Global Information Assurance Certification Paper

Information Security Checks and Balances

GIAC Security Essentials Certification (GSEC)
Practical Assignment, v1.4b – Option 1

Prepared By:
Jacqueline L. Burns

Submission Date: June 4, 2004

TABLE OF CONTENTS

Abstract

Security breaches from within an organization can cost a financial institution, especially if the breaches are not detected, due to the assistance of an insider. All too often management assumes that an attack is only to do harm or upset the balance a work day. What if the real threat is to gain access to the system, and collect information? This kind of insider attack is not to harm, but to give access to an interested party to ascertain insider information and get out. The intruder do not want to harm the network, especially if they can gain access to the data, down load the data, and then decode the data at their convenience.

Having checks and balances in place can detour and even prevent this type of fraudulent activity. This paper will cover some policies, procedures and process that should be in place in order to minimize this type of insider fraud.

Introduction

Having information security (IS) employees accomplish the tasks of many former employees is the norm, in a time were downsizing and offshore outsourcing is standard practice for financial institutions. Internal controls are often the first check and balance to be overlooked. Typically, internal controls are part of the financial institution policies and procedures, but the smaller financial institutions do not have a strong orientation toward checks and balances or separation of duties, because that would require more people and money.

To reap the benefits of downsizing or off shoring smaller less experienced staff must accomplishes the work of more experienced staff, at the same time giving more control to the end user. Listed below are ten components that should be considered, if not included, in the IS policies and procedures at the enterprise and department level, to deter insider fraud.

Components

To have an adequately controlled and secured information security department there must be a number of components embedded in the Information Security policies and procedures to prevent and detect misuse, as well as, guidelines for conducting insider investigations.

Components List

1) Screening overseas contracted information security personnel
2) Creating clear lines of authority, roles and responsibility
3) Having a well defined separation of duties
4) Having proper procedures for monitoring for fraudulent activity
5) Maintaining adequate documentation of all changes
6) Conducting audits checks on logs for upgrades and changes
7) Having a clear change and control process
8) Conduct internal training
9) Social Engineering

Contracted IS Employees

General Information

The process of screening contracted employees should include the investigation of information from the past and present background checks. A local, national, and international criminal record check should also be part of the potential contractor's hiring process.

As standard with most financial institutions overseas contractors are not subjected to the same screening and background checks as local employees. The loyalty of the overseas contractor is not to the financial institution which hires them, but to the country that allows them to work. This changes the focus of loyalty of the contractor which also changes the level of risk, depending on where the overseas contractor is located.

The problem occurs when financial institutions have no control over the hiring procedures and practices used by overseas contractors. This should be a major concern because overseas contractors often have privileged access to the financial intuition's employee and customer information. Due to the increase in outsourcing of information of security functions, the more the likely hood that insider fraud will occur. One way the contracting financial intuition can insure that background checks are preformed on all potential contract employees is to request this during the contract negotiations. To require overseas contractors to screen both locally and internationally and to hold the contracting organization liable if the contracted employee commits fraud. Thus reducing the parent company's risk and increasing the overseas contractor's risk. This would give the overseas contracting firm a greater reason to do a more through background check on potential employees. If any of the previous suggestion are not included in the financial instruction's policies and procedures or standards of operations could be putting the financial institution at great financial risk.

One practice that should be causing concern to financial institutions is the need for overseas programmers and computer enthusiasts needing to make a name for them selves by doing something to cause major media attention. All this in an effort to get hired as a former hacker with experience, by some computer security consulting firms, which further increases the risk of security compromises.

With the emergence of faster technology and less expensive equipment, the ability for overseas contractors to take advantage of even restricted access to critical systems can be a risk, because what they don't have access to they will create away to gain access. It is not unusual for overseas contractors to know the infrastructure better than current local employees. Overseas contractors should be closely watched and monitored until a level of reasonable trust can be established, and all potential risks have been mitigated.[1]

Overseas contractors represent a unique security threat in that they are generally not subject to the same hiring process as local employees, but they are assigned the same high level of access to the system and network.[2]

Example of the Danger:

A major financial institution discovered a Trojan horse in software created by an overseas contracted employee. The Trojan horse was created by the contracted employee with prior international convictions related to virus writing and spreading. The overseas contracting firm failed to investigate this employee who installed the code in anticipation of using it as a tribute to his country.[1]

It should be noted that not all potential criminals have a prior criminal record.

Roles & Responsibility

General Information

Roles and responsibility is an area where a well thought out and defined process and continued updating is essential in order to prevent insider fraud. As the role evolves and more duties are assigned to an information security's area of responsibility, the potential for fraud increases. The roles and areas of responsibilities should be subject to reviews by an audit committee, to discuss information security's individual responsibilities in order to determine if the overall level of risk exists. This review of the roles and responsibilities will also give the management an opportunity to either mitigate the potential risk or except the risk. Also, management should understand their own roles and responsibilities along with that of their subordinates.

In essence, a periodic reviewing of roles and responsibilities may help to identify areas where duties can be reassigned or separated to reduce the risk of error or fraud, or situations in which additional resources or controls are needed to adequately manage the risk.[3]

Example of the Danger:

Regional Branch manager, for a bank in Middle America were charged in an intricate computer fraud that cost the bank millions of dollars over ten years. The investigators discovered that the motivation was to have enough money to retire. Among the strategies used was manipulating the computer accounting system to funnel certain cash transactions into a dummy account. At the end of the day, the perpetrator would take the overage amount and funnel it into a secondary account and then falsifying the records to erase any trace of their fraud. [3]

Separation of Duties

General Information

The term separation of duties 'mean the practice of separating functions or roles among different individuals, in order to keep a single individual from subverting a process.'[4] For example, the security personnel responsible for creating the firewall rules should not be the same as security personnel responsible for auditing the firewall logs. That one person's work serves as a complimentary check on another person duty. The most important part of this

definition is that no one IS person shall have complete control over any process from conception to implementation.

Separation of duties must be utilized to provide control and protection. If separation of duties is impossible, alternative controls must be utilized and documented. The following is a list of ideal separation of duties, to try and mitigate fraudulent activity:

1. Firewall Administrator must be separate from Firewall monitor.
2. Firewall policy changer must be separate from the review and reconciliation of reports and errors.
3. IDS Administrator must be separate from the IDS monitor.
4. IDS policy changer must be separate from the review and reconciliation of reports and errors.
5. Mainframe security administrator must be separate from programming
6. Utilize job rotation, and cross training must be used to allow for review of work by others.
7. Information security access privileges must be changed to reflect changes in job responsibilities.
8. System Domain Administrator must be separate from Mainframe administrator.
9. Information Security development activities should not access production data assets, except for the selection of records for test or support activities for applications.
10. Information security personnel should not be allowed to directly operate data processing systems which process financial transactions or business records or deliver services to the customer.
11. The staff that maintains access control systems and change control systems must be separated from input, programming, and operation of data processing systems
12. Personnel responsible for system development, computer operations, access control, and change control staff must not be allowed to originate business (production) transactions.
13. Incident response monitor should not be network, firewall and mainframe administrators. This individual should have an unbiased observer to the fraudulent act. This is to assure that your administrators are not the cause of the problem.

Separation of duties has a barring on ensuring that access and authorizations are valid and properly recorded. If different individuals process two separate components of a function, each person provides a check and balance over the other. Separation of duties acts as a deterrent to fraudulent behavior because it requires assistance with another individual to complete the fraudulent act.

Example of the Danger:

A network administrator at the Walnut office of the View sonic Corporation was sentenced to one year in prison for hacking into the company's computer

system and wiping out critical data, an act that shut down a computer server that was central to the company's foreign operations. He was in charge of several computer servers and had complete access to the network, with little separation of duties or checks and balances.[6]

Monitoring IS Activity

General Information

Monitoring is a great way of observing changes that occur on the system by your administrators. The monitoring software will track any changes that are made by designated personnel. The problem with using software packages is that someone must monitor and report on the activities, which is normally someone in the IS department. Usage of a software package to monitor administrator's activities requires a third party to review the reports.
If the separation of the duties for monitoring is not feasible, then you might want to consider an offsite firm to monitor all network traffic. This will allow you to utilize the expertise of an third party and the comfort of knowing someone is watching the administration staff. This is a good way of mitigating the risk of fraudulent acts.

Example of the Danger:

A mainframe administrator at a financial institution learns he is going to be downsized. He decides to download large parts of the organization's customer data. He contacts the systems administrator responsible for the information and offers to release the data for a fee and a promise of no prosecution. He agrees to his terms before consulting with proper authorities. Prosecutors reviewing the case determine that the administrator's deal precludes them from pursuing charges. [7]

Documentation

General Information

The most efficient method for keeping track of changes to firewalls and IDS systems is the utilization of documentation. It is vital to have a record of changes that has occurred, and why those changes were necessary. Documentation that is continually updated can be used as a source for why these policies are in place, and to be a deterrent to fraud.

The documentation of security programs should include requirement documents, that tell the story of what the security administrator need to do to restore the policy to it original state, comments that explains how and why this request was instituted, and if the request goes against the department standards, an explanation of why the need to deviate from the norm.

The documentation of any changes to the firewall policies should show what the new policy should look like, and any policies that was affected by the changes, is a good approach to annotating information security policies. Having a process and procedure to insure that changes are approved, added to the

security documentation, and who has the authority to make new changes to the systems is an important ritual to deter fraudulent entries into the firewall system.[2]

All aspects of the security systems should be thoroughly documented to ensure that new changes will not conflict with the current setup. As security engineers and administrators are promoted or leave for other companies, the proprietary information they carry with them must be documented, so that it can be passed to future generations of security engineers and administrators. If the original engineer created a policy that deviate from the industry standard because of a specific reason are types of changes must be documented. Another important part of documentation is that the documentation must be available, and known to others in the department and management, for auditing, and general review.

The documentation should address current status or configuration. It should also provide some context for why the system settings are as they are. In software, this may tie back to the business rule that is being implemented. For infrastructure, it should reference overall network and security design documents. Documentation is a log into what and how things are configured in the information security department.[2]

Example of the Danger:

A senior information security engineer, that controlled all of the firewall policies, quit because of a better job offer. He was the only person at the bank with the knowledge and understanding of how the firewall policies were setup. Without documentation the company had a hard time finding a replacement to understand how and why some of the policies were created. This required the financial institution to rehire the old engineer as a consultant to document and train a new engineer, which put the institution at a greater risk, because they still did not know if he had established back doors to their system. The bank had no choice be to assume the risk.

Auditing Logs

General Information

One of the worst situations that can happen to any financial institution is to be infiltrated and not be aware of it. The longer a intruder is able to be on your network the more damage that can be caused. It doesn't do any of good if there are logs for the firewalls and IDS and no one ever reviews them. The time it takes to review volumes of files that are used to log events can be very boring, and time-consuming. It is also easy to put the reviewing of the logs off when the day is very busy. One option is to purchase software that can be used to streamline the process of auditing log files.

Log file data should be considered as valuable as the most valuable data that is stored on your network. Do not regularly delete the log files to save disk space. Instead safely store the information away for a period of time, because when a security breach occurs, it is possible that the actual breach occurred many months back.

Keeping and auditing log files to be scrutinized later should be standard practice. Auditing security logs is a valuable tool that can be used to enhance security, and mitigate potential risk.

Change Control

General Information

The checking of FW policies by different individuals means that there is an opportunity for one of them to catch an error before a policy is fully executed and before decisions are made based on potentially fraudulent information. Unfortunately, a few people may be encouraged to engage in fraudulent activities.

The change control process should show the reason or source for the change. The change control policy should have a matrix on who in the organization must approve different types of change requests. The change control procedure should include some, if not all, of the following information:

1. The procedure to request for a change
2. Clearly state what information must be supplied
3. A matrix of who needs to approve the change
4. Steps necessary for the change to be implemented and tested
5. A back out option, if the change fails
6. A standardized format of how the change should be documented

It is important to establish procedures and internal controls on how changes can be made to firewall, network, security monitoring applications, and other security settings. To help prevent fraudulent behavior, the scope of changes that a single individual can make should be a limited. If possible, it would be essential to require two or more individuals to make changes. There should be an established notification procedure that determines who must be notified for what types of changes and within what time frames. Pre-established configurations should be created and maintained, as set of approved change control format to expedite the process.

When changes are made, the following information should be annotated in an After Action Report:

1. The date and time of the change
2. The objective of the change
3. The details of the change itself
4. The person or persons who implemented the change
5. The individuals who requested the change
6. The success of the change

The change control procedure should not make the process of doing a change difficult. It should actually allow management to have a log of all changes made to the system and why.[5]

Protecting your system from internal attacks requires more than the writing of policies and procedures. It requires a strong commitment to change control and training to mitigate the risk of fraudulent activities.

Internal Training

General Information

All the policies and procedures in the world won't help if employees are not aware of them. It is very important to train your security personnel on the policies and procedures. Security personnel should be aware of what is expected of them and what will happen if an ethical breach does occurs.

Another over looked aspect of training, is that managers of the IS department must be trained to understand what security measures they're using, what is out there and what should be changed to mitigate risk. Having the mangers trained will allow them to make informed decisions, and the knowledge to, at least, spot fraudulent activity.

Cross training is a way of creating a check and balance because there will be more than one person that knows how the security systems are installed, and why the systems are set up that way.

In the need to save money and minimize risk, information hoarders on your staff are an expense no company should want to bare. The motto should be, "if the employee doesn't want to share security information, then that employee doesn't want to be there." Information hoarders are a security risk that the company has already assumed, can't transfer and is to costly to mitigate, so the only other solution is not to have them in your company.

Internal security training is valuable to management and associates, because it keeps every informed of the changes in the security field.

Social Engineering

General Information

Get to know your security staff! This is the best information that this paper can give you. Management by proxy is not a good idea for the security department, because of the level of control that that group has over the financial institution. Getting to know your security staff will give you first hand knowledge when someone is unhappy or overworked. This gives you, as a manager, time to either correct the issues, or prevent an unhappy employee from creating fraudulent acts.

Conclusion

Relying on a single information security person to handle security access to servers, applications, firewalls, networks, internet, extranet, and any other access that the bank needs to control, with little to no checks and balance has the potential to be the next frontier for scandal, for financial Intuitions information security department.

Do you know who is on your networks after hours? Do you know who is on your network during hours? Do you know the reason for the firewall policies on your system? Do you know who is reviewing your security logs? If you can not honestly answer the previous questions then you need to begin to make plans to mitigate your risks, starting with your policies and procedures, and ending with the enforcement of those policies. In reviewing your company's policies and procedures, make sure the policies are really policies and not suggestions that security employees feel free to ignore at their convenience.

REFERENCES

1. Shaw, Eric, Ph.D., Ruby, Keven G., M.A. and Post, Jerrold, M.D. "The Insider Threat to Information Security". 28 November 2001. URL:http://www.wasc.noaa.gov/wrso/security_guide/infosys.htm
2. Global Justice Information Sharing Initiative Security Working Group. "Applying Security Practices to Justice Information". Version 2.0. March 2004. URL:http://it.ojp.gov/documents/asp/disciplines/section1-2.htm
3. University of California, Santa Cruz Campus controller's Office. "Financial Controls, separation of Duties". 1 November 1999. URL:http://www.ucsc.edu/finaff/cc/tips/sepduty.htm
4. U.S. Department of Justice. "Former Employee of View Sonic Sentenced to One Year for Hacking into Company's computer, Destroying Data". 23 February 2004. URL: http://losangeles.fbi.gov/2004/viewsonic022304.htm
5. Global Justice Information Sharing Initiative Security Working Group. "Applying Security Practices to Justice Information." Version 2.0. March 2004. URL: http://it.ojp.gov/documents/asp/disciplines/section2-5.htm
6. Allen, Julia & Stoner, Ed. "*Detecting Signs of Intrusion"*. (CMU/SEI-SIM-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000. URL: http://www.cert.org/security-improvement/modules/m09.html.
7. *Computer Security Resource Center (CSRC)*, National Institute of Standards and Technology (NIST), Computer Security Division (CSD), "compilation of computer related security best practices". URL: http://csrc.nist.gov/
8. *Computer ethics Institute.* "The Ten Commandments of Computer Ethics." 16 April 2001. URL:http://www.cpsr.org/program/ethics/cei.html.