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.

Mitigating Insider Sabotage

Companies and organizations tend to focus on the exterior threat to their network infrastructure. A rising threat is that of the disgruntled insider. This highly sanitized case study will show how failing to create an effective termination policy and deploy correct user access controls to deter insider sabotage can be costly. It will show that companies and organizations need to focus equally on physical security technologies and information security practices.

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Mitigating Insider Sabotage

GIAC (GSEC) Gold Certification

Author: Joseph Garcia, garcia.josephj@gmail.com
Advisor: Egan Hadsell

Accepted: September 21, 2009

Abstract

Companies and organizations tend to focus on the exterior threat to their network infrastructure. A rising threat is that of the disgruntled insider.

This highly sanitized case study will show how failing to create an effective termination policy and deploy correct user access controls to deter insider sabotage can be costly. It will show that companies and organizations need to focus equally on physical security technologies and information security practices.

© SANS Institute 2009, Author retains full rights.

1. Introduction

Intruders and "hackers" are perceived as ready to compromise information systems and steal valuable customer/proprietary data at any time. News reports showing major data breaches are making a lot of headlines recently. With stories such as the one of Albert Gonzalez, who had penetrated the likes of TJX Companies Inc., Heartland Payment Systems, Hannaford Brothers and 7-Eleven (Zetter, 2009). Since some of the original TJX breach reporting (Wilson, 2007), there has been a constant stream of news items that connect to that event. In March of 2007, it was reported that TJX had approximately 45.7 million credit card numbers stolen, as well as driver's license and other personal information (SearchSecurity.com Staff, 2007). In August of 2008, 11 people, lead by Albert Gonzalez along with Christopher Scott, Damon Patrick Toey and eight foreign nationals, were charged in connection with the TJX case (Lemos, 2008). In May of 2009, it was reported that Heartland had paid out $12.6 million dollars to that point in response to its breach, more than half of which was for fines leveled at them (Kaplan, 2009).

Cases like the TJX one show that as time goes on cybercriminals are getting more organized. With that, security for organizations needs to get tighter. In 2008, Computer Security Institute conducted a survey of 522 computer security practitioners. The respondents were from government agencies, corporations, universities, financial and medical institutions. It showed that 94% of the respondents used firewalls, 97% use anti-virus software, 51% used log management software, 69% used intrusion detection systems and 54 % used intrusion prevention systems (Richardson, n.d.). These numbers, although a sample of the security community, probably give a fair representation of how data security is handled throughout the industry.

Even though "hackers" are out looming on corporate security perimeters, insiders will always be a large threat to an organization. They have access to critical resources, both physical and digital, in their workplace. This is beginning to become more apparent in today's economic environment, where companies are forced to down size in order to

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

meet budgetary requirements. The number of disgruntled former employees is on the rise. There are those employees who, in the face of upcoming financial problems, will look to cash in by selling their former employer's intellectual property. In a survey conducted of 400 senior IT professionals, there was a sharp rise in the percentage of respondents that would take proprietary data in 2009 compared to 2008 (Cyber-Ark Software Inc, 2009). Their responses were as follows:

Type of Information	**2009**	**2008**
Customer Database	47%	35%
Email Server Admin Acct.	47%	13%
M&A Plans	47%	7%
Copy of R&D Plans	46%	13%
CEO's Password	46%	11%
Financial Reports	46%	11%
Privileged Password List	42%	31%

Table 1: Cyber-Ark survey results

It is not only the employees who are willing to steal data though. There are also the employees who are just looking to exact their revenge by destroying data and vital computer equipment. In a report by the Carnegie Mellon CERT which analyzed 190 insider threat cases, they showed 80 of those cases were linked to IT sabotage between 1996 and 2007. Of those 80 cases, 75 of them were not linked to financial gains by the saboteur. More than half of the insiders were seen as disgruntled and most acted out due to a negative event in the workplace. The report showed 30% used their own username and password and 24% used another employee's login credentials (Capelli, Moore, Trzeciak, Shimeall, 2009). Reports of data sabotage seem to be becoming more frequent. Let us look at the following three examples:

A Jacksonville, Florida woman named Marie Cooley who worked for an architecture firm, believed that she was going to be fired after seeing a classified job advertisement for a similar job at her company. She entered her place of employment on

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

a Sunday evening, deleted seven years worth of data and pulled network cables causing system downtime. The data deleted by Ms. Cooley was estimated to be valued at approximately $2.5 million dollars and included designs and drawings belonging to the firm. Marie Cooley is facing up to 5 years in prison for her actions (Washkuch, 2008).

On November 5th, 2005, Danielle Duann, a former IT director for an organ donation center, was fired from her position. The center was the sole provider of organ procurement services for more than 200 hospitals. On November 7th and 8th of 2005, she gained remote access to her former employer's network. She then proceeded to delete numerous database files and software applications, as well as their backups. She tried to conceal her actions by disabling logging functions on the servers and also erased the logs that recorded her remote access. The financial loss to the organ donation center was approximately $94,000. Ms. Duann is facing 10 years in prison and fines up to $250,000 (Gross, 2009).

There are also the disgruntled ex-employees that were terminated due to poor performance and are now facing the hardship of finding a job in a terrible job market. A case that made the news that fit into this category was that of Jon Paul Oson. He sought revenge after getting a poor job evaluation. He was hired in May of 2004 by a nonprofit group, which provided support services to 17 clinics in Southern California. A few months later, he was promoted to technical services manager. In October of 2005, he received his unfavorable evaluation and promptly resigned. On December 23rd of 2005, he logged into the servers of his former employer and proceeded to disable the backup program, which archived the medical records for thousands of patients. Six days after that, he logged back in and deleted patient appointment data, medical charts and assorted other files. He was able to accomplish this within a 43-minute span. Oson was sentenced to 63 months in prison and was ordered to pay more than approximately $409,000 in restitution (Goodin, 2008).

An employee may show signs that they have the potential for sabotage. What if they don't show that potential? Maybe that person did not have problems with another

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

employee in the workplace. Maybe their financial situation at home was fine. Maybe they were treated well by their superiors and he or she were the model employee until the day of their termination. How does a security professional protect against this scenario? There are certain safeguards that can be put in place that can help mitigate the damage done by an inside attack and help minimize operational downtime. This can save a company or organization money and man-hours better spent elsewhere.

2. Background

In the winter of 2009, the security supervisor for a large medical center, "General Hospital", had contacted the local police department's computer crime unit regarding computer tampering. They reported that approximately 21,000 of the hospital's Accounts Payable bills were deleted from hospital computers without permission. There were no backups of data available that would have helped get Accounts Payable back up and running with minimal downtime. This caused the hospital approximately $30,000.00 in data recovery fees. There were also "man-hours" used by staff members to help correct this situation, which would have been better served for its original purpose. Further, if certain bills had gone unpaid by "General Hospital", over time, shipments of crucial supplies and medications used by the center on a daily basis would not have been delivered. Now, here are the details of this case study.

The hospital's security supervisor stated, that in the hospital's effort to become ecologically sound, they hired staff members whose job it was to electronically scan Account Payable bills into storage on a computer server and then to recycle the paper. The Accounts Payable department had ten staff members and one supervisor to carry out these duties. Work days, were from Monday through Friday and hours were from 9:00 am to 5:00 pm. Upon being hired, employees would be assigned to a computer workstation and given a login username and password, as well as a photo identification card. In general, the supporting departments of the facility were closed on the weekend but certain departments did have members that would come in to perform certain duties in an overtime capacity. This was not a widespread practice and was mostly used by staff that had a deadline for completed work. They had to sign into and out of a "weekend"

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

logbook, which was kept at the security dispatcher's desk. Other employees may have just needed to pick up property left behind during the regular workweek. In this case, an employee did not have to sign into or out of the logbook. In either situation though, if an employee needed to enter the building on a weekend, they needed to call the security dispatcher and request that a patrol officer open the building for them. The responding patrol officer would inspect the requesting employee's identification card and if it were valid, the employee would then be granted access and the doors would be locked behind the employee. In order to exit the building, the dispatcher needed to be called again, a patrol officer would respond back, open the building and lock it immediately after an employee exited. Calls to the dispatcher were digitally recorded and archived on a daily basis. There was no Caller ID information available for the recorded line.

The security supervisor then explained that on a particular Tuesday afternoon, it was discovered by the Accounts Payable department's supervisor that approximately 21,000 files were missing from the department's database. This was due to the supervisor looking to pay a recurring bill that was due approximately the same time each month. When he could not find the file, he conducted a query of the Accounts Payable department's database, based on the number of deleted files, by employee, for a one-month period. The report showed a typical amount of deleted files from most staff members, ranging from five to fifteen files in a month's time. Most deletions occurred when errors were made and rescans needed to be done. Two staff members though, showed an exorbitant amount of deleted files. For the purpose of this paper, they will be named "Amy" and "Mary". "Amy" had deleted approximately 18,000 documents from her workstation and "Mary" had deleted approximately 3,000 documents from hers. Another query showed that the deletion of files by "Amy" and "Mary" were conducted on one Sunday morning during a two-hour period. The Accounts Payable supervisor informed the security supervisor, that "Amy" has been employed with the center for ten years and has never had any disciplinary issues to date. "Mary" though, had been employed with the medical center for two years, but was just recently terminated the previous Thursday for insubordination and for failing to perform her duties.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The Accounts Payable supervisor stated that "Mary" had a falling out with another staff member earlier in 2008 and they began to fight and argue on a regular basis. He stated that after he intervened, they had agreed to stay away from one another and limit their interaction with each other. For some reason, they began to fight again and "Mary" initiated most of the fighting. Then on a Thursday, she began arguing with her co-worker with "Mary" pushing the other employee. Upon her supervisor confronting her, "Mary" became belligerent, started cursing at everyone and refused to go back to work. After failing to get "Mary" to go back to work, he brought her into his office and informed her that she would be terminated and be escorted from the facility. He also informed here that she was not allowed to re-enter the facility ever again. He had requested her identification card be returned. "Mary" told him that she left it home that day. The Accounts Payable supervisor then informed her that he would instruct Human Resources not to release her final paycheck until her identification card was received by certified mail. She was then escorted from the facility.

The security supervisor stated that there were no video cameras installed at any of the facilities of "General Hospital". He did state though, that they had call capture software for recording incoming phone calls to the dispatcher's station. He states that he reviewed the dispatcher call archives for the Sunday in question and found three calls for the day. The first was a female requesting access to the building, which housed the Accounts Payable department. The second was the same female requesting to be given access to the building. Finally, the third call was a request from the same female, to be let out of the building. He interviewed the security officer who responded to the requests. The security officer stated that "Mary" was the requestor, that the he knew her to be an employee of the facility for the past two years and that he gave her access to the building. The security officer also informed the supervisor, that he was also the patrolman to respond to let "Mary" out of the building. The supervisor also reviewed the weekend logbook and found only one person signed into it. It was an attorney for "General Hospital", who had been employed at the center for approximately twenty-five years without incident. It was a regular occurrence for him to come to the facility on a Sunday in order to prepare for the coming workweek. He had never failed to sign into the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

"weekend" logbook.

Through eyewitness accounts and statements made by "Mary" during interviewing, she was placed under arrest and charged with Burglary, Computer Trespassing and Computer Tampering.

3. Assessment

To this point, the overall story of this case study has been detailed. During the investigation conducted by the local police department's computer crime investigators, flaws in "General Hospital's" security policy were discovered. The risk to the information kept by the Accounts Payable department was high. This was due to two factors. The first was the threat of having too many employees having unrestricted access and rights to critical information. The second is the vulnerability of the information kept due to poor physical security and computer password/usage policies.

There was no single security solution available to make the Accounts Payable department database more secure. A defense-in-depth approach should have been applied at this location. The thought process behind defense-in depth, is that it is harder to defeat multiple layers of protection than a single barricade. An information centric approach would be the best fit for the Accounts Payable department's needs. You can think of this as the information you are trying to protect at the center of a set of concentric rings (Northcutt, 2007). A new ring is added for each layer of protection instituted. To help visualize this, see the below diagram:

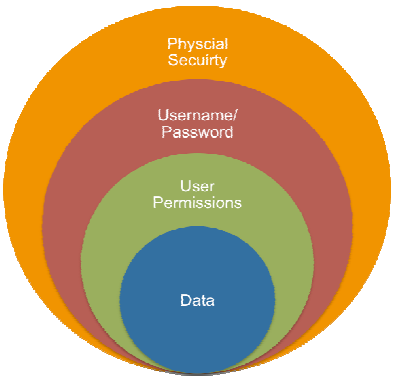


Figure 1: Information Centric Defense-in-Depth

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The following three sections will focus on the areas breached during the Accounts Payable incident. Each area will be addressed in order of its breach. In addition, they will include the recommended solutions to fix them.

4. Physical security

Physical security has existed in various forms for thousands of years. It is meant to deter an attacker from gaining access to a physical location such as a military installation, home or office. It can also prevent an attacker from accessing a resource such as an ammunition cache, personal belongings or in this case, data. Some examples of physical security are sentries, guard dogs, a moat surrounding a castle, mine fields, barbed wire, burglar alarms, smart cards and video surveillance. It is generally the first line of defense against an attacker, but it can also be layered. Meaning, that if an attacker penetrates one area of defense, the next may defend strongly enough to impede them or turn that attacker away. The following section will show, how a poor physical security policy led to a successful physical security compromise against "General Hospital".

4.1 Physical security failings

As was mentioned earlier, a security patrol officer responded to the request of a female caller to be given access to the facility. Upon his arrival, he observed a female, whom he recognized to be "Mary" from the Accounts Payable department. She originally informed the dispatcher that she was going on vacation and needed to make sure that documents she was working on were complete for her supervisor prior to leaving the city. Since he recognized "Mary", the patrolman unlocked the door and allowed her access to the building. He never asked to see her identification card at any time, nor did she offer to show it to him. Once inside, "Mary" not only had access to her former department, but approximately six others. There were no interior security controls in place to prevent access to each of the seven departments other than a glass door with a single lock. If "Mary" had been an identity thief looking to steal personal identifiers, the complacency of the responding patrol officer just put all of "General Hospital's" employee's at risk. In addition, this could have cost the center approximately half a

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

million dollars in credit protection services paid out to the approximately 5,000 employees of the center.

The calls made to the dispatcher's station were digitally recorded and archived on a daily basis, but there was no Caller ID information available for the recorded calls. If all that this investigation had to tie a phone conversation to a suspect were the phone calls, the lack of Caller ID would be a hindrance. Furthermore, there were no video cameras in place at the facility. In a building which housed the legal department, billing and patient records, reasonable persons would believe that this location would be (or should be) under video surveillance.

The next section will detail the recommendations made to "General Hospital" with regards to improving on their physical defenses.

4.2 Physical security technologies

There were a few holes in "General Hospital's" physical security defenses. The first was regarding their use of generic photo identification cards. These are an unacceptable form of identification when it comes to protecting such data as patient information, billing and accounts payable records. In this case, all it took was a single factor of authentication to get access to a "secure" facility- the "who you know" factor. Just because the security guard recognized "Mary" and knew she worked in the building, he felt it was all right for him to allow her access, no questions asked.

This is where contactless smart card technology comes in. These cards can be programmed with personal, employment and biometric data, which is stored on the card's chip. It will also contain data regarding which access points the cardholder can and cannot enter. Additionally, they can work with different types of card readers. It was recommended to use contactless smart cards combined with a card/fingerprint reader for main entrances and card readers for interior access points. Various vendors offer software templates that allow for the customization of the smart card. The smart card can have printed information on it such as organization's logo, background image, employee

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

name, photograph and name of the employee's facility department on its face. Another feature to employ could be to periodically change the background image on the card. That way if someone attempting to access a facility with an older card they can be detained until their access status is sorted out. The information printed on the cards can be used by security to challenge an employee for their credentials while in a certain part of the facility. For example, an employee may be in an area of the facility during business hours that they do not belong in, such as a telephone closet, and get discovered during a security sweep.

To gain access to the main entrances to any of their facilities would require two-factor authentication: who you are (fingerprint-biometric) and what you have (smart card). Without both, access would not be granted. Contactless smart cards are used in conjunction with smart card readers and a host terminal. More than likely, the access point would be either a half height or full height turnstile. When an employee places their contactless card next to the card reader, it will transmit to a host terminal. A database record on the host terminal would be accessed using a numeric identifier and will point to a database record containing information on the employee, including biometrics. If the database shows the employee record as valid, the person will then have to place a designated finger onto the fingerprint reader. The biometric information is then transmitted to the host terminal. If the fingerprint that was placed on the reader and the numeric identifier that was originally transmitted from the card's chip match the data in the database record, access it granted. Now once someone has gained access to a facility, it does not mean that they are allowed to enter any department's office they wish. It was also recommended that contactless smart card readers be placed at the main entrance to each department. This way, if someone has only been granted access to the Accounts Payable department, that information would be programmed into their database record. Then, if they attempted to gain access to the legal department, patient records, etc., the card reader would reject the card and the door would not unlock. This type of system can also be set up to log when someone has gained access to and exited from a facility/department.

