# Global Information Assurance Certification Paper

*SANS Security Essentials*
*GSEC Practical Assignment, Version 1.4c, Option 1*


# Reducing the Internal Risk

**Scott Steiner**
**11/22/2004**

## Table of Contents:

## Abstract / Introduction

Many organizations fear that hackers will penetrate their network through cracks and backdoors in the perimeter to steal corporate data and trade secrets, but chances are, this information is readily available right through the front door. The majority of all security budgets focus solely on reducing external threats, overlooking the internal risk by trusting their recruitment process of selecting employees with high morals and values. In 2000, Microsoft published "A list of 10 Immutable Laws of Security Administration", and the first law states: "Nobody believes anything bad can happen to them, until it does" (1). How many times have you heard: "What are the chances of an employee doing that?" or "That will never happen to us"? Gartner estimates that 70 percent of security incidents which actually cause loss to enterprises involve attacks from the inside (2).

By design, your corporate network, servers, and workstations have a strong presence of initial security, but over time, the obstacles that are put in place will slowly be torn down by your system administrators, application developers, support personnel, and even your average users who do not hold any special privileges. This is due to the lack of education, policy and audit. Organizations must place internal security ahead of convenience by setting policy, establishing controls and monitoring for compliance. Doing so will reduce the risk of accidental leakage or deliberate theft of intellectual property from internal employees.

## Physical Security

To coincide with "The 10 Immutable Laws of Security Administration", Microsoft has recently published another list, "The 10 Immutable Laws of Security". Law three covers physical security and reads that if someone has physical access to a computer, they can take control of it (3). This emphasizes that a strong physical security program is just as important in protecting your intellectual property as a strong information security program. Denial of service attacks can be the simplest in nature with someone unplugging a production server to someone physically destroying a computer or server with a hammer. Theft of backup tapes, server hard drives, or laptops pose the greatest risks of data theft as they are easily concealable, and highly portable.

While someone may not be brave enough to physically take one of the above mentioned items, a bootable disk can be inserted into the computer to overwrite the data on it, or made to bypass the security settings and boot the computer with administrator privileges, even allowing you to change the administrator password. All of these actions can be performed with the Windows SuperWinPE disk and do not require a local account on the computer (4). A query on internet search engines such as Yahoo! or Google will locate several websites with other bootable disks available for download, with detailed instructions on how to utilize them. By logging in as the administrator, an

attacker can read, modify, or delete any file currently on your computer, as well as install key-logging programs or remote viewing software to be able to access your computer and data in the future. This would allow an attacker access to your computer any time they wish, leaving you with a false sense of confidentiality. If you are lucky enough to catch the security breach, since the attacker did not log on using a local or domain account, and connects to the computer using the administrator account, identifying who accessed the computer will be nearly impossible.

Key loggers and remote viewing tools are gaining in popularity and publicity. A key logger is simply a small hardware device or an application that is installed on a computer and captures the keystrokes typed by the user. There have already been several corporate cases of employees installing a key logging device onto a co-workers computer to identify passwords and sensitive information. When leaving your computer unattended, locking your office or securing your laptop in a cabinet (if you are in a cubicle environment) are the best ways to prevent being victimized . If you can not secure your computer, physically looking at the back of your computer to identify a rogue device will also suffice, but getting users to check their computers on a daily basis is impractical. To prevent key logging or remote viewing applications from being installed, install a file integrity checking tool such as Tripwire.

Implementing electronic access control for your data rooms and network closets will help eliminate unauthorized access to your critical servers and network devices. Physical security is not solely the responsibility of the corporate security department, but rather inclusive of each individual. Employees should treat their computers as an extension of their wallet or purse. Locking your laptop in an office cabinet, as well as your office door will help prevent computers and their data from being compromised at work. These are the first steps to physically protecting your computers from late night intruders, contractors, or employees. Securing your computer during lunch break or lengthy meetings is just as important to prevent against attackers during the daytime working hours. If an employee knew that every day at 12:00 you take an hour and a half to go use the fitness center across the street, it would be more then enough time for them to slip into your office and compromise your computer.

**Social Engineering**

Social engineering is defined as “a hacker’s clever manipulation of the natural human tendency to trust. The hacker’s goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system (5).” The most common approach to social engineering is by using the telephone. Most people give away information trying to be useful or helpful and it makes a Help Desk an easy target. An example of social engineering would be for an employee to go to another

employee's office and call the help desk, impersonating the voice of the target victim to get the password reset. Another example of social engineering would be to pose as a manager or executive, calling another executive and asking them to fax a contract or piece of sensitive information that can be used as leverage or blackmail. An attacker may also call an employee or the help desk, then ask to be transferred to another employee. When the employee sees the number of the caller ID, it will show up as the Help Desk or the employee who originally transferred the call. It may be at this time the attacker poses as the HR department in need of his social security number or as the help desk asking for their password.

