made:
    a. *Audit account logon events* was changed to audit *success, failure*
    b. *Audit account management* was changed to audit *success, failure*
    c. *Audit directory service access* was changed to audit *failure*
    d. *Audit logon events* was changed to audit *success, failure*
    e. *Audit object access* was changed to audit *failure*
    f. *Audit policy change* was changed to audit *success, failure*
    g. *Audit system events* was changed to audit *success, failure*
6. The following user rights were adjusted and reviewed under the Local Security Settings on my test system[xxii]:
    a. *Access this computer from network* was edited to only allow "Administrators and Users". I felt that only these two groups needed this access. [Please note I followed the guidelines from the National Security Agency's Guide to Securing Windows XP rather than SANS's Securing Windows 2000 step by step guide as I felt it provided better guidance for my Windows XP workstations.]
    b. *Act as part of the operating system* needed no adjustment as it was already set for no rights being held by any group.
    c. *Add workstations to domain* needed no adjustment as it again was already set for no rights being held by any group. This right is only needed on a domain controller and not on a workstation.
    d. *Adjust memory quotas for a process* needed no adjustment as it had previously been set for "Administrators, Network service and Local service". This setting is used for computer processing to allow processes to have quotas.
    e. *Allow logon through Terminal Services* was not changed from the default of "Administrators and Remote Desktop Users". Remote connectivity is being monitored on my test site as well as my firm, as previously discussed, and the business risk is deemed appropriate. This function is needed in order to have access as a Terminal Services client to allow for internal help desk functionality.
    f. *Backup files and directories* was not changed from the default of "Administrators and Backup File Operators". This function allows a user to backup computer files and directories.
    g. *Bypass traverse checking* was adjusted to include only Administrators. This prevents inheritance of permissions.
    h. *Change the system time* was adjusted to only include "Administrators". The category of "Power users" was removed. System clock settings are

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

critical to auditing a system and should only be adjusted by Administrators.

i. *Create a pagefile* was not changed from the default setting of "Administrator". This allows a user to change and create pagefiles.
j. *Create a token object* was not changed from the default setting of no rights being held by any group. This function allows the creation of a token and it is recommended that this right never be given to any user.
k. *Create permanent shared objects* was not changed from the default setting of no rights being held by any group. This restricts the ability to create permanent objects such as \\Device.
l. *Debug programs* was not changed from the default setting of Administrator. It was my feeling that it was not necessary to change this access to "no one"
m. *Deny access to this computer from the network* was not changed from the default settings of Guest and Support_388945a0. Both of these accounts are disabled inside the system. The Support_388945a0 account is a vendor's account for the Help and Support Service and when used generates a random password.
n. *Deny logon as a batch job* was not changed from the default setting of no rights being held by any group.
o. *Deny logon as a service* was not changed from the default setting of no rights being held by any group.
p. *Deny logon locally* was not changed from the default settings of Guest and Support_388945a0.
q. *Deny logon through Terminal Services* was not changed from the default setting of no rights being held by any group. Since remote connectivity has been deemed to be an acceptable business risk, this was not denied.
r. *Enable computer and user accounts to be trusted for delegation* was not changed from the default setting of no rights being held by any group.
s. *Force shutdown from a remote system* was not changed from the default setting of Administrators. Since the Shavlik Hfnetchk program is being used at my office to remotely push patches to the workstations, this setting is appropriate.
t. *Generate security audits* was not changed from the default setting of Local Service and Network Service to ensure security audit log entries are prepared by the system.
u. *Increase scheduling priority* was not changed from the default setting of Administrators. This allows a user to boost the priority of a process.
v. *Load and unload device drivers* was not changed from the default setting of Administrators. This is needed for plug and play devices.
w. *Lock pages in memory* was not changed from the default setting of no rights being held by any group. This allows a user to lock pages in physical memory.
x. *Log on as a batch job* was not changed from the default setting of Support_388945a0.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

y. *Log on as a service* was not changed from its default of Network service.
z. *Log on locally* was not changed from the installed Administrators, users, _vmware_ [VMware is installed on my test workstation in order to run Linux], and Power users.
aa. *Manage auditing and security log* was not changed from the default setting of Administrators. This limits the ability of users to view and clear the security log.
bb. *Modify fimware environment variables* was not changed from the default setting of Administrators. This allows a user to modify system variables stored in RAM on systems.
cc. *Perform volume maintenance* tasks was not changed from the default setting of Administrators. This allows a user to run maintenance tasks such as Diskcleanup and Disk defragmenter.
dd. *Profile single process* was not changed from the default setting of Administrators and Power Users. This allows a user to perform profiling on a process.
ee. *Profile system performance* was not changed from the default setting of Administrators.
ff. *Remove computer from docking station* was not changed from the default setting of Administrators, Users and Power Users. This is needed for laptop users to undock their systems from a docking station.
gg. *Replace a process-level token* was not changed from the default setting of Local Service and Network Service. This allows a user to modify a security access token used by a process.
hh. *Restore files and directories* was not changed from the default setting of Administrators and Backup Operators. This allows a user to restore files and directories.
ii. *Shut down the system* was not changed from the default setting of Administrators, Users, Power Users, and Backup Operators.
jj. *Synchronize directory service data* was not changed from the default setting of no rights being held by any group. This is also known as Active Directory Synchronization.
kk. *Take ownership of files or other objects* was not changed from the default setting of Administrators.

All of these steps were taken to ensure that only those users that were identified by me as the best for each setting had rights accordingly.

7. The Telnet service was disabled. Even though the service was set to manual, I determined that there was no need for this service to be running inside the network.
8. In Word 2002, Macro security was reset to Medium [Click on tools, macros, then on security, click on medium or high]. Since my firm uses some firm customized programs that have Visual basic scripting, I determined that I would need to set the security setting on “medium”. This setting allows the end user to “choose”

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

whether a macro can be run. (I will need to provide additional end user training and documentation as part of my firm's implementation in order to make end users aware of the implications of this setting.)

9. In Internet Explorer, the security settings were reviewed. I determined that the default recommended settings were sufficient to meet the requirements of my firm. Again, additional end user training and documentation will be incorporated into my firm implementation in order to make end users aware of the changes. The following settings were tested in my home test network and were fully acceptable:
    a. Local Intranet was set at "medium-low"
    b. Trusted sites was set at "low"
    c. Internet was set at "medium"
    d. Restricted sites was set to "high"
10. My current practice is to proactively block ports that are identified by the web site Incidents.org[xxiii] unless they are needed by the firm. Due to the use of non standard ports, the use of two firewalls and network address translation, performing a port scan shows 22 typical ports as being in "stealth mode" [see Appendix B, Figure 8 and 9]

All of these changes were made to my test workstation and to my network computers to allow me to set a "benchmark" or a "standard" security level for all computers in my network. Ensuring that each attached workstation is set at uniform standardized levels allows me to better monitor the risk levels of my network.

Use of Registry key changes

Using "Standard or Power User" settings, Quickbooks 2002 was able to function appropriately. However, for older versions of Quickbooks [in this case Quickbooks 99 was tested], even the "Power User" setting did not allow the program to function properly. It required the "Local Administrator" setting to be in place. Since this version of the program will no longer receive payroll tax updates in 2003 and therefore, is being phased out by the vendor, I determined that leaving this program in a non-functional state was acceptable. For those users in my office that might need access to such legacy programs or are deemed to need additional security levels beyond that of Power User [the normal user account which disallows the ability to install programs], the ability to add granularity using registry keys was considered. Examining the CVE web site[xxiv] for vulnerabilities specifically targeting Quickbooks users, I found no such explicit vulnerabilities for Quickbooks in the listings. Thus in cases where the "Power User setting" was deemed to be insecure on certain workstations, or where users required "legacy access"; I felt that the best balance between functionality and security was met using the following procedures to allow the installation and updating of Quickbooks. When deemed necessary, in the registry, where Quickbooks is loaded, under "Hkey", "Local Machine", "Software", under the key for "Intuit", on all versions of Quickbooks loaded, right mouse click on the version, click on permissions and adjust permissions to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

allow "Full Control" and select the user name. The Regini[xxv] tool can be used to also give this permission by using a value of "7".

Currently I have only used this specific registry permission on a few closely monitored workstations. A few workstations have CDRW drives to allow for large file transfers which are necessary for business reasons. These workstations required that the CDRW burning program's registry be adjusted to allow for full access. At this time, all workstations have been left at "Power level" permission level. At this time, given the nature of my firm and its needs, this level of permission provides the proper balance of business requirements with security requirements

Adjusting Firewalls for Egress filtering and notification

I reviewed my current practice of allowing all traffic out the firewall and deemed that it was inappropriate for continued practice. As a result of the recommendations from SANS and other security organizations to ensure that egress filtering is in place I immediately adjusted the firewall settings accordingly. Both my network at the office and my test network at home currently have two products that provide firewall protection. The most outward facing device is attached directly to the telephone company's connection and is assigned a static IP address. This device is attached to one of two Network cards in the server that contains the ISA server. This device provides firewall type features through its use of Network address translation. This device cannot be set for egress filtering. The attached ISA server which provides internet connectivity however, does have egress filtering capabilities. It has been set up to allow for third party access to Internet applications through ISA server.[xxvi] The following steps were taken to adjust the ISA server to continue to allow for legacy applications such as Quickbooks 2002 to have access to the Internet, but not so as to allow potential Trojan programs the same abilities.

The adjustments to the ISA server included the following:

1. The rule to allow any workstation access to the Internet was deleted and a new ISA rule was created to apply only to Authorized network users.
2. The check box to ask unauthenticated users for identification was re-enabled. [See Appendix B, Figure 6]

Furthermore, intrusion notifications for ports were activated on the ISA server. While the Netopia firewall is already set to block inbound traffic from port 80 and 443, ensuring that the ISA server was re-tuned for egress filtering will greatly increase the security of the network. The external hardware [Netopia] firewall/router's settings were reviewed to see if it allowed transmission of logging as well. I am aware of the concept of log submission to dshield.org[xxvii] and will be replacing the existing external router/firewall with a model that provides the ability to email the logs to the dshield.org web site.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The impact of all of these settings was reviewed. While a few legacy applications failed to work properly after resetting the firewall settings, I determined that the applications were rarely used and could be phased out. I felt that the increased security was of greater benefit than the rare use of the applications that required "unauthenticated" access to the firewall. Alternative programs are already in place and thus the change is more of an end user education process rather than a business need issue.

As a result of my SANS education, I plan to monitor the logs of each device more proactively than had been previously done. In addition, I will be purchasing a Composition notebook [stitched and bound] in order to maintain a formal log of the network condition and success of backups rather than simply relying on the email notifications. In addition, I will be more proactive in documenting that the steps I take on a daily basis to ensure the good working condition of the network.

Changes to Employee Manual

My firm's employee manual is in the process of being revised to include new policies for passwords, email, antivirus, and remote access. The revisions to the policy manual are included in Appendix C. It is now a requirement of all employees who work on firm computer files on their home computers to obtain antivirus software and firewall software. Selected sections of the Security policies[xxviii] of the SANS Institute are being incorporated into the employee manual. Special emphasis on ensuring that data is kept secure while the data is on the network as well as on laptops out in the field will ensure that risk is mitigated in all environments where the accountants perform their work.

AFTER PROCEDURES

Additional remedial recommended procedures

On the test network, after adjusting the local user permissions, adjusting the security policy for auditing, and resetting the security settings as recommended, the MSBA tool was run once again. This time the sample workstation tested with significantly less risk factors than before.

The outward facing internet connections were scanned for vulnerabilities. I felt that the current level of user permissions, egress filtering and settings for notifications was sufficient at this time and provided a good balance between security and business functionality.

I have now made these recommended changes to the server system at my office. After performing these changes, I was pleasantly surprised that normal business processes were not harmed or modified in a discernable manner. Since I have ensured that all "active" business applications are under annual maintenance agreements, very few applications failed or refused to work. The few that did not work under these restrictions were all deemed to be no longer supported by their vendors, or not worth the business

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

risk. I was pleasantly surprised that all of these actions caused no major hardship in the working and interoperability of my firm's computers and yet my risk was lessened.

All future applications will continue to be evaluated in this manner to see if permissions levels can be lowered even further in the future. Vendors will be contacted to determine their plans for programming in a more secure manner. As the updated applications are identified that can be installed in a more native secure method, these too will be evaluated.

I will maintain my current practice of pro-active patching, up to date anti-virus, as well as employee education. In addition to the weekly scans for patches, I plan to add a regular review of security procedures to ensure compliance with my industry and with the "best recommended practices" as recommended in the computer industry. I will be purchasing additional tapes to allow a full week's worth of backups to be taken offsite and rotated for reuse.

The training afforded me by the SANS Institute provided me with the much needed integration of my accumulated knowledge to assist me in finding the proper balance between security and business functionality. In addition, my application of "**defense in depth**" was increased during the course of this case study.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

[i] The accounting program designed by Intuit Incorporated, called Quickbooks is just one example of a program that has been redesigned over time. Currently my firm supports several versions of this same program that is typically updated on an annual basis. Older versions of this software were designed and built when only Windows 98 and 95 operating systems were in use. This is just one example on this particular workstation, legacy applications may also require netbios over TCP/IP to continue to be enabled. To ensure that netbios is restricted for internal purposes, I mandate that ports 135-139 are blocked at the server and Internet gateway. Ensuring that only tcp/ip is bound to the outward facing Network card and specific rules are set for blocking traffic is key to a properly firewalled server. Outward facing network ports should be scanned for traffic using tools available at the web site Foundstone.com [Superscan], or other such tools.

[ii] Intuit, Unknown author, "Warning: Quickbooks could not locate a valid Installation Key Code, Knowledgebase article 125249", URL: http://www.quickbooks.com/support/faqs/qbw2000/125249.html

[iii] Intuit, Unknown author, "Warning: Quickbooks could not locate a valid Installation Key Code, Knowledgebase article 125249", URL: http://www.quickbooks.com/support/faqs/qbw2000/125249.html

[iv] Microsoft Corporation, Unknown author, "Check for Correct User Privileges", URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/apcompat/apcompat/check_for_correct_user_privileges.asp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[v] Microsoft Corporation, Unknown author, "Check for Correct User Privileges", URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/apcompat/apcompat/check_for_correct_user_privileges.asp

[vi] SANS Institute, Various authors, The Top 10 Windows Vulnerabilities, SANS Institute handout, December 2002, SANS Conference, Copyright 2002, vulnerability number 4

[vii] Carnegie Mellon Software Engineering Institute, "CERT® Advisory CA-2001-22 W32/Sircam Malicious Code", July 25, 2001 URL: http://www.cert.org/advisories/CA-2001-22.html

[viii] Carnegie Mellon Software Engineering Institute, "CERT® Advisory CA-2001-26 Nimda Worm", September 18, 2001, URL: http://www.cert.org/advisories/CA-2001-26.html

[ix] SANS Institute, Various authors, The Top 10 Windows Vulnerabilities, SANS Institute handout, December 2002, SANS Conference, Copyright 2002, vulnerability number 9

[x] Microsoft Knowledge base "How to Allow Third-Party Internet Application Connections Through ISA Server 2000" 8/6/2002, URL: http://support.microsoft.com/?kbid=295667

[xi] State of California, Senate Bill 1386, "An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information." September 26, 2002 URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[xii] Shavlik Corporation provides a free version of it's Hfnetchklt for firms as well as sells the Enterprise version called HfnetchkPro, 2002, URL: http://www.shavlik.com

[xiii] Foundstone, "Superscan tool" URL: http://www.foundstone.com/knowledge/free_tools.html

[xiv] "Gator" is an Internet Explorer add-on that tracks your Internet surfing and "leaks" data to sponsoring organizations. 2002 URL: [http://www.gator.com/]

[xv] Microsoft TechNet Security – "Product Security Notification:" URL: http://www.microsoft.com/technet/security/bulletin/notify.asp?frame=true

[xvi] Bickel, R. , M. Cook, J. Haney, M. Kerr DISA, CT01 T. Parker, USN, H. Parkes, National Security Agency, "Guide to Securing Microsoft Windows XP®", October 30, 2002, URL: http://nsa2.www.conxion.com/winxp/download.htm#Zipped%20Archive

[xvii] Bickel, R. , M. Cook, J. Haney, M. Kerr DISA, CT01 T. Parker, USN, H. Parkes, National Security Agency, "Guide to Securing Microsoft Windows XP®", October 30, 2002, URL: http://nsa2.www.conxion.com/winxp/download.htm#Zipped%20Archive , Page 7

[xviii] Please note all settings were done on a test network by me. As a result of the testing, I have applied the settings now to the actual network.

[xix] Microsoft Corporation, Unknown author, "Microsoft Baseline Security Advisor", 2002, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP

[xx] Center for Internet Security, "CIS Benchmarks and Scoring Tool for Windows 2000 and Windows NT", 2002, URL: http://www.cisecurity.org/bench_win2000.html Currently the Center for Internet Security

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

has tools for Windows 2000 server and workstation and Windows NT. A sample of increased security case study as a result of the tools provided by the Center for Internet Security Benchmarks can be found at this site URL: http://www.cisecurity.org/HunTelCSv6.pdf

[xxi] St. Bernard's Software's UpdateExpert also provides this ability. It is recommended in an Enterprise setting to use Microsoft's Software Update Service or other third party tools to monitor the security issues on systems. URL: http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

[xxii] Many of the descriptions are taken directly from the SANS Institute, SANS Securing Windows 2000 Step by Step guide, Version 1.5, SANS Institute, July 2001 and Bickel, R. , M. Cook, J. Haney, M. Kerr DISA, CT01 T. Parker, USN, H. Parkes, National Security Agency, "Guide to Securing Microsoft Windows XP®", October 30, 2002, URL: http://nsa2.www.conxion.com/winxp/download.htm#Zipped%20Archive

[xxiii] Internet Storm Center "Internet Storm Center Infocom", URL: http://isc.incidents.org/

[xxiv] Mitre Corporation, "Common Vulnerabilities and Exposures", 2002, URL: http://www.cve.mitre.org

[xxv] Microsoft Knowledgebase 237607 - How to Use Regini.exe to Set Permissions on Registry Keys: http://support.microsoft.com/default.aspx?scid=KB;en-us;q237607

[xxvi] Microsoft Knowledge base "How to Allow Third-Party Internet Application Connections Through ISA Server 2000" 8/6/2002, URL: http://support.microsoft.com/?kbid=295667

[xxvii] DShield "DShield - How to submit your firewall logs to DShield", URL: http://www.dshield.org/howto.html

[xxviii] SANS Institute, Michele Crabb-Guel , "Model Security Policies" URL: http://www.sans.org/newlook/resources/policies/policies.htm Portions of the Model Security Policies provided by the SANS Institute have been incorporated verbatim in the revised employee manual.

BIBLIOGRAPHY

Bickel, R. , M. Cook, J. Haney, M. Kerr DISA, CT01 T. Parker, USN, H. Parkes, National Security Agency, "Guide to Securing Microsoft Windows XP®", October 30, 2002, URL: http://nsa2.www.conxion.com/winxp/download.htm#Zipped%20Archive

Bragg, Roberta, CISSP, CISSP Certified Information Systems Security Professional, Que Publishing, 2003

Carnegie Mellon Software Engineering Institute, "CERT® Advisory CA-2001-22 W32/Sircam Malicious Code", July 25, 2001 URL: http://www.cert.org/advisories/CA-2001-22.html

Carnegie Mellon Software Engineering Institute, "CERT® Advisory CA-2001-26 Nimda Worm", September 18, 2001, URL: http://www.cert.org/advisories/CA-2001-26.html

Center for Internet Security, "CIS Benchmarks and Scoring Tool for Windows 2000 and Windows NT", 2002, URL: http://www.cisecurity.org/bench_win2000.html

Intuit, Unknown author, "Warning: Quickbooks could not locate a valid Installation Key Code, Knowledgebase article 125249", URL: http://www.quickbooks.com/support/faqs/qbw2000/125249.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Microsoft Corporation, Unknown author, "Check for Correct User Privileges", URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/apcompat/apcompat/check_for_correct_user_privileges.asp

Microsoft Knowledge base "How to Allow Third-Party Internet Application Connections Through ISA Server 2000" 8/6/2002, URL: http://support.microsoft.com/?kbid=295667

Microsoft Corporation, Unknown author, "Microsoft Baseline Security Advisor", 2002, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP

Mitre Corporation, "Common Vulnerabilities and Exposures", 2002, URL: http://www.cve.mitre.org

SANS Institute, Various authors, The Top 10 Windows Vulnerabilities, SANS Institute handout, December 2002, SANS Conference, Copyright 2002

SANS Institute, SANS Securing Windows 2000 Step-by-Step Guide, Version 1.5, SANS Institute, July 2001

SANS Institute, Michele Crabb-Guel , "Model Security Policies" URL: http://www.sans.org/newlook/resources/policies/policies.htm

State of California, Senate Bill 1386, "An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information." September 26, 2002 URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Security Administrator online "Security Templates Define and Enforce the Rules: " January 2002, URL: http://www.secadministrator.com/Articles/Index.cfm?ArticleID=23375&pg=1

Security Metrics, "Port Scan", 2002 URL: Figure 7: Graphic of Condition of outside ports as scanned by Security Metrics https://www.securitymetrics.com/portscan.adp

Appendix A

Graphical views of Microsoft Baseline Security Advisor prior to corrective actions on a Testing platform:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Update Scan Results

Score	Issue	Result
✗	Windows Security Updates	3 security updates are out of date or could not be confirmed. What was scanned Result details How to correct this
✓	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
	IIS Security Updates	IIS is not running on this computer.
	SQL Server Security Updates	SQL Server is not installed on this computer.
	Exchange Server Security Updates	Exchange Server is not installed.

Figure 1 – Graphics taken from the Microsoft Baseline Security Analyzer - scan indicating 3 Security updates out of date or could not be confirmed.

Security updates that are out of date are marked with a yellow X

Score	Security Update	Description	Reason
✗	MS02-055	Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255)	File C:\WINDOWS\system32\hhctrl.ocx has a file version [5.2.3718.0] that is greater than what is expected [5.2.3669.0].
✗	MS02-068	Cumulative Patch for Internet Explorer (324929)	File C:\WINDOWS\system32\urlmon.dll has a file version [6.0.2800.1143] that is greater than what is expected [6.0.2800.1126] - File C:\WINDOWS\system32\shdocvw.dll has a file version [6.0.2800.1143] that is greater than what is expected [6.0.2800.1133].

Security updates that the tool cannot confirm as installed on the scanned computer are marked with a blue asterisk

Score	Security Update	Description	Reason
*	MS02-008	XML - HTTP Control Can Allow Access to Local Files	Please refer to Q306460 for a detailed explanation.

Figure 2 – Graphics taken from the Microsoft Baseline Security Analyzer - detailed view of MSBA scan warnings. Please note that due to limitations in the MSBA, these errors are incorrect and can be safely ignored. A separate scan using Windows Update was performed and tested cleanly. Thus it is wise to perform analysis with several tools

Windows Update

- Welcome
- Pick updates to install
  - Critical Updates and Service Packs (0)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 3: Graphic taken from Microsoft Windows Update - View of Windows update indicating no needed critical updates on this workstation

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (2 of 6) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✗	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
✗	Password Expiration	Some unspecified user accounts (5 of 6) have non-expiring passwords. What was scanned Result details How to correct this
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

Figure 4 – Graphics taken from the Microsoft Baseline Security Analyzer - Indications that passwords are currently not complex enough.

Score	User	Weak Password	Locked Out	Disabled
	Guest	Weak	-	Disabled
	HelpAssistant	-	-	Disabled
	[redacted]	-	-	Disabled
✗	[redacted]	Weak	-	-
✓	[redacted]			
✓	__vmware_user__			

Figure 5 – Graphics taken from the Microsoft Baseline Security Analyzer - details of the users identified with weak passwords. The Guest Account has been disabled. [Please note, user names have been blocked for privacy purposes]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Score	Issue	Result
	Auditing	Enable auditing for specific events like logon/logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	12 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Windows 2000 or greater. What was scanned

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
	SQL Server Status	SQL Server is not installed on this computer.

Figure 6: Graphics taken from the Microsoft Baseline Security Analyzer - Indications that auditing is not properly set for this workstation. Shares are used in this home test system but not used at my firm.

Enable auditing on each Windows system on your network. After you enable auditing, you can choose which events to monitor, such as successful or failed logon attempts. In addition, certain files and directories can be audited on NTFS file systems for modifications or deletions.

To enable auditing on a computer running Windows XP or Windows 2000

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. In Control Panel, double-click **Administrative Tools**, and then click **Local Security Policy**.
3. In Local Security Settings, double-click **Local Policies**, double-click **Audit Policy**, and then click the events that you want to audit. It is recommended that you audit the following events:

   Audit account logon events (Success, Failure)
   Audit account management (Success, Failure)
   Audit directory service access (Failure)
   Audit logon events (Success, Failure)
   Audit object access (Failure)
   Audit policy change (Success, Failure)
   Audit system events (Success, Failure)

Figure 7: Graphics taken from the Microsoft Baseline Security Analyzer - Information on enabling Auditing on a system

The following list of services should only be enabled on computers that require their functionality. Services that are not required should be disabled to reduce the attack surface of the system.

Score	Service	State
	To not	Stopped

Figure 8: Graphics taken from the Microsoft Baseline Security Analyzer - Unnecessary services installed on the system.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Vulnerabilities

Score	Issue	Result
✗	Macro Security	4 Microsoft Office product(s) are installed. Some issues were found. What was scanned Result details How to correct this
✗	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
✗	Outlook Zones	Microsoft Outlook 2002: Some security issues were found. What was scanned Result details How to correct this

Figure 9: Graphics taken from the Microsoft Baseline Security Analyzer - Additional vulnerabilities with Office Suite, Internet Explorer and Outlook found on system.

Score	Issue	User	Advice
✗	Microsoft Word 2002	[redacted]	Macro security is set to low, which is not secure.
✓	Microsoft Excel 2002	All Users	No security issues were found.
✓	Microsoft Outlook 2002	All Users	No security issues were found.
✓	Microsoft PowerPoint 2002	All Users	No security issues were found.

Figure 10: Graphics taken from the Microsoft Baseline Security Analyzer - Specifically Macro Security set too low [please note, user name is blocked for privacy purposes]

Score	User	Zone	Level	Recommended Level
✗	[redacted]	Local intranet	Custom	Medium-Low
✗	[redacted]	Trusted sites	Custom	Low
✗	[redacted]	Internet	Custom	Medium
✗	[redacted]	Restricted sites	Custom	High

Figure 11: Graphics taken from the Microsoft Baseline Security Analyzer - Internet Explorer settings need to be reviewed as they are currently customized and may not meet the specific requirements of the firm. [please note, user name is blocked for privacy purposes]

Score	User	Zone	Level	Recommended Level
✗	[redacted]	Restricted	Custom	High

Figure 12: Graphics taken from the Microsoft Baseline Security Analyzer - Outlook 2002 settings need to be reviewed as they are currently customized and may not meet the specific requirements of the firm. [please note, user name is blocked for privacy purposes]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix B

Graphical views of corrective actions taken on a Testing platform:

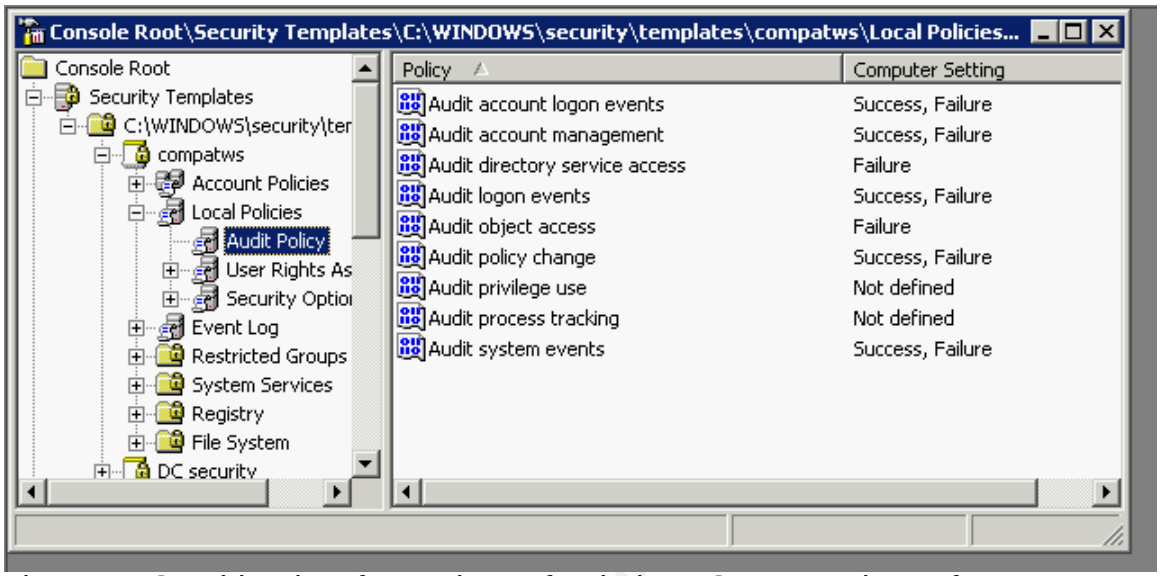

Figure 1: Graphic taken from Microsoft Windows Server – Microsoft Management Console - Adjusting Group policy setting on the Domain controller server. Click on Start, MMC, click on "File", "Add/Remove snap-in", Add the Security templates. Ensure that any adjustments are running in a test environment before applying these changes in an actual network environment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Policy	Security Setting
Access this computer from the network	Users,Administrators
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow logon through Terminal Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Administrators
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	SUPPORT_388945a0,Guest
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	SUPPORT_388945a0,Guest
Deny logon through Terminal Services	
Enable computer and user accounts to be trus...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	SUPPORT_388945a0
Log on as a service	NETWORK SERVICE
Log on locally	__vmware__,Guest,Administrators,Users,Power Users,Backup Operators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators,Power Users
Profile system performance	Administrators
Remove computer from docking station	Administrators,Users,Power Users
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE
Restore files and directories	Administrators,Backup Operators
Shut down the system	Administrators,Users,Power Users,Backup Operators
Synchronize directory service data	

Figure 2: Graphic from Local user policy after adjusting settings

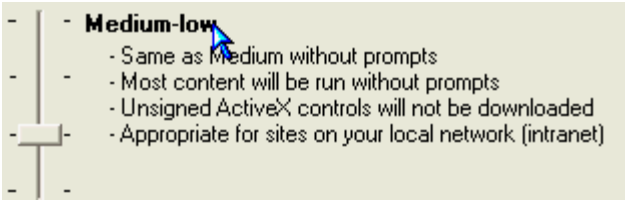

Figure 3: Graphic taken from Microsoft Internet Explorer version 6 - Internet Explorer Security Settings - Local intranet recommended to be set to “medium-low”

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

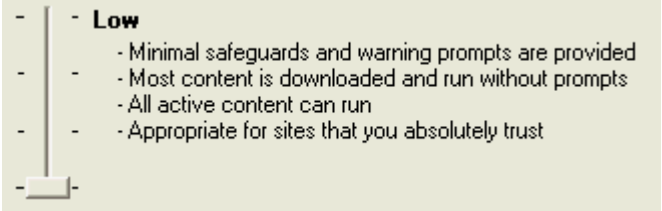

Figure 4: Graphic taken from Microsoft Internet Explorer version 6 - Internet Explorer Security Settings - Trusted sites recommended to be set to "low"

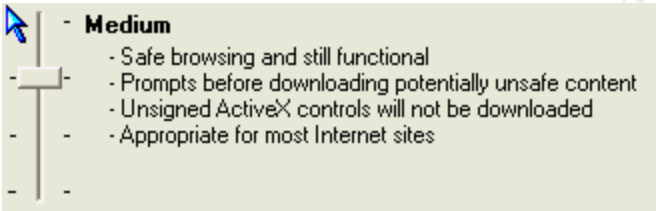

Figure 5 Graphic taken from Microsoft Internet Explorer version 6 - Internet Explorer Security Settings - Internet settings recommended to be set to "medium"

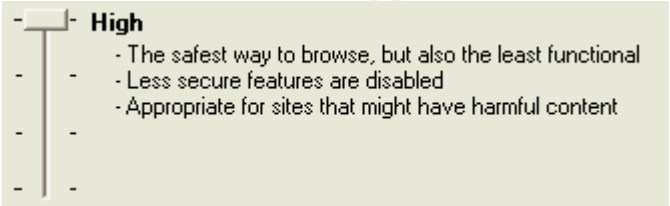

Figure 6: Graphic taken from Microsoft Internet Explorer version 6 - Internet Explorer Security Settings – Restricted Sites recommended to be set to "high"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

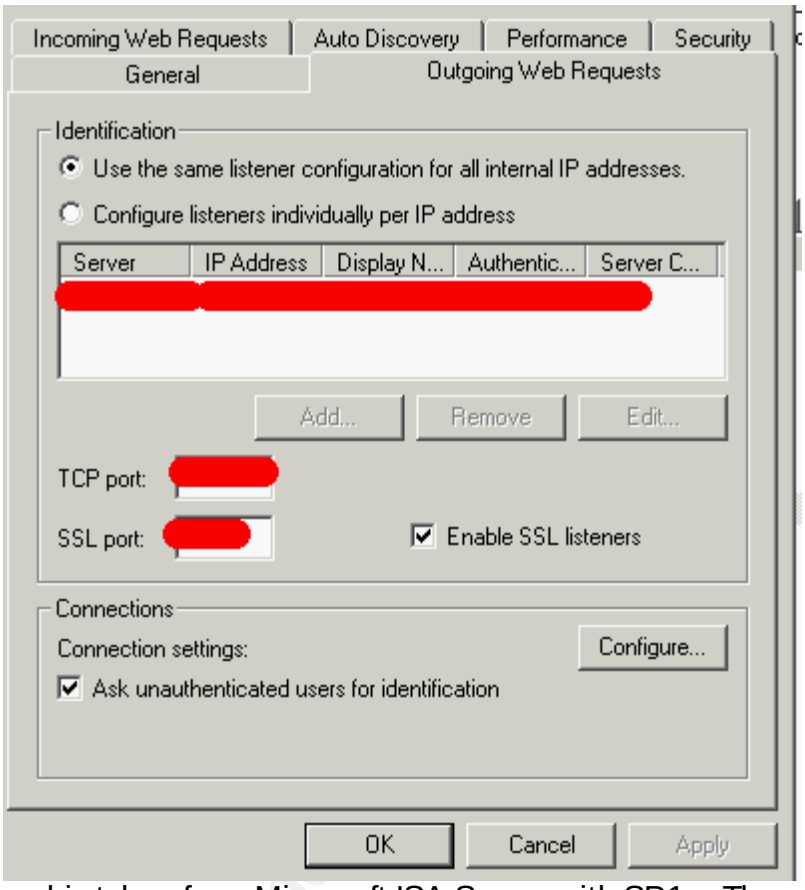

Figure 7: Graphic taken from Microsoft ISA Server with SP1 - The setting to ask unauthenticated users for identification was rechecked. [Server name blocked for privacy purposes]

© SANS Institute

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Program	Port	Status	Explanation
FTP	21	Stealth	File Transfer Protocol (FTP) allows users to transfer files to other computers over the Internet. A poorly configured FTP server allows hackers to copy your files, install trojan applications on your computer or obtain unauthorized remote command prompt access to your computer.
SSH	22	Stealth	Secure Shell (SSH) uses encryption to secure information sent over a network. While it typically improves security there are numerous problems with older versions of SSH which may allow brute force attacks.
Telnet	23	Stealth	Telnet allows a remote user to access your computer and perform commands. It is susceptible to brute force attacks and clear text password sniffing. A computer is most configured if this port is open. Use SSH instead.
SMTP	25	Stealth	SMTP is used to send email. There are numerous vulnerabilities with SMTP such as unauthorized hard disk file access, username verification or SPAM email redirection.
DNS	53	Stealth	Domain Name Services are used to tell other computers what your IP address is. There are several exploits associated with this service.
Finger	79	Stealth	Finger provides information such as usernames and usage information. Turn this service off or block this port to stop others from gaining valuable system information.
HTTP	80	Stealth	World Wide Web services allow you to publish web pages to the Internet. There are hundreds of severe security vulnerabilities associated with this service. Keep your WWW server software updated.
POP3	110	Stealth	Post Office Protocol (POP) software downloads email. Hackers may use weaknesses in POP to intercept your email, create fictitious mail accounts or gain remote access to your computer.
NetBIOS	139	Stealth	NetBIOS is used by Microsoft Windows and some UNIX/Linux programs to share files. If your hard disk is shared improperly (write access to everyone without authentication) you may be giving the world access to your hard disk. (Trojan files can be copied to your computer.) Make sure this port is closed and your hard drive shares are configured properly.
SNMP	161	Stealth	Simple Network Management Protocol (SNMP) port may allow a hacker to obtain information about your computer. There are also security vulnerabilities associated with this port. You should turn off this service if you don't need it.
SSL	443	Stealth	HTTP servers use Secure Sockets Layer (SSL) to encrypt data from web browsers. There are hundreds of severe security vulnerabilities associated with this service. Keep your WWW server software updated.
MS DS	445	Stealth	Microsoft Directory Services is used by Microsoft Networks for security authentication. Typically this port should not be exposed to the Internet.
Socks Proxy	1080	Stealth	An unsecured SOCKS Proxy may disqualify you from IRC server access. Make sure this port is closed.
KaZaA	1214	Stealth	KaZaA is a popular peer to peer file sharing program with many known vulnerabilities and at least one known worm (Benjamin) targeting it.
UPnP	5000	Stealth	Universal Plug and Play allows your computer to automatically integrate with other network devices. There are known security vulnerabilities associated with this service.
HTTP Proxy	8080	Stealth	HTTP Proxy provides a way for a hacker to pretend to be your computer. Others who may have been hacked may see your computer address and vent you to justify why you hacked them.

Figure 8: Graphic of Condition of outside ports as scanned by Security Metrics https://www.securitymetrics.com/portscan.adp

Program	Port	Status	Trojans Common to Port
Trojan	6776	Stealth	2000 Cracks, BackDoor-G, SubSeven, VP Killer
Trojan	7000	Stealth	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
Trojan	12345	Stealth	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill
Trojan	20034	Stealth	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
Trojan	27374	Stealth	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Mule, Ttfloader
Trojan	31337	Stealth	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini

Figure 9: Continuation of Graphic of Condition of outside ports as scanned by Security Metrics https://www.securitymetrics.com/portscan.adp

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX C:
REVISED SECTIONS OF THE EMPLOYEE MANUAL
WITH DIRECT IMPLICATIONS TO MY FIRM'S INFORMATION TECHNOLOGY

14. INSPECTION AND SEARCH POLICY

All furniture, equipment, computers, files, etc. on the Company's premises are the Company's property and must be maintained according to the Company's rules and regulations and should only be used for work-related purposes. The Company has implemented an inspection and search policy to protect against the unauthorized removal of Company property from its premises, to keep alcohol and illegal drugs off the premises, and for general safety reasons.

Therefore, the Company reserves the right to inspect and/or search any item brought onto Company premises. This includes, without limitation, any laptop or personal computer, or any package, lunch, toolbox, purse, briefcase or other personal item the employee may bring on the premises. The Company also reserves the right to monitor the use of its computer system and electronic communications devices, such as the voice mail, email system and fax machine, and reserves the right to access, review, copy, delete and disclose any personal information contained on any Company electronic communication device or on its computer system, including Company-owned PCs used by individual employees.

Any such inspection and/or search may be conducted with or without notice and with or without the employee's consent. An employee's refusal to cooperate in an inspection and/or search may result in disciplinary action up to and including termination.

If an employee does not want any personal item inspected and/or searched pursuant to this policy, they should not bring such item onto Company premises or property. Additionally, employees should not use the Company's computer system, e-mail system, voice mail system, or fax machine for any personal information they wish to keep private, as the Company treats all such information as business information and it will be treated no differently than other business information.

15. ELECTRONIC COMMUNICATION DEVICES POLICY

The Company uses various forms of electronic communication devices, including, but not limited to, computers, e-mail, telephones, voice mail, and fax machines. All electronic communications, including all software and hardware, are the sole property of the Company and are to be used only for Company business to transmit or receive business information and are not to be used for personal use. The Company treats all messages sent, received or stored in any of the electronic communication devices as business messages. The Company reserves the right to access and review, copy or delete electronic files, voice mail messages, etc., for any purpose and to disclose them to any

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

party (inside or outside the Company) it deems appropriate. The Company further reserves the right to monitor the use of electronic communications as is necessary to ensure that there is no misuse or violation of Company policy. Use of any of the Company's electronic communications devices in violation of this policy may lead to discipline up to and including immediate termination.

Should employees make incidental use of the e-mail system, fax machine, etc., to transmit personal messages, such messages will be treated no differently than other messages, i.e., the Company reserves the right to access, review, copy, delete or disclose them for any purpose. Accordingly, employees should not use the computer, e-mail system, voice mail system, or fax machine for any personal information they wish to keep private.

The Company's e-mail system permits employees to communicate with each other internally and with selected outside individuals and companies that the Company, in its sole discretion, decides should be connected to the system. Users should treat the computer and e-mail systems like a shared file system -- with the expectation that messages sent, received or stored in the system (including any individual hard disks) will be available for review by any authorized representative of the Company for any purpose.

Confidential Information

Essentially, Company e-mail messages should be treated in the same way as other Company confidential printed material. There are three common circumstances where confidentiality can be breached:

1. An employee leaves the e-mail program running on his or her screen, or leaves an e-mail message on his or her screen. In either case, this allows others to view e-mail messages should they sit at the employee's computer.

2. A confidential message is printed on a printer in an employee's office or perhaps on a shared printer down the hall. Anyone with access to that printer can view this document.

3. An e-mail message is inadvertently sent to someone who was not intended to receive it. Caution should be exercised regarding any confidential message before it is sent.

Caution should be used when using the Internet. The Internet is a convenient, inexpensive way of sending business communications that are not security risks or time sensitive. Employees should not rely on the Internet for critical communications due to the possibility of compromise.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Users must exercise a greater degree of caution in transmitting Company information on the e-mail system than they take with other means of communicating information, (e.g., written memoranda, letters or phone calls) because of the reduced human effort required to redistribute such information. Confidential information should never be transmitted or forwarded to outside individuals or companies not expressly authorized to receive that information and should not be sent or forwarded to other users inside the Company who do not need to access the information. Always use care in addressing e-mail messages to ensure that messages are not inadvertently sent to outsiders or the wrong person inside the Company. In particular, exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Lists are not always updated or maintained and users should take measures to ensure that the lists are current. If highly confidential information needs to be transmitted, please contact Susan Bradley, IT administrator for assistance in sending confidential information via encrypted means.. The State of California expressly bars the emailing of information that contains Social Security numbers.

E-Mail Security and Computer Security

The security on the Company e-mail system and other computer programs is only as good as password security can be. If an employee's network and e-mail passwords are easy to discover, an employee's e-mail can be accessed by anyone with that intention. It is strongly advised that employees not use their first or last name, the Company name or other such passwords. It is also mandatory that employees change their passwords every 90 days.

Viewing and Protecting E-Mails

In order to guard against dissemination of confidential information, users should not access their e-mail message for the first time in the presence of others. E-mail passwords should be routinely changed every 90 days.

Copyrighted Information

Use of the e-mail system to copy and/or transmit any documents, software, or other information protected by copyright laws is prohibited.

E-Mail Etiquette

It should be noted that e-mail messages may be read by someone other than the intended addressee and may even have to be disclosed to outside parties or a court in connection with litigation. Accordingly, care should be taken to ensure that messages are courteous, professional and businesslike.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Other Prohibited Uses

The Company prohibits use of the e-mail system or the Company computer system to engage in any communications that are in violation of Company policies including, but not limited to, transmission of defamatory, obscene, offensive or harassing messages, or messages that disclose personal information about other individuals without authorization.

Storing and Deleting E-Mail Messages

The Company strongly discourages the storage of large numbers of e-mail messages on the system for a number of reasons. First, e-mail messages frequently contain confidential information, it is desirable to limit the number, distribution and availability of such messages to protect the Company's information. Second, retention of messages fills up large amounts of storage space on the network server and personal hard disks, and can slow down the performance of the network server, backup tapes, or individual hard disks for genuinely important documents. The fewer documents the Company computer has to search through, the quicker and more economical the search will be.

Accordingly, it is Company policy that employees may not retain e-mail messages in their electronic inboxes longer than 90 days. Messages older than 90 days must be deleted from the employee's electronic inbox in accordance with the Company's *E-Mail Management and Retention Policy* set forth in Section 16 of this Handbook.

Internet Access

The Internet offers a vast amount of easily accessible information to those who have access to it. The Firm is linked to the Internet to allow employees access to information and resources for Company purposes and in order to enable employees to perform their job duties more efficiently. Any employee access to the Internet for non-Company purposes must be authorized in advance and in writing. Any "downloading" from the Internet by employees for their personal use must be authorized in advance and in writing. Accessing pornographic, offensive or other inappropriate information in violation of Company policy is expressly prohibited and may lead to discipline up to and including immediate termination.

Personal Programs, Screen Savers, Wallpaper and Games

Employees may *not* load or unload any programs on the Company's computer system without management approval. Any unauthorized personal programs, screen savers, wallpaper or games found on the computer system will be removed from the system without contacting the employee responsible for loading them. Unauthorized loading or unloading of programs may result in disciplinary action up to and including termination.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Hacking

Any employee caught "hacking," introducing a "virus" or foreign agent, or attempting to pierce the Company's security arrangements on the Company's computer system will be subject to immediate termination.

Company Information

An employee who removes information concerning the Company or the Company's clients from any part of the Company's computer system and uses that information for personal reasons is subject to discipline, up to and including immediate termination

16. E-MAIL MANAGEMENT AND RETENTION POLICY

The Company's electronic mail ("e-mail) system allows employees to communicate with each other internally and with outside individuals, companies and agencies in order to conduct the Company's business. It is each employee's responsibility to manage and protect the Company's business records resulting from all e-mail communications.

E-mail messages on the Company's computer system, including personal e-mail messages, will be treated in the same manner as any other correspondence received by the Company. For example, regular mail of importance is kept, whereas junk mail is discarded. The Company reserves the right to access, review, copy, delete or disclose them for any purpose. Accordingly, employees should not use the Company e-mail system to transmit personal information they wish to keep private.

All e-mail communications are subject to discovery during legal proceedings and can be used as electronic evidence in the event the Company is involved in litigation. Furthermore, unmanaged and unidentified e-mail messages residing on the Company's computers may pose a threat to the Company's ability to document and reconstruct business and decision-making processes.

The following policy advises employees of their responsibilities regarding the routine removal of messages from electronic file folders, and the storage and retention of e-mail communications which constitute official Company records.

E-mail messages generally fall into three categories:

1. Records which document the business of the Company, such as those involving clients. These types of e-mail should promptly be printed and a hard copy should be placed into the relevant subject matter file. Internal e-mails pertaining to internal Company business and employee and personnel matters will be kept by the Administrator.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2. Messages that have a limited or transitory value to the Company, such as a message announcing the date and time of a meeting, need not be saved pursuant to this policy. Retention of such messages serves no purpose and takes up space. Such messages should be deleted as soon as they no longer serve an administrative purpose. However, if the purpose of the meeting was to discuss a particular Company project, the e-mail would be considered a business record and should be treated as such.

3. Non-records, such as personal e-mails. These types of e-mail messages should promptly be deleted from the electronic inbox.

It is Company policy that employees may not retain e-mail messages in their electronic inboxes longer than 90 days. Messages older than 90 days must be deleted. If the e-mail message pertains to Company business, a printed hardcopy of the e-mail message must be retained for the Company's files. If an e-mail is sent internally, the employee who sent the e-mail is responsible for ensuring that a printed hard copy of the e-mail is put in the appropriate file. The same is true of e-mails sent to persons outside the Company. With respect to e-mails received from outside parties, the employee to whom the e-mail is addressed is responsible for ensuring that a printed hardcopy of the e-mail is placed into the appropriate file promptly upon its receipt.

If unsure as to whether to retain a particular e-mail message or the appropriate file to which it belongs, please check with your supervisor or the Administrator.

All e-mail, including personal use of e-mail, is subject to the Company's Electronic Communication Devices Policy contained in Section 15 of this Handbook.

17. ANTI-VIRUS POLICY

The company provides corporate antivirus for all attached workstations. Anyone found disabling or tampering with that antivirus software will be subject to disciplinary actions.

Files or macros attached to an email from an unknown source should not be opened. These should be deleted from the system immediately and deleted from the "trash" folder.

If a file that has been blocked by the email system due to its potentially hazardous attachment and the sender is known and the email is expected, contact the computer administrator for access to this email.

Users who work at home on firm projects are required to maintain antivirus and firewall protection on their home computers. If such protection is not already on a user's home system, contact the administrator for inexpensive resources for this home protection.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Delete spam, chain and other junk mail and do not forward any emails regarding potential viruses. Many times these are hoaxes and should not be forwarded.

18. PASSWORD POLICY

The firm will change passwords every 90 days. It is recommended that the following guidelines are used when setting up any firm password:

- The password does not contains less than eight characters
- The password is a word not found in a dictionary (English or foreign)
- The password is not a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

19. REMOTE ACCESS

In general

When accessing the network from a remote location, the same attention to security and privacy that is required at the office regarding client files should be adhered to. Those

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

employees previously identified by Management as needing remote access should ensure that at all times the connection to the firm's resources do not in any way jeopardize the safety and security of the network. Therefore, anyone with permission to run remote access is required to have installed an up to date antivirus and an active firewall.

Remote access via Kiosks

It is recommended to use personal equipment to remotely access the firm's network resources and refrain whenever possible from using open, Internet café style connections. Those users with remote connectivity will require special training on the risks of such access and will be instructed on ensuring that usernames and passwords are not saved on such devices. Use this type of access only in an emergency and only when deemed to be appropriate for the need. Remote access may be needed while traveling. A request should be made before such a trip for a laptop for this purpose.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**