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

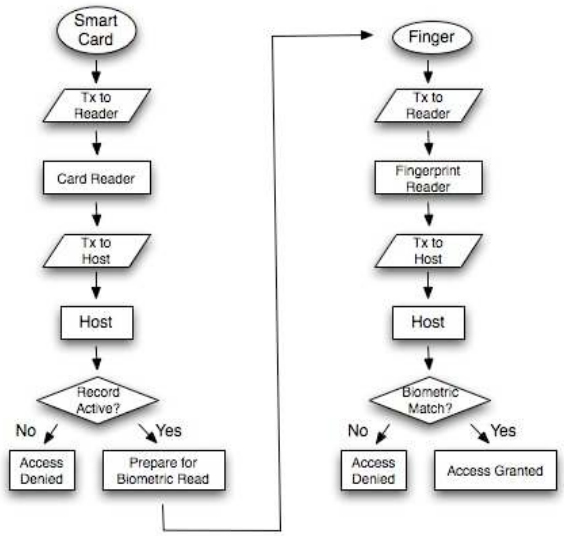


Figure 2: Access authentication with a Contactless Smart Card/Fingerprint Reader

Should "General Hospital" follow the recommendation of a revised termination policy, as mentioned in section 7.1, in addition to the use of smart card technology, once security is advised of an employee's termination they can shut down the former employee's building access. Part of the new policy would be that if a card/biometric reader denies an employee, a security officer would have to contact human resources to determine that person's employment status. If human resources conclude that the person is a current employee, access is granted. The contactless card database would need to be updated regularly to ensure the database's integrity. If human resources department reveals that the person has been terminated or has resigned, then security would perform an initial investigation as to why this person is trying to access the building. Local law enforcement may also need to be called at that time.

Also, as mentioned previously, there were no video surveillance cameras on site at "General Hospital". If "General Hospital" did not have the policy of sending security personnel to respond to open a building when requested by another employee, they would have no other way to identify someone entering a building. If someone gained access to a building via an entry point illegally, no alarm would have sounded and no security officer would have responded. How would they be able to identify if someone had entered the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

building? They couldn't. It was recommended that "General Hospital" deploy video surveillance cameras on entry and exit points of their buildings, their server rooms, and any office which may contain business or patient records and the garage. It was also suggested that they consider deploying surveillance to critical infrastructure items such as electrical, water, heating and cooling controls.

A good idea from the Center's security team had been the use of phone call capture software. The only problem was that software that had been deployed at the security dispatcher's desk was inadequate. The security supervisor had commented that he requested a better version of the software, which included Caller ID, but was turned down for budgetary reasons. He stated that the software they were using was approximately 2 years old and outdated for their needs. Most of the current call recording software programs cost in the $40-$50 USD range and some are available cross platform for Windows, Mac and Linux. This is where a security professional must step up and show his/her employer that the Return on Investment (ROI) for a $50 piece of software will pay for itself in the future.

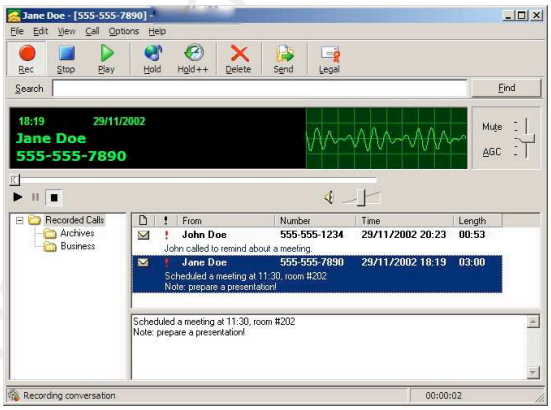


Figure 3: Sample screenshot of phone call capture software (Callcorder.com, 2009)

Adding the above recommendations to "General Hospital's" existing physical security policy would not only cut down on unauthorized physical access dramatically, but would also help to identify a possible perpetrator.

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

5. Passwords

Passwords are the keys that are used to access a computer and the information stored on a computer. Regarding computers, Merriam-Webster defines a password as "Something that enables one to pass or gain admission: as: a sequence of characters required for access to a computer system" (Merriam-Webster Online Dictionary, 2009). The Computer Desktop Encyclopedia goes a bit further to define a password as "A secret word or code used to serve as a security measure against unauthorized access to data. This is normally managed by the operating system or Database Management System. However, the computer can only verify the legitimacy of the password, not the legitimacy of the user" (Computer Desktop Encyclopedia, 2009).

By co-workers sharing passwords and by management allowing them to go unchanged without recourse, it is essentially giving away the keys to the digital information kingdom of an organization.

5.1 Password sharing and misuse

When "Mary" was hired for her position with "General Hospital" in the Accounts Payable department, she had been assigned a computer workstation, but no login username and password. She was informed that the "tech guys" would take a couple of weeks to get them assigned to her. In the meantime, "Amy", who had been employed by the Center for approximately eight years, took "Mary" under her tutelage and tried to help get her some basic training in her job functions. Since "Mary" did not have a login username and password, "Amy" let "Mary" use her login credentials. She also allowed "Mary" to use her workstation to get some of her work done in the meantime. About one month later, "Mary" finally received her own login username and password. When interviewed by the computer crime investigators, "Amy" stated that she had the same login username and password for approximately two to three years. "Mary" had written down "Amy's" username and password in case she needed them later.

5.2 Effective password policy

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

If information security is important to an organization, then having an effective password policy in place is crucial. Along with security awareness training (see Section 7.2) to help educate employees on the techniques of social engineering, strong password construction is paramount to that policy.

Some examples of weak passwords are:

- Contains real name, user name, pet's name
- A dictionary word (e.g., House, dog, car, etc…)
- No password
- Strings of characters (e.g., 12345 or abcdefg)

Strong passwords contain some of the following characteristics:

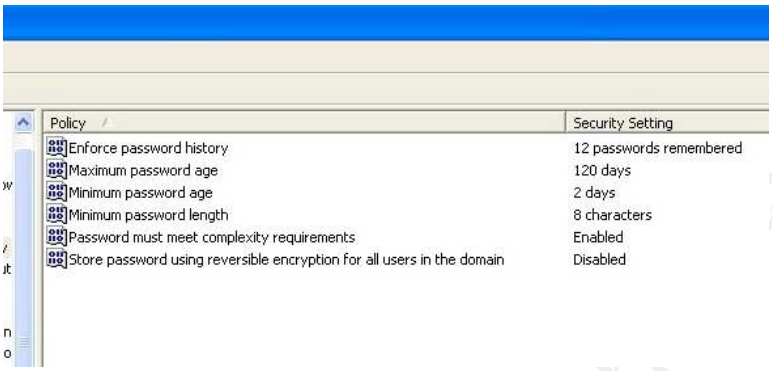
- Contains both upper and lower case characters (e.g., a-z, A-Z)
- Contains digits and symbols (e.g., 1, 2, 6,9,), !, @, #, ?)
- Are 14 characters or longer
- Created from a passphrase

Creating a passphrase can make a password easier to remember without compromising its security. This will also help an employee avoid having to write it down and keep it within their workspace (like the concept but the sentence is long and awkward; either reword or remove the last part. Creating an example passphrase using the framework for a strong password listed above, using J@ck&j1Llr0cK! is a much better choice than just using jackandjillrock. Once rules are in place for the creation of strong passwords, it must be decided how to protect passwords from being compromised or having an attacker use one to compromise the information systems. For example:

- Account lockout threshold (how many times an invalid password is entered before being locked out)
- Lockout duration
- Reset after lockout
- Password history
- Maximum password age

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

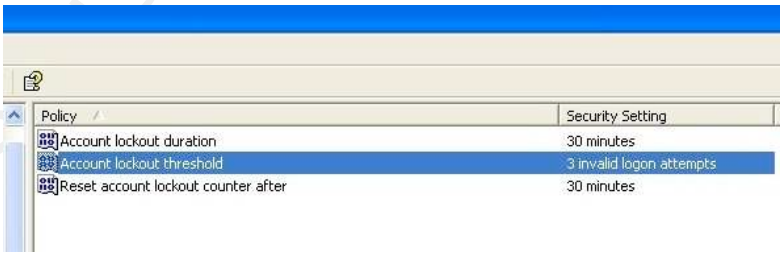
Using the Microsoft Management Console (MMC) and adding the Group Policy snap-in, you can access the Group Policy settings. Access the Password Policy controls from Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. You will see the following:



Policy	Security Setting
Enforce password history	12 passwords remembered
Maximum password age	120 days
Minimum password age	2 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Figure 4: Password Policy settings

As seen above, you can change the settings for password history, maximum password age, minimum password age, minimum password length and password complexity. The last setting in the Password Policy is store password using reversible encryption for all users in the domain. This setting is disabled by default and for good reason. It actually stores the password in clear-text and should not be used unless absolutely necessary. The next policy to consider changing is the Account Lockout Policy. This policy controls the settings related to users (or attackers) attempting to login to the network and entering incorrect passwords. To access the Account Lockout Policy in the MMC, go to Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy and one will see the following:



Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Figure 5: Account Lockout Policy settings

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

With these settings you can set how many times a user can attempt to login with an incorrect password before being locked out of the system. Also here, is the account lockout duration. This determines how long the account will be locked out for until a user can attempt logging in with a correct password. Finally, there is the reset account lockout after setting. This setting determines the amount of minutes that must pass before the bad logon attempt counter resets to 0. This setting must be set to a time less than or equal to the account lockout duration.

Once the above details are determined, it is then time to decide on a plan to protect passwords that are used within an organization. An organization's written password policy should contain rules as to how passwords should and should not be used. It should also include what disciplinary action may be taken if the policy is violated. See Appendix A for an example of what the password policy for "General Hospital" should be modeled to look like.

6. Permissions

User Permissions are defined by the Computer Desktop Encyclopedia as "The authorization given to users that enables them to access specific resources on the network, such as data files, applications, printers and scanners. User permission also designate the type of access; for example, can data only be viewed (read only) or can they be updated (read/write)." (Computer Desktop Encyclopedia, 2009). This means, once it has been determined who can have access to organizational resources, it then has to be determined how much access to those resources they are given.

Users are typically given more access than is necessary to perform their daily tasks. In the book "Insider Threat" by Dr. Eric Cole and Sandra Ring, it states, "The access that someone has contains at least 35% more access than what is actually need to perform their job function. Most compromises are caused by someone using that additional 35%, which means if we took away the access that is not needed, we would be taking away the access that is utilized to cause harm" (Cole, E & Ring, S, pp. 334-335,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2005). By using the Principle of Least Privilege, which is also known as a "Need to Know" basis, you give users the access they need and not the access they don't. Below is a diagram that illustrates how access is typically granted. It is interpreted from an illustration in the book "Insider Threat" (Cole, E & Ring, S, Figure 9.1 Granting Access, p. 334, 2005).

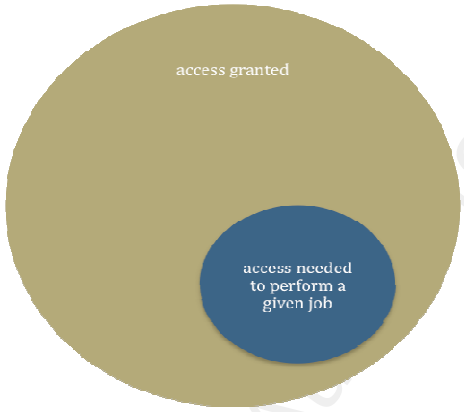


Figure 6: Granting Access

Here is a question. If you have an employee who handles the delivery of mail to other employees and company executives, does he need a key to the CEO's office if he is just supposed to give the mail to the CEO's secretary? The answer would be a resounding no. So to make this fit for this particular case study, if you have an employee who is there just to do data entry, does that employee need to have the right to delete entries? Does he or she even need the right to take ownership of files and folders? That would be a resounding no. So why give someone that kind of access in the first place? Is it ignorance? Is it laziness? Whatever it is, it needs to be corrected in order to have a sound information security policy in place where data sabotage can destroy a business or organization.

6.1 Lack of permissions control

Once "Mary", or anyone for that matter, was given access to the account payable database, she/they had the ability to create, edit and delete any document that existed in that database. A user would not have had to make any request- written, verbal or

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

otherwise. A user would be able to do what they wished at will. There was also no digital spreadsheet or even a handwritten log to detail when files were deleted. There were no regularly scheduled audits of the database in place and the original discovery of deleted files was discovered by accident. It was unknown when a query regarding the amount of deleted files was last conducted. What if "Mary" had access to other critical assets on the network without having proper permissions set for her user account? What would be the extent of the damage that could have been inflicted by "Mary"? Now, lets look at how having the proper permissions set for a user could have helped "General Hospital" protect their assets.

6.2 Proper user permissions

When planning to set up how permissions will be applied, it is important to determine what access is needed for an employee to do their daily work. The most infamous standard of permission is Full Control. This is what most people want, but not what they actually need and only a few people should have. A user that is assigned Full Control permissions will have the ability to do whatever they wish: Read, Write, Create and Delete. NTFS does allow for the use of special permissions though. Some examples of these are: Read Attributes, Write Attributes, Create Files/Append Data, Delete, and Read Permissions. These are more granular controls that as they combined are with each other to help form the required permissions.

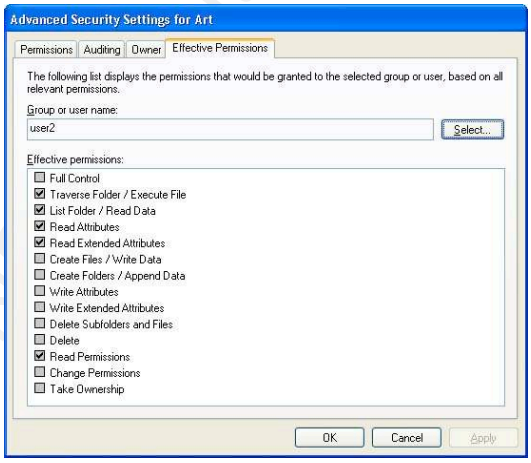


Figure 7: Example of NTFS Special Permissions (Microsoft TechNet. 2009)

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

When assigning permissions, it is helpful to create groups of users that require similar access to resources and then apply permissions to the group instead of individual users. It is also important not to explicitly deny a user. This is due to the fact that if they have certain rights to other resources on a network and then those rights are denied on another part, the denial will supersede all other permissions. It is best to deny rights by not clicking to allow them. For "Mary", what should have occurred was "Mary" to be created as a user on "General Hospital's" domain. An "Accounts Payable" Organizational Unit should have been created under "General Hospital's" domain and had a Group Policy applied to what rights would be necessary for that OU (Read and Create). Then "Mary" would have been added to that OU and whenever accessing the resources of the "Accounts Payable" OU, the Group Policy would take effect. This way, if she had full control in another OU, this would not affect "Mary's" use of that OU.

Also, a restriction that could have been placed on "Mary's" user account would be that of Logon Hours. By default, users are allowed to logon at any time. When a user account is created, by going to Start > Administrative Tools >Active Directory Users and Computers and right clicking on "Mary", then click Properties > Account > Logon Hours, an administrator arrives at the Logon Hours dialog box. It is here that the days and times which "Mary" or any other Accounts Payable user could have their logon hours determined. The best setting for an Accounts Payable employee would have been Monday through Friday, from 9 am to 5 pm. With that, "Mary" would not have been able to access the Accounts Payable computers and delete files. Since "Amy's" user account would have been set the same way, "Mary" would have had the same results.

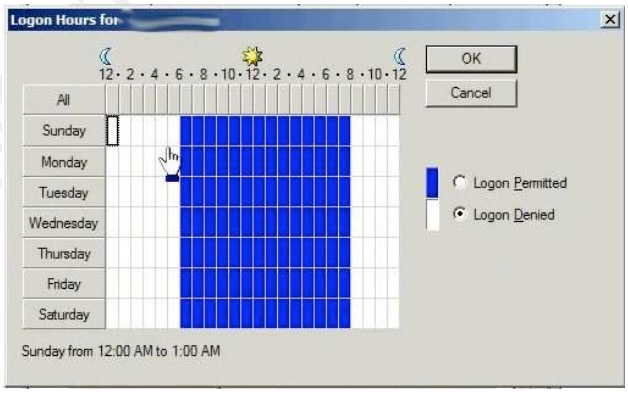


Figure 8: Sample screenshot of the Logon Hours dialog box

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

7. Additional policy recommendations

The previous three sections covered the policy fixes that were recommended to "General Hospital" to address the specific issues that were involved in this incident. Those issues led to the deletion of vital data. This section will now deal with the additional recommendations that were made to build upon that foundation.

7.1 Termination procedure

As was seen in this case, "Mary's" supervisor was carrying out the center's termination procedure upon his decision to release her from her duties. While she was being terminated, she had her personal belongings boxed up by security and was eventually led out of the building. She was informed never to return to the building again. While being led from the building by security and given a stern warning is ok, it is obviously far from good enough. Questions immediately come to mind. Why was she able to enter the facility after her termination and without an identification card? Also, why wasn't a security supervisor or the IT supervisor ever notified upon her termination?

"Mary" was able to enter the building without being challenged for her lack of employee identification, both the day of her termination and the date of this incident. Not only did her building hold the Accounts Payable records, it also housed employee records. It was recommended that a security supervisor must be notified of or present at an employee's termination. Once notified (or present), the employee is added to a list of terminated employees. A copy of this list would be generated and left at all security stations. The list should contain pertinent information such as name, date of birth, date of termination, former department, as well as a photograph for identification purposes. This would make the patrol officers and radio dispatchers aware of who does not belong in any part of the facility. Also, this list would contain contact information for a Human Resources representative that could be used to verify the list against employee records. Furthermore, when combined with the smart card technology that was recommended in section 4.2 of this study, security could have terminated "Mary's" access credentials to the building. This would have made entering the building and offices much more difficult to achieve by the saboteur.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

It was also recommended that a mandatory notification be made to the IT supervisor upon an employee's termination as well. In this situation, if IT would have been notified, they could have terminated "Mary's" login credentials immediately. This would not have stopped the deletion of data since "Mary" still had "Amy's" login information, but it would have minimized the damage done, saving the hospital money and man-hours.

7.2 Employee education

Another important, but generally overlooked area to defense, is employee education. Employees, because they are human, are usually the weakest link in a company's/organization's defense. That weakness can be lessened through periodic training. This can make employees aware of what the best security practices for their organization are. There are both paid for and free training available. This training can come in the form of paperwork, online seminars and in-person training. An organization will never achieve 100% compliance, but if it can get 70-80% of its employees to "buy into" it's security policy, that is a lot of prevented attacks. This training can include such subjects as social engineering and hacking techniques, password policy and company computer usage policy. For example, Microsoft provides a free "tool kit" that includes a white paper, which details how to create an effective security awareness training program. It also includes sample materials such as brochures, newsletters, fact sheets and presentations, which can be customized to fit a specific organization's needs (Microsoft TechNet, Security TechCenter, 2009).

For the purpose of this case study, security awareness training would have educated "Amy" in the pitfalls of password sharing. It would have also kept her informed on the need to change her password on a regular basis. Having that knowledge in hand may have prevented her from giving her login credentials to "Mary" in the first place. In case she had given her credentials to "Mary", changing her password regularly would have kept "Mary" from accessing her user account in order to delete files. In turn, that would have kept 18,000 records from being deleted, saving "General Hospital" the cost of money and time in recovering crucial data. Remember, "Mary" stated that she

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

had written down "Amy's" logon credentials two years prior to her deleting those records. Other password sharing education could include not sharing your password over the telephone, via email or with employees from other departments.

7.3 Scheduled audits

It was found that the Accounts Payable department was failing to regularly audit their records. As was mentioned earlier, it was unknown when an audit of the Accounts Payable database was conducted prior to this event. Also, the supervisor was not checking on the number of files being deleted from the database on a daily, weekly or monthly basis. It was recommended that the supervisor check on the amount of deleted files on a daily basis. Since there are only 10 Accounts Payable staff members, conducting a daily audit would not be so time consuming. That way, if a new event occurs, it could be dealt with in a timely manner.

Also, at a minimum, if the recommendation to have IT notified immediately of an employee's termination is not enacted, then a periodic review of employee login credentials should be conducted. This would require the cooperation of both the Human Resources department and the IT department. If this were to be the case, then a representative of each department should be made to meet once a week to review a list of former employees and it is here that their privileges would be revoked. This would even apply to current employees who have been transferred to other departments, received promotions or had remote access rights granted/revoked due to job description. Employees moved to different departments would have different access needs than when they were in their previous assignment and promoted employees would have higher access to system resources than they had previously. This would help in mitigating not only a physical attack, but also one that may occur over a VPN connection that may have been forgotten about.

8. Data backup

It goes without saying that if data is part of your everyday operation, steps must be taken to ensure the safety and integrity of that data. This is something that should be

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

considered when creating and evaluating an organization's business continuity plan and disaster recovery plan, especially a medical center. A data center off-site would provide protection in case of a disaster or a computer intrusion and get a business/organization back up running in a fairly reasonable amount of time. There are options available with third party, off-site data backup companies that include pre-scheduled daily backups to real-time replication. With these options, downtime can range from a couple of days to just minutes. Cost must be a consideration when deciding which option to implement. As the backup option becomes more comprehensive, the more costs are associated with it.

9. Conclusion

There is no single security measure that will provide a complete solution to protecting an information system from an attacker, especially the insider. That is why a Defense-in-Depth approach to security usually proves to be the best option. With a mix of freely available utilities included with an operating system and some budgetary consideration that needs to be given to upgrading physical security, layers can be stacked to keep an attacker from gaining access to precious digital information.

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

10. References

Capelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009, January). Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1. Retrieved August 23, 2009, from http://www.cert.org/insider_threat

Cole, E., & Ring, S. (2006). Insider Threat: Protecting the enterprise from sabotage, spying, and theft. Rockland, MA: Syngress Publishing

Cyber-Ark Software. (2009, June 10). 2009 Trust, Security & Passwords Survey Research Brief. Retrieved August 17, 2009, from http://www.cyber-ark.com/constants/download-registration.asp?returnUrl=constants%2Fwhite-papers.asp&Subject=Cyber-Ark+-+Downloads+Form+-+Cyber+Ark+Snooping+Survey&dload=Cyber-Ark_Spring_2009_Snooping_Survey.pdf

Freedman, Alan (2009). Computer Desktop Encyclopedia (iPhone application), [computer program]. Available Distributor: The Computer Language Company Inc., Point Pleasant, PA (address: 5521 State Park Road, Zip: 18950), from http://www.computerlanguage.com

Goodin, D. (2008, June 6) Disgruntled admin gets 63 months for massive data deletion. The Register [Online]. Retrieved July 6, 2009, from http://www.theregister.co.uk/2008/06/13/it_manager_rampage_sentence

Gross, G. (2009, May 1) IT Director pleads guilty to deleting organ donation records. PC World Business Center [Online]. Retrieved June 7, 2009, from http://www.pcworld.com/businesscenter/article/164221/it_director_pleads_guilty_to_deleting_organ_donation_records.html

Kaplan, D. (2009, May 8). $12.6 million spent so far to respond to Heartland breach. Retrieved August 18, 2009, from http://www.scmagazineus.com/126-million-spent-so-far-to-respond-to-Heartland-breach/article/136491

Lemos, R. (2008, August 6). Feds charge 11 in TJX ID fraud case. Retrieved August 18, 2009, from http://www.theregister.co.uk/2008/08/06/id_fraud_hacking_case

Microsoft TechNet, Security TechCenter. (2009). Security Awareness Content.zip [Data File]. Available from Microsoft TechNet, Security TechCenter Web Site, http://technet.microsoft.com/en-us/security/cc165442.aspx

Microsoft Technet. (2009). Bb457112.f13zs02_big(en-us,TechNet.10).jpg [Online Image]. Available from Microsoft TechNet, Web Site, http://technet.microsoft.com/en-us/library/Bb457112.f13zs02_big%28en-us,TechNet.10%29.jpg

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Northcutt, S. (2007, February 26). Information Centric Approach to Defense-in-Depth. Retrieved July 6, 2009, from http://www.sans.edu/resources/securitylab/321.php

Password. (2009). In Merriam-Webster Online Dictionary. Retrieved August 7, 2009, from http://www.merriam-webster.com/dictionary/password

Phone Recording Tool [Online Image]. (n.d.). Retrieved August 16, 2009, from http://www.callcorder.com. http://www.callcorder.com/images/phone_recording_tool.gif

Richardson, R. (n.d.). 2008 CSI Computer Crime & Security Survey. Retrieved August 18, 2009, from http://www.gocsi.com/forms/csi_survey.jhtml;jsessionid=KBMX4IAROASGLQE1GHPCKHWATMY32JVN

SeachSecurity.com Staff. (2007, March 29). TJX says at least 45.7 million card numbers stolen. Retrieved August 18, 2009, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1249421,00.html

Washkuch, F. Jr. (2008, January 25) Florida woman accused of deleting $2.5 million in data. SC Magazine [Online]. Retrieved August 17, 2009, from http://www.scmagazineus.com/Florida-woman-accused-of-deleting-25-million-in-data/article/104575

Wilson, T. (2007, January 18). TJX Breach Skewers Customers, Banks. Retrieved August 18, 2009, from http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208804300

Zetter, K. (2009, August 17). Threat Level Privacy, Crime and Security Online TJX Hacker Charged With Heartland, Hannaford Breaches. Retrieved August 18, 2009, from http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Appendix A: Sample password policy

General Hospital Password Policy

1.0 Overview

All employees and personnel of General Hospital (including contractors and vendors with access to General Hospital's systems) are responsible for taking the appropriate measures, as outlined below, to select and secure their passwords. This is to ensure the security of General Hospital's network, protect data integrity and to protect computer systems.

2.0 Purpose

The purpose of this policy is to protect organizational resources on General Hospital's network by establishing a standard for strong password creation, the protection of passwords and with how frequently passwords must be changed.

3.0 Authority

This policy is fully supported by General Hospital's executive board and the human resources department. General Hospital's IT manager administers the policy, which is currently effective for all General Hospital employees and computer systems.

4.0 Scope

This policy applies to all personnel who are responsible for any computer account on which resides on General Hospital's network and has access to General Hospital's files, including but not limited to domain, web and email accounts.

5.0 Policy

5.1 General

- All system level passwords must be changed on quarterly basis.
- All user level passwords (e.g., workstations, email) must be changed every six months.
- Passwords must not be inserted or attached into email messages or any other form of electronic communication (e.g., instant messenger software).

5.2 Guidelines

A. Password Construction Guidelines

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Passwords have to meet a minimum standard of complexity. Weak passwords usually have the following characteristics:

- Have less than 8 characters
- Contain words that are found in a dictionary (English or foreign)
- Name of the organization
- Patterns of letters or numbers (e.g., aaaaa, 123456, abcdefg)
- Names of the user's family members, pets, favorite books, etc.
- No password at all

In order to be considered a "Strong Password", a password must contain the following:

- Minimum length: No less than 14 characters
- Created from a passphrase (e.g., N3wY0rkG1@nts!)*
- Contains at least one from each of the following categories:
  Upper case letter (e.g., A-Z)
  Lower case letter (e.g., a-z)
  Number (e.g., 0-9)
  Special or punctuation character (e.g., ! , % $ ^ & *[#)
- Passwords may be reused every 12 password renewals. Meaning that a password may not be reused within the following 11 times after initial creation.

*Note- do not use the above example as a password

B. Password Protection Guidelines
- Passwords are to be treated as confidential information. Under no circumstance are employees to give, tell or give hint to their password to another person. This includes co-workers, supervisors, family members, friends or administrators.
- Passwords are not to be transmitted electronically using such methods as e-mail, instant messaging or social media (e.g., Facebook, Twitter, MySpace, etc.). A password may be used to gain remote access to General Hospital's resources using a VPN, SSL protected site, etc.
- Never reveal a password to anyone over the phone.
- Do not write your password down.
- Do not leave your password on a "stickie note" attached to your monitor, computer or taped to the bottom of your keyboard.
- Do not use the "Remember Password" feature of applications.
- Do not use your General Hospital password while using personal, non-work related website accounts. Similarly, do not use personal, non-work related passwords for your General Hospital password.
- Do not store your password on a mobile device (e.g., Blackberry, iPhone, etc.) without encryption.

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- If someone demands your password, refer that person to the Information Security Department and to this document.
- If you believe that your password has been compromised, report details to the Information Security Department in order to change your password.
- As part of ongoing security vulnerability testing, the IT Department may attempt to guess user passwords. If a password is cracked during an audit, the user will be required to change their password immediately.

6.0 Continuance

This policy is a living document and as such may be modified at any time by the executive board, IT manager or the human resources department.

7.0 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination or employment.

Name: _____

Signature: _____

Date: _____

Joseph Garcia, garcia.josephj@gmail.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced