Global Information Assurance Certification Paper

Name: Tim Van Acker
Version: Practical Assignment version 1.4b, Option 2
Title: Securing Sensitive Data in a Research Environment: A Case Study
GIAC Security Essentials Certification (GSEC)
Submitted: 8 January 2004

Abstract/Summary

The costs associated with collecting research data in the United States and internationally are substantial, resulting in many funding agencies, such as the National Institutes of Health (NIH), now requiring recipients to make the data they collect available to the broader research community.

> NIH … believe[s] that data sharing is essential for expedited translation of research results into knowledge, products, and procedures to improve human health. The NIH expects and supports the timely release and sharing of final research data from NIH-supported studies for use by other researchers.[1]

Dissemination of research data can present challenges for the project staff charged with securing the sensitive data, especially on machines over which they have no administrative control. This case study defines a major risk - deductive disclosure - associated with longitudinal research data and gives an overview of the defense-in-depth security plans I developed to help one research project protect the data they disseminated to researchers around the country who are storing and analyzing the data on a number of different computer systems. I also developed for this research project some "fill in the blank" forms mirroring the security plans to assist researchers who are applying to use the data.

These security plans are now being implemented in research environments nationwide. I reevaluate these security plans and forms periodically to ensure current best practices are maintained. I have included as appendixes some samples of these security plans and the accompanying "fill-in-the-blanks" forms.

Before Snapshot

Several years ago, staff on one of the research projects in my organization developed guidelines for disseminating sensitive data to researchers around the country. These guidelines included eligibility requirements, a request for a security plan to protect the sensitive data, requirements for Institutional Review Board (IRB) review of the security plan for handling and storing sensitive data, a data confidentiality agreement to be signed by the data recipient, and notification that site visits may occur to verify the data was being used and protected in the manner specified in the researcher's application.

[1] "Final NIH statement on sharing research data." 26 February 2003. URL: http://grants2.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html

When the data were first disseminated to hundreds of researchers around the country, Unix was an operating system many social science researchers did not know and DOS/Windows 3.x was slowly giving way to Windows 95. From a social science research perspective, all the proper steps had been taken to safeguard the data. Besides the guidelines already mentioned, all variables that could identify an individual had been removed. The data sets were also password-protected using an archiving program before they were copied to a CD. The CD was then mailed to the researcher and the researcher in turn was required to call the project's data manager to acquire the password in order to unzip the password-protected data set. Knowing that technology, and therefore vulnerabilities of technology, would change over time, the researchers were required to renew their applications for continued use of the data every three years, and in so doing, were also required to update their security plan.

When the first researchers received the data, there was only one round of data collected. By the time their contract renewals were due, there were two more rounds of data added to the data they originally received. Data gathered on the same individual or group of individuals over a period of time is known as longitudinal data.

> Longitudinal research refers … to the process of tracking a group of individuals over time to establish how the state of that group varies and, more importantly, to establish the average relation between an individual's state at one time and his state at another…Usually this methodology requires that an observation on a person at a particular time be linked with observations made on that person at subsequent times, for each person in a sample. The vehicle for linkage is typically, though not always, the individual's identification. The linkage implies some degradation of privacy….[2]

Longitudinal data, even when the individual's personal identification has been removed, increases the likelihood of deductive disclosure. Deductive disclosure is the discerning of an individual respondent's identity and responses through the use of known characteristics of that individual.[3] If someone knows a survey respondent in a longitudinal study and he has access to the data, it may be possible to identify the respondent's record simply by knowing a few non-sensitive pieces of information about the respondent. The risk of deductive disclosure on the part of a researcher is quite low, because the researcher has signed a confidentiality agreement which was approved by his Institution's review board stating he will not attempt to deduce an individual's identity and if he accidentally does, he will report the incident to the IRB.

Reasons for unauthorized use of data vary, from the merely curious or mischievous to the more complicated uncovering of illegal or high-risk health

[2] Boruch, Robert F. and Joe S. Cecil, p.31.
[3] Doyle, Pat, Julia I. Lane, Jules J.M. Theeuwes, and Laura V. Zayatz, p.138.

behavior. If a person is able to get access to the data, he could take advantage of deductive disclosure. Hence the need for a security plan that protects against such unauthorized access to the data.

Security of the data was left up to each individual researcher who devised his own data security plan. While some researchers submitted security plans that incorporated new technologies, such as using the Windows NTFS permissions to restrict access to the data directory, others were at a loss as to how to provide the most basic security measures.

As operating systems change over time, so do their benefits and vulnerabilities. Asking researchers to come up with a detailed security plan to ensure the safety of the data was a lot like asking them to draft a detailed plan for building a combustion engine: neither task lay within their field of expertise.

With this analogy in mind, I was initially enlisted to help review the backlogged renewal applications and new application submissions for security issues from a system administrator's perspective. After reviewing a few security plans several things became clear:

- most researchers requesting the data were at a loss as to how to create and implement a security plan that would offer a minimal amount of protection for the data,

- researchers were using different computing platforms, so recommended guidelines for securing the data on a number of different computing platforms were needed,

- a more efficient method for communicating recommended security guidelines for different computing platforms would be useful, as would personal interaction between the researchers and someone with experience securing systems, and

- guidelines developed for this project could be used for other research projects that have sensitive data that needs protecting.

By the time I got involved with this project, the data gathered by this research project had been disseminated to over 250 sites and had been used by over 1,000 researchers around the country for a period of six years. The security plans that were being submitted to protect the data relied primarily on user IDs and passwords to log into the system. Little thought was given to physical security of the systems on which the data were stored or to protecting the data at the directory level and practically no thought at all was given to protect the data from unauthorized access across the internet.

Physical security of the systems on which the data were stored as well as protecting the data at the directory level and from unauthorized access across

the wire had become crucial. Although there were no identifying variables in these data, the risk of deductive disclosure had become a real possibility because some of the original subjects in the research study were now college students and could very well be enrolled in colleges or universities where these data were being analyzed. It would be a simple matter for a former survey respondent to gain access to the data if the machine on which the data were stored was not secured properly, both physically and from unauthorized access. Wondering who else from his area participated in the research study, and curious as to their responses, all that would be needed for this person to gain access to the data set was physical access to the computer where the data resided.

For all new applications to use this data and for all application renewals, it had become imperative that the security plans address the need to ensure the data was accessible by only authorized users.

During Snapshot

Since researchers were using various computer systems to analyze this data, I developed security blueprints for a number of different systems, including a stand-alone computer, a computer connected to a private network (also known as a cold room or a secure data facility), a Windows- and Macintosh-based computer connected to the network, and Windows and NetWare servers. In collaboration with our Unix administrator, I also developed some guidelines for securing Unix workstations and servers.

I began by researching how best to secure each of these systems, taking into consideration both best practices for securing these systems as well as the time and money involved. Since all operating systems have vulnerabilities, in addition to securing the systems against the most common vulnerabilities listed on the SANS/FBI Top Twenty Vulnerabilities List,[4] I added to this list from best practices for each system. Works I referenced for determining best practices for the different operating systems are listed at the end of this paper in the section titled *References*.

I took a defense-in-depth ("the practice of building multiple layers of security into a given system or network")[5] approach when I developed these security blueprints. Several analogies have been made to help define the defense-in-depth approach to security. One is the comparison between an egg and an onion. If someone can breach the shell of an egg, that person will have gotten past all existing protective layers, whereas there are many layers to an onion: when you peel away one layer of an onion, another layer is revealed.

[4] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." URL: http://www.sans.org/top20
[5] Tippett, Peter. URL: http://www.infosecuritymag.com/2002/feb/columns_executive.shtml

When I began developing these security blueprints the image I had in mind was not that of an egg or an onion, but rather the 1,000 meter hurdles. In order for an unauthorized user to gain access to the data, or cross the "finish line," that person would have to "jump" over one hurdle after another until all hurdles had been cleared. Knowing that each researcher's environment may be slightly different than another's and that one researcher may not be able to implement every single security precaution I recommended, I viewed each of my security recommendations as a hurdle. The more hurdles to overcome, the more secure the system, but if one or two precautions couldn't be implemented for some reason, the other hurdles should be sufficient to provide an acceptable measure of security.

Although there are several dangers with trying to produce a list of "do's" and "don'ts" for securing specific systems (e.g., there are no complete lists, everyone has his own idea of what should or should not be on the list, new vulnerabilities are discovered weekly so the list will be in constant need of updating, to name a few), there are several security components that can be implemented on any system. I identified three main areas for securing each system: physical security of the machine, controlling access to the data directory, and ensuring only authorized users were able to gain access to the machine from across the wire.

Under these three areas, the following security components, or "hurdles," were implemented and are common to each of the blueprints used for this research project:

- physical security
- granting access according to "least privilege"
- requiring strong passwords
- limiting services running on the system to only those absolutely needed
- patching the operating system and applications immediately when patches are available for newly discovered vulnerabilities
- using data encryption and antivirus software
- using shredding software
- incorporating a firewall on the system
- and enabling auditing and checking the log files.

I began with securing the machine on which the data reside physically, because physical security, while arguably the most important aspect of security as a whole, is often the most overlooked.[6] If an unauthorized person has physical access to a machine, that machine can not be truly secured. If one has physical access to a machine, it is a trivial matter to reboot that machine with a special boot diskette designed to give one the ability to change the local administrator's password, at which point the unauthorized person is granted full administrative control of the local machine.

[6] Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz, p.255.

The physical security of the system in my blueprint consisted of the following components. Any machine with our data on it must reside in a locked office, one to which only authorized personnel have a key. The BIOS must be configured to boot from the hard drive only and must be password protected so only authorized users can change the BIOS configuration. In some instances where unauthorized personnel had keys to the room where the computer was located, I required that the computer case be locked so an unauthorized person could not remove the CMOS battery or change the BIOS jumper, thereby disabling the BIOS password.[7]

After ensuring only authorized personnel would have access to the machine on which the data resides, I specified only authorized users should be given permission to access the directory where the data reside, using the security features of the operating system to control such access. For instance, Windows NT4 and Windows 2000 systems use the NTFS permissions. In addition to limiting access to the directory to only authorized personnel, I specified the users were to use strong passwords through the use of the operating system's password policy, including length, age, and complexity requirements.[8]

I then encouraged the researcher to limit services running on the system to only those absolutely needed.[9] This simple practice can be implemented on any operating system and, though it may be a subjective practice (e.g., what one person considers unnecessary another may deem completely necessary for his environment), is effective in limiting the risks for the operating system. Although I gave the individual researcher latitude on this security option, I did insist that the machine on which our data were stored did not have the following services running: the server service on workstations not acting as servers, IIS, Peer Web Services, RAS, Gopher, FTP, IP Forwarding, Simple TCP/IP Services, and SNMP.

Many of the other security steps could easily be nullified if the operating system and applications (such as Internet Explorer) are not patched in a timely manner. Therefore I also required that the researcher patch the operating system and applications immediately when patches become available for newly discovered vulnerabilities. Fortunately there are some tools available to assist the researcher in patching his operating system and applications. For researchers using the Windows operating system, the *Windows Update* feature of the operating system assists them in applying the latest critical and security updates.[10]

---

[7] "How to disable the BIOS password." URL: http://www.cpucare.com/FAQS/Disable%20Bios%20Passwords.html

[8] "The Simplest Security: A Guide To Better Password Practices." http://www.securityfocus.com/infocus/1537

[9] "Configure computers to provide only selected network services." URL: http://www.cert.org/security-improvement/practices/p038.html

[10] "How To: Keep your Windows Computer Up-to-Date." URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q311047

As an added measure of security, I encouraged the use of data encryption software. Encryption "is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people."[11] There are a number of programs available for encrypting data,[12] including the Encrypting File System built into Windows 2000 and Windows XP.[13] In the unlikely event that the other security steps are circumvented and someone gains access to the machine or data directory, taking the extra precaution of encrypting the data directory helps to ensure that only an authorized person with the appropriate pass phrase, or private key, would be able to access the data.

A quick search with one's favorite internet search engine will find a number of free or low cost utilities that can be used to undelete files that have been deleted from a computer or server. In order to ensure our data could not be recovered from a computer from which the data had been deleted, I required the use of a secure erasure software package.[14] Deleting files from a computer usually removes the location of the file on the disk from the File Allocation Table (FAT). A secure erasure program will write random 1's and 0's on the media where the file reside. Many of these secure erasure programs allow the user to specify the number of times the random data will be written to disk, decreasing the likelihood that a recovery program will be able to recover the original data.

In order to help protect the data against back-door Trojans and other malicious email viruses, including Microsoft Word macro viruses, I also required the use of antivirus software. In order for the antivirus software to be relatively effective, the system should be configured to update the definition files and to run a complete system scan on a regular basis.

Working in tandem with an up-to-date antivirus program, I required the proper use of a personal or departmental firewall to "deny all traffic" from accessing the local machine on which our data are stored.[15] According to Steve Gibson of Gibson Research Center, "A firewall absolutely isolates your computer from the Internet using a "wall of code" that inspects each individual "packet" of data as it arrives at either side of the firewall — inbound to or outbound from your computer — to determine whether it should be allowed to pass or be blocked."[16]

As the last layer of defense, I required the use of auditing on the systems on which our data is stored and I encouraged the researchers to check their log files periodically. Specifically, I recommended that the system be configured to audit login success and failure, failed attempts at exercising user privileges, and system events such as shutdowns. I encouraged the researcher to move the log files out of the default location (%system-root%\system32\config*.evt on a

[11] URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html
[12] URL: http://www.winappslist.com/security/encryption1.htm
[13] "Best practices for the Encrypting File System." URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;223316
[14] "File Wipers." URL: http://www.winappslist.com/security/file_wipers1.htm
[15] "Appendix A Common Vulnerable Ports." URL: http://www.sans.org/top20/#ports
[16] "Personal Internet Firewalls that really work." URL: http://grc.com/su-firewalls.htm

Windows system) and secure the new location with NTFS permissions. I also recommended that they restrict access to the log files to administrator only.

There were a number of other operating system specific “hurdles” I recommended, but those listed above are the ones that were common across all blueprints.

After Snapshot

Along with the preceding suggested steps for securing their systems to store and analyze the data, I created forms that match the security steps to make it easier for the researcher to tell our project staff which security steps they took.

I reevaluate the specific steps enumerated in each scenario periodically in order to maintain current best practices for securing each system.

The example security blueprints listed in the appendixes, as well as several others, are currently being implemented by researchers around the country. Through support from this project, I am available for consultation via email and telephone to researchers and their network administrators who have questions or would like assistance implementing the security recommendations.

The security plans and the forms have streamlined the application process, providing quicker turn-around for approving application renewals and new applications, and they have also given this research project a higher level of data security.

There are two other notable events that took place as a result of my contribution on this project. I was invited by the National Institutes of Health to this project’s annual workshop where I consulted with researchers from around the country on their security plans and I was written into the grant for the next round of funding as the project’s security advisor.

References

"Final NIH statement on sharing research data." 26 February 2003. URL: http://grants2.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html (8 January 2004).

Boruch, Robert F. and Cecil, Joe S. Assuring the Confidentiality of Social Research Data. University of Pennsylvania Press, 1979. 31.

Doyle, Pat, Lane, Julia I., Theeuwes, Jules J.M., and Zayatz, Laura V. Confidentiality, Disclosure, and Data Access. Amsterdam: Elsevier Science, 2001. 138.

"The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. October 8, 2003. URL: http://www.sans.org/top20 (8 January 2004).

Tippett, Peter. "Defense in Breadth." February 2002. URL:

http://www.infosecuritymag.com/2002/feb/columns_executive.shtml (8 January 2004).

Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK Version 2.1. SANS Press, April 2003. 255.

"How to disable the BIOS password." URL: http://www.cpucare.com/FAQS/Disable%20Bios%20Passwords.html (8 January 2004).

Granger, Sarah. "The Simplest Security: A Guide to Better Password Practices." 17 January 2002. URL: http://www.securityfocus.com/infocus/1537 (8 January 2004).

"Configure computers to provide only selected network services." URL: http://www.cert.org/security-improvement/practices/p038.html (8 January 2004).

"How To: Keep your Windows Computer Up-to-Date." 03 December 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q311047 (8 January 2004).

"Encryption." 27 October 2003. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html (8 January 2004).

"Encryption." URL: http://www.winappslist.com/security/encryption1.htm (8 January 2004).

"Best practices for the Encrypting File System." 5 December 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;223316 (8 January 2004).

"File Wipers." URL: http://www.winappslist.com/security/file_wipers1.htm (8 January 2004).

"Appendix A Common Vulnerable Ports." Version 4.0. October 8, 2003. URL: http://www.sans.org/top20/#ports (8 January 2004).

Gibson, Steve. "Personal Internet Firewalls that really work." 6 October 2003. URL: http://grc.com/su-firewalls.htm (8 January 2004).

"The 60 Minute Network Security Guide." Version 1.2. 12 July 2002. URL: http://www.nsa.gov/snac/support/guides/sd-7.pdf (8 January 2004).

Gibson, Steve. "Internet Connection Security for Windows Users." URL: https://grc.com/x/ne.dll?bh0bkyd2 (8 January 2004).

Microsoft Security and Privacy. URL: http://www.microsoft.com/security/ (8 January 2004).

"How Secure is your Mac?" URL: http://www.securemac.com/ (8 January 2004).

"Apple Security Updates." 22 December 2003. URL: http://docs.info.apple.com/article.html?artnum=61798 (8 January 2004).

"Resources to Help Improve Security." 24 October 2003. URL: https://www.unc.edu/security/resources.html (8 January 2004).

Appendix A

A Sample Security Blueprint: Stand-Alone Computer

Securing data on a stand-alone computer

A standalone computer is one that is in no way connected to another computer or networked device, such as a switch, hub, or router (with the possible exception of a printer), or connected in any way to the internet or a company or departmental LAN. The standalone computer can be running Windows 2000 client or server, Linux, or Mac OS X. Since the computer is not connected to the internet or a local or wide area network, the emphasis for securing the data on a standalone computer is placed on physical security of the computer and controlling access to the data directory.

Following are the minimum steps recommended to secure the data on your standalone PC:

Physical Security of a Standalone Computer

1. Configure the BIOS to boot the computer from the hard drive only. Do not allow the standalone computer to be booted from the diskette or CD-ROM drive.
2. Password protect the BIOS so changes cannot be made to the BIOS without authorization.
3. Secure the computer on which the data resides in a locked room, or secure the computer to a table with a lock & cable (locking the case so the battery cannot be disconnected, which will disable the BIOS password).
4. Remove or disable the network interface card (NIC) so it cannot be used.
5. Install encryption software[17] for directories containing secure data. (Windows 2000 encryption is free and works well)
6. Install and periodically run a secure erasure[18] program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. Shred 2 is inexpensive, works well, and can be downloaded from PC Magazine for a minimal fee.[19]

Controlling Access to the Data Directory

1. Restrict access to the data to project personnel using the security features available via the operating system (e.g., login via userid/password and NTFS permissions in Windows 2000/XP, ACLs in Linux and OS X).
2. Require strong passwords.[20]
    - You can run L0phtcrack to look for bad passwords[21]
    - You can use SCM to enable password complexity[22]
3. Password protect screen saver and activate for 3 minutes of inactivity.

The steps for securing the data on a private network (also known as a “cold room” or “secure data facility”) are similar to the preceding steps used to secure a stand-alone computer so will not be duplicated here.

[17] http://www.winappslist.com/security/encryption1.htm
[18] http://www.winappslist.com/security/file_wipers1.htm
[19] http://www.pcmag.com/article2/0,4149,13352,00.asp
[20] http://www.securityfocus.com/infocus/1537
[21] http://www.atstake.com/products/lc/download.html
[22] http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp

Appendix B
Sample Security Checklist for Stand-Alone Computer

Detailed description of computer system where data will be stored and analyzed

1. Type of Hardware/Operating System.
2. Physical location of hardware.
3. How backups are handled/how data will be excluded from the backup routine.
4. Who has physical access to the equipment?
5. Who has permission to use the equipment?
6. Is the system used by other projects?
7. Where hard copy info will be printed.
8. How hard copy data will be handled/stored/disposed of.
9. Secure storage location (building, room number, and type of storage unit) of original data CD.

Security system that would prevent unauthorized access to the data

The following steps are minimum steps that should be taken to secure your standalone computer that houses the data. Please indicate below which security steps you have implemented. If you do not implement all of the following steps, please write a short explanation for why you can not implement a specific item.

Physical Security of a Standalone Computer

1. I configured the BIOS to boot the computer from the hard drive only. I am not allowing the standalone computer to be booted from the diskette or CD-ROM drive.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

2. I password protected the BIOS so changes cannot be made to the BIOS without authorization.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

3. I secured the computer on which the data resides in a locked room, or secured the computer to a table with a lock & cable (locking the PC case so the battery cannot be removed).
___ Implemented ___ Not Implemented (please explain why, if not implemented)

4. I removed or disabled the network interface card (NIC) so it cannot be used.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

5. I installed encryption software for directories containing secure data (i.e. Windows 2000 encryption).
___ Implemented ___ Not Implemented (please explain why, if not implemented)
Name of encryption software _____

6. I installed and periodically run a secure erasure program. This program will be run monthly and after the secure data has been removed from the computer at the end of the contract period.
___ Implemented ___ Not Implemented (please explain why, if not implemented)
Name of secure erasure software _____

Controlling Access to the Data Directory

1. I restricted access to the data to project personnel using the security features available via the operating system (i.e. login via userid/password and NTFS permissions in Windows NT/2000, ACLs in Linux and OS X).
___ Implemented ___ Not Implemented (please explain why, if not implemented)

2. I require strong passwords.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

3. I activate a screen saver with password after 3 minutes of inactivity.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

Appendix C
Sample Security Blueprint: Windows Computer on a Network

Securing the data on a Windows computer connected to a network

A network is comprised of two or more computers and/or network devices (i.e. printer, switch, hub, router) which are connected to the internet or a company or departmental LAN. Since the computer is connected to the internet or to a local or wide area network, the emphasis for securing this computer is placed on physical security of the computer, access to the data directory, and protecting the data from unauthorized access across the wire.

The first two security steps, "physical security of a computer on a network" and "controlling access to the data directory," are nearly identical to the steps listed above in the "securing data on a stand-alone computer" scenario, so will not be duplicated here. The following are additional minimum steps you should take to secure the data on a computer running Windows 2000 if the computer is connected to the internet or a company or departmental network:

1. Do NOT install IIS or MS SQL server on Windows boxes which will house sensitive data
2. Turn off all unneeded services[23] (the following list is provided as an example, and may not be a complete list for your environment)
    - Server Service
    - IIS
    - Peer Web Services
    - RAS
    - Gopher
    - FTP
    - IP Forwarding
    - Simple TCP/IP Services
    - SNMP
    - Disable unneeded network protocols (e.g. IPX or NetBEUI)
3. Do not install Windows File & Printer Sharing
4. Do not enable file sharing
5. Remove the Everyone group from the Access this Computer from the Network user right (User Manager-->Policies-->User Rights)
6. Disable the Guest account
7. Replace group Everyone with the appropriate group(s) on critical system folders, files and registry keys
8. Remove, disable, or rename administrative shares (c$, d$, admin$)[24]
9. Restrict/Prevent anonymous access and enumeration of accounts and shares (only one of the following is required)
    - You can use the Security Configuration Manager (SCM)[25]
    - Manually Edit the Registry[26]
    - More information on NULL sessions and their vulnerabilities can be found on the SANS website[27]
10. Create a new userid for administrative purposes and add this userid to the Local Administrator's group. Remove the original administrator userid from the Local Administrator's group ("dumb it down") and remove the account's Access this computer from the network right.
11. Encrypt the SAM: from SP3 and above, run
    - syskey.exe

[23] http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp
[24] http://support.microsoft.com/default.aspx?scid=kb;en-us;318751
[25] http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp
[26] http://support.microsoft.com/default.aspx?scid=kb;en-us;246261
[27] http://www.sans.org/rr/papers/index.php?id=286

12. Install all OS and application (i.e.: Internet Explorer) security patches
    - You can use Windows Update[28]
    - You can use HFNetchk[29]
13. Install Antivirus software and keep the virus definition files updated
14. Secure performance data[30]
15. Enable auditing
    - Audit Login success & failure
    - Audit failed attempts at exercising user privileges
    - Audit system events such as shutdowns
    - Move log files out of the default location and secure with NTFS permissions (%system-root%\system32\config*.evt)
    - Restrict access to the log files to administrator only
    - Check your logs often!
16. Disable or remove Windows Scripting Host[31]
17. Use a corporate, hardware, or personal (software) firewall:
    - Hardware: Linksys Instant Broadband EtherFast Cable/DSL Router[32]
    - Software personal firewall[33]
        - ZoneAlarm or ZoneAlarm Pro[34]
        - Tiny Personal Firewall[35]
        - Sygate Personal Firewall[36]

[28] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q311047
[29] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q303215
[30] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q146906
[31] http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html
[32] http://www.linksys.com/products/product.asp?prid=142&grid=5
[33] http://grc.com/lt/scoreboard.htm
[34] http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp?lid=zadb_zadown
[35] http://www.tinysoftware.com/home/tiny2?la=EN
[36] http://smb.sygate.com/products/spf_standard.htm

Appendix D
Sample Security Checklist for Computer on Network

Detailed description of computer system where data will be stored and analyzed

1. Type of Hardware/Operating System.
2. Physical location of hardware.
3. How backups are handled/how data will be excluded from the backup routine.
4. Who has physical access to the equipment?
5. Who has permission to use the equipment?
6. Is the system used by other projects?
7. Where hard copy info will be printed.
8. How hard copy data will be handled/stored/disposed of.
9. Secure storage location (building, room number, and type of storage unit) of original data CD.

Security system that would prevent unauthorized access to the data

The following steps are minimum steps that should be taken to secure your Windows 2000/XP Computer that houses the data if your computer is connected to a network. Please indicate below which security steps you have implemented. If you do not implement all of the following steps, please write a short explanation for why you can not implement a specific item.

Physical Security of a Windows 2000/XP Computer on a Network

1. I configured the BIOS to boot the computer from the hard drive only. I am not allowing the standalone computer to be booted from the diskette or CD-ROM drive.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

2. I password protected the BIOS so changes cannot be made to the BIOS without authorization.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

3. I secured the computer on which the data resides in a locked room, or secured the computer to a table with a lock & cable (locking the PC case so the battery cannot be removed).
___ Implemented ___ Not Implemented (please explain why, if not implemented)

4. I installed encryption software for directories containing secure data (i.e. Windows 2000 encryption).
___ Implemented ___ Not Implemented (please explain why, if not implemented)
Name of encryption software: _____

5. I installed and periodically run a secure erasure program. This program will be run monthly and after the secure data has been removed from the computer at the end of the contract period.
___ Implemented ___ Not Implemented (please explain why, if not implemented)
Name of secure erasure software: _____

Controlling Access to the Data Directory

1. I restricted access to the data to project personnel using the security features available via the operating system (i.e. login via userid/password and NTFS permissions).
___ Implemented ___ Not Implemented (please explain why, if not implemented)

2. I require strong passwords.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

3. I activate a screen saver with password after 3 minutes of inactivity.
___ Implemented ___ Not Implemented (please explain why, if not implemented)

Protecting the Data from Unauthorized Access Across the Wire

1. I did not install IIS or MS SQL server on the Windows computer that houses sensitive data.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

2. I turned off all unneeded services and disabled unneeded network protocols.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

3. I did not install Windows File & Printer Sharing
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

4. I did not enable file sharing on local Windows machines
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

5. I removed the Everyone group from the Access this Computer from the Network user right.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

6. I disabled the Guest account.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

7. I replaced group Everyone with the appropriate group(s) on critical system folders, files and registry keys.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

8. I removed, disabled, or renamed administrative shares.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

9. I restricted/prevented anonymous access and enumeration of accounts and shares.
   ___ Implemented ___ Not Implemented (please explain why, if not implemented)

10. I created a new userid for administrative purposes and removed the original administrator userid's administrative privileges.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

11. I protected the administrative password.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

12. I encrypted the SAM.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

13. I installed, and will maintain, all OS and application (i.e.: Internet Explorer) security patches.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

14. I installed an antivirus software program and will keep the virus definition files updated.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)
    Name of antivirus software: _____

15. I secured performance data.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

16. I enabled auditing and will check the logs often.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

17. I disabled or removed Windows Scripting Host.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)

18. I use a corporate, hardware, or personal (software) firewall.
    ___ Implemented ___ Not Implemented (please explain why, if not implemented)
    Name of firewall: _____