Social engineers usually work in teams, collecting small amounts of information at a time, which they piece back together to cause severe damage. To prevent social engineering, policies on how to give out information need to be put in place, as well as providing training sessions to your employees on how to prevent being victimized.

**Local Administrator Passwords**

If your organization is like the majority, you have a Microsoft Windows network using Windows NT, 2000, 2003, or XP. Last year a survey by IDC showed 94% of client computers worldwide use a Microsoft operating system. Another survey showed that over 55% of server licenses are for Microsoft server operating systems (6). While the margin of server licensing has a smaller dominance, Microsoft products are typically the most targeted systems due to user familiarity and global exposure of its vulnerabilities.

The administrator account is a built in Windows system account with full control of the local computer, whether it is a server, workstation, or laptop. Typically, an organization will have a separate administrator passwords for the servers and the workstations to prevent server support personnel having control of workstations and client support personnel having control of servers.

Normally, a corporate security policy states that the local administrator password will be changed every 6 or 12 months or after turnover of an employee that is aware of the administrator password. In a perfect world we would all adhere to this policy, but in most organizations head count is lower then the daily workload and this policy gets abused. The reality of things is your organization's local administrator password is 1, 2, maybe even 3 years old and was probably last changed when the client support group upgraded the OS platform.

This password is initially only given to the client support personnel, but it quickly loses its accountability due to support personnel putting convenience ahead of security. This happens when help desks or client support technicians remedy trouble calls over the phone by having a general user log in as the administrator

to walk them through a resolution, rather then visit the user's desk. Temporary contractors come and go and client support technicians and help desk employees move into newer positions within the organization, and soon you have 50-60 current and former employees who know this password.
The largest level of concern is not that this password is passed around, but that there is one password that will administer every employee's computer, from the CEO to the mailroom clerk. If an attacker knows the computer name of the CEO, which can be identified by opening the "My Network Places" in Windows XP, or "Network Neighborhood" in Win NT/2000, they can copy the entire disk drive. (Many organizations name their computers with a naming convention that includes the employee's name, floor number, and/or the department they work.) This is probably one of the largest overlooked risks in any organization, knowing who has the administrator password?

With Active Directory, changing the administrator password is a much easier task then in years passed, yet it still gets overlooked by higher priority projects. Most managers make this an objective, but only assign personnel to it when it is convenient, or when an incident occurs. A better approach to having a single password for the administrator account is to identify your executives and key personnel (Finance, Legal, HR) and create a password for these computers that is different from your average employees, this way if the password is leaked to a mailroom employee clerk, he can't copy the HR directors files, seeing who is getting a promotion next year and who isn't.

For the server portion, the passwords are normally much more controlled as fewer employees have a need to use this account and there are only a fraction of servers when comparing it to workstations. Even though the exposure of the server administrator account is probably smaller, there is more of a desire to gain access to critical infrastructure servers which may contain customer information or employee payroll data. One of the largest risks associated with the administrator account is that it can never be locked out, making it susceptible to a brute force attack, therefore a strong physical security program is needed to protect physical access to the organizations servers.

**Logon Scripts**

Each time a user authenticates to your domain, you are probably running some type of script that will do various tasks like mapping network drives, checking the anti-virus signature, running the Windows Update function, adding a domain group to the local Administrators group. Wait, what is that last one?

One common practice in large organizations is to add the user's domain account to the local Administrators group so that if they have a need to install software, they aren't calling the help desk to give them administrator level access, reducing the spread of the administrator password. Today's users are smarter then in years past, and know that someone may be able to log on to

their computer and see what they have been doing. If you give a user administrator privileges, it is just a matter of time before they remove all other people from the local Administrators group, making it difficult for a client support technician to service their computer when they have a problem because they no longer have administrator privileges, or even the ability to log into it at all. Someone in your organization will do this, and the solution will be to create a local computer administrators group on the domain, then add all of the employees to it they think will ever have the need for local computer administrator access. Adding a line to the logon script will then insert this group into the local Administrators group each time the user logs on to the computer. This will ensure that the client support technicians and all of those other employees who may need access have Administrator privileges to each computer from the CEO to the mailroom clerk.

It seems like a perfect plan on paper, and it is except when you start thinking about security. The drawback to the above solution coincides with the local administrator password, it gives no confidentiality to the computers that your executives and key personnel store their files. If there are 10-15 employees in this group, coupled with the large number of contractors and employees who know the local administrator password, your key personnel are not going to be happy when told after a security breach of how many people had access to their files. Giving employees access to more information then they need coincides with the “principles of least privileges”. The “principle of least privilege” states that you need to only give the least amount of privileges to an employee to do their job (7).

Again, there is a separate client and server risk associated with this topic. The second aspect of this logon script is that it gets executed each time a user account gets authenticated to the domain. This is independent of whether it is a workstation or a server. Best practices state that server and domain administrators use accounts with minimal privileges for their regular use and use accounts with elevated privileges when administering the Active Directory or critical servers. The server group will recognize this and execute this best practice, while also removing the logon script for their accounts with elevated privileges to prevent any scripts being run on the servers automatically. The catch to this is that the same treatment is not given to application developers, SQL database administrators, and project managers who log in to production servers. These employees are only given one user account and when they log into a server, it will insert the local computer administrator group, now giving access to an additional 10-15 employees who do not need to access the PeopleSoft, compensation, and customer database servers.

The only way to prevent this is to remove it from the logon script. Separate your servers and computers of your key personnel from your average users and use Group Policy to make this insertion only on the average users, or use the built in administrator account to log into the computer, after all, everyone in the client

support group knows the password.

**Naming Conventions**

When your organization decided on a naming convention, the decision makers probably had little mind of security and solely made their decision on convenience. Many organizations deploy a naming convention for workstations that consists of a combination of a site code, laptop/desktop, user name, floor number, and department. For servers it is usually a combination of site code, server role (mail server, application server, database server, file server, print server) and a sequential number. By browsing the network using "My Network Places" and seeing a computer named "bos07taxrclark", even an outsider to your organization would be able to determine that this computer belongs to the domain user RClark in the Tax department, and that this person works in the Boston office on the 7th floor. This gives a map to an attacker for seeking out key employees in the Tax, Legal, Human Resources, Payroll, or Executive Management to copy confidential documents from their computers. If an employee or contractor has the local administrator password, or belongs to a domain group providing administrator access, they would be able to quickly identify key personnel computers and copy sensitive information from the computers.

**Shared Folders**

Shared folders are a way for multiple users to access the same resources (data) after all, this is the most basic reason to have a local area network in the first place. There are two types of shared folders, public, which are network shares that reside on a server and accessible by everyone in the organization, and private, which are individual shares that reside on a user's computer and intended for just a few other employees. In some organizations you may also have department shares, which reside on a network server but are only accessible by certain departments or groups to give availability to data, as well as the ability to take advantage of larger amounts of storage space. An example would be that the database administrators have a department share that the SQL backups get stored, or the Human Resources department has a department share to place sensitive documents that need to be accessible by the entire department.

If you have to sum up shared folders, it would have to be convenience and availability. From the lowest-level user to the highest-level administrators, they all use and abuse network shared folders when it comes to data storage. If you search through your organization's public network shares you will more then likely find software installation files, Microsoft Outlook .pst files, backups of user's desktops, software images, and application and database backup files, all of which may leak personal or sensitive information.

While public network shares are readable by everyone, it is not often that users intentionally store sensitive files on them, but rather place these files in individual shares that are only accessible by a few individuals. There are a few ways that these private shares get abused and the information is made available to others that should not have access to it. The first is when a user sets up a share. By default Windows will add the "Everyone" group to be able to access the newly shared folder. Unless the user removes this group and explicitly adds the desired users account, it will allow anyone on the domain to be able to access your information as long as they know this share exists. How does someone know you have a shared folder on your computer? The easiest way is to use a software probing tool such as GFI's Languard which can be downloaded for free at http://www.gfi.com/pages/files.htm. Languard will identify any shares that exist on the network and will provide you with a detailed list (8). If you do not want to tip off your network intrusion detection system (IDS) with a tool such as Languard, you can simply open up "Network Neighborhood" or "My Network Places", depending on which version of Windows you are using, open the Windows Network and manually click on each workstation or server in your network looking for exposed shares with sensitive information stored inside them.
If you do manually search for shared folders using this method, you may not see them, but they can still exist. By default, the entire C:\ drive is shared for administrative purposes, however it is hidden and only accessible to administrators. By placing a dollar sign at the end of a share name, it will hide the share, making it not viewable by browsing. One way to identify a hidden share is by typing in the server or workstation name into the run command followed by c$, for example: \\servername\c$. If you have administrator access to this server, or someone added a domain group to which you belong to the share, a window will display with all of the folders on the C:\ drive. If you do not have access, an authentication window will display, prompting you to enter a user name and password of an account that does have permissions to access this share. Server engineers typically set up the C:\ for system files only, and the D:\ is where the application data is stored. By entering \\ServerName\D$ into the browser, you may be able to expose critical data on production servers thought to be hidden. Some shares are visible but won't contain any critical data, however, check to see if the write or execute option is allowed to everyone. This could allow a denial of service attack if someone used a disk writing utility that would write bogus data to the drive, causing it to write to all available space, which would eventually cause the server to crash.

Some of the largest abusers to the private shares is the client support group. The client support group will generally set up department shares with convenience in mind for installing software, troubleshooting, or imaging a computer for replacement or operating system upgrades. They will also set the permissions for most of these shares to allow read, write, and modify to all users in the domain. By calling the organization's help desk and requesting the installation of software, instead of a technician coming to a desk, a technician

will point the user to where the software is located and provide verbal instructions on how to install the software. This provides the user with immediate assistance and can allow the higher paid client support technicians to concentrate on higher level service calls. While it may not be a concern to store software for Blackberry, CD/DVD drivers, and SpyBot, it is a concern when Server software, VPN, ADP, and PeopleSoft installation files are located. You may also find licensed software such as Windows operating systems, Outlook, Visio, and Project. Not only will you find the installation files, license keys written in text files, but supporting documentation on how to install it, the application and database servers to connect to, and test accounts to log into the application to test the software installation.

**Putting it all Together**

Each of the topics above is a risk by themselves, but when you begin to combine them, the threat rate increases exponentially. By browsing the public shared folders on the network drives it may leak enough information to tip off someone about how business is conducted at your organization and how it is departmentally organized. If an insider on your network has access to the local administrator password, and navigates through the "My Network Places" to browse your network, they can identify computers that belong to key personnel. Once the reconnaissance effort is over, the attacker can begin copying sensitive documents from their computers.

Another leak is from the shared drives set up by the client support department. Whether these drives are on a private, a public, or a hidden share, they are still available and can be located by calling the help desk to get access to the software shares. Windows also caches this information through the "Run" command box. By clicking on Start, then Run, and then on the drop down box, previously accessed paths of the shared folders are stored from the last time a client support technician installed software to your computer.

From a risk mitigation perspective, locate subfolders which reveal software such as KillDisk and Ghost. For efficiency purposes, organizations are using Norton's Ghost to image computers with a corporate image, loading all of the needed, and in many cases, unneeded software onto a new computer. This software is so efficient that instead of spending time researching and troubleshooting an Operating System error, the client support team will in many cases re-image the computer. Inexperienced support groups find it takes less down time for the user, and less support time for the technician. The drawback to this is the client support team will use Ghost to make a backup to one of their shared folders, then re-image the computer. They save this backup for a few days on the shared folder until the system has been tested and properly functioning, leaving the image of the computer residing on this share. An inside attacker could locate the client support software share, locate the software to install Ghost, then find images of employees computers and use Ghost to install an exact

copy of the files of their computer to a computer of an attackers choice. Using bootable CD's mentioned above in the Physical Security section, it will allow an attacker access to any file on the computer.

In the above two situations, data is exposed on a one by one basis, leaving inside attackers to probe for bits and pieces of information that can be put together to cause a severe exposure, or possibly leverage a sought out individual attack on another employee. An organization may have an employee who was passed over for promotion, feels they are being treated unfairly, or simply wants to make a case against somebody, and will use the above steps to collect information. An attacker who wants to cause damage to the entire organization is going to target the production servers and attempt to collect employee and customer information, or cause a denial of service interruption to your Internet and database servers.

**Summary**

The topics that I have covered are items that can provide realistic opportunities to an insider to attack your organization. They are items that are given very little attention in day-to-day operations, put behind projects that focus on external security such as patch management, anti-virus, firewalls and intrusion detection systems. It is up to you to implement policies that prevent unauthorized access and shared files to critical infrastructure servers, removing the availability of software from the network drives, securing images of employees computers which contain confidential documents, and changing the local administrator password, or disabling the account altogether. By auditing these areas and enforcing these policies, you will reduce the exposure from internal threats.

**Works Cited List**


1. 10 Immutable Laws of Security Administration. Scott Culp. November 2000 http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

2. High-Profile Thefts Show Insiders Do the Most Damage. John Pescatore. November 26, 2002. http://www3.gartner.com/DisplayDocument?doc_cd=111710

3. 10 Immutable Laws of Security. http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx

4. Run Windows XP from a bootable CD-Rom or DVD with GUI and network support. Bart Lagerweij. November 3, 2004. http://www.nu2.nu/pebuilder/

5. Social Engineering Fundamentals, Part I: Hacker Tactics. Sarah Granger. December 18, 2001. (http://www.securityfocus.com/infocus/1527)

6. Microsoft Sill Rules the Market. Matt Hines. October 8, 2003. http://news.com.com/Microsoft+still+rules+server+OS+market/2100-7344_3-5088233.html

7. Generally Accepted Principles and Practices for Securing Information Technology Systems. Marianne Sawnson and Barbara Guttman. September 1996. Page 30. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

8. GFI. http://www.gfi.com/lannetscan/

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |