Global Information Assurance Certification Paper

Securing Information Assets From Internal Threats
By Fernando Pérez
Practical Assignment Version 1.3

Introduction

The need to protect information is as old as information itself. The first documented effort to protect information goes back to the Roman Empire, when Julius Caesar used a mathematical cipher, known as the "Caesar Cipher, to encode and decode messages. Not only this was intended to protect information from the enemy, but also from internal threats such as spies.

In our times, we have more ways to encrypt information than back then, and new techniques are developed everyday to help us protect from external threats. However, in the corporate world, management will always have to trust users within their organizations to access non-encrypted information in one way or another.

According to a 2001 Information Security Magazine Survey, internal breaches of security are undetected and dangerous. Of those organizations surveyed:

- 86% of computer crimes originate inside the network (Intranet Security)
- 58% experienced abuse of computer access controls
- 24% experienced intentional disclosure of proprietary data
- 1 in 10 U.S. companies surveyed experienced a database breach
- 25% of the reported breaches were in the financial sector
- 18% were in the telecom & healthcare industries

According to the FBI, the average cost of an internal breach is $2.4 million while the average cost of a break-in from the Internet is $27,000.

How do we protect our information from internal exposure? That is the question we will try to answer in this document.

Risks and Threats

In the world of information technology ("IT"), the terms information privacy, integrity, authenticity, and reliability have always been an afterthought until now. The growth of the Internet, the use of electronic data by organizations to run their business, and new government regulations (i.e. The National Information Infrastructure Protection Act of 1996) are three factors that have force Information Technology organizations to be more conscious about securing their information assets.

While most organizations focus on implementing security controls on the network perimeter to protect from incoming threats, they still lack adequate protection inside the firewall. Currently, more authorized users than ever are allowed on the networks (i.e. employees, external customers, partners, contractors and guests), so it seems impossible to accomplish the task of protecting information assets from internal threats. The problem is worsened because server operating

systems are extremely vulnerable and password protection on most networks is for the most part ineffective.

A good example of an internal threat that can go undetected is a logic bomb. This type of threat is one of the most dangerous and destructive. A logic bomb is malicious code intentionally placed in the system and set to run at a certain date and time.

Some other internal attacks could include: Trojan horses, unauthorized copying of confidential data (including source code), password sniffing, data diddling, unauthorized software/data modifications, viruses, and worms.

The one thing that all these threats have in common is that they can all could be initiated by an internal threat, such as an unhappy employee

Security Policies

The first step to protecting information assets is developing an adequate Information Security Policy. There is not a one-size-fits-all policy for all organizations. A good security policy should take into consideration risks and vulnerabilities, and provide comprehensive coverage of an organization's infrastructure. It should seek balance between access and security. Without strong management policies, the organizations security programs will be less effective and not necessarily align with management objectives.

The policy should establish the foundation of corporate information as an asset that must be protected. The policy itself is part of the organization's information assets. It should include sections discussing proprietary software and data, and make all members of the organization responsible and accountable for the information assets of the organization.

The basic elements of a policy are the scope, High-Level Policy Statement, Accountability, Non-compliance Statement, Monitoring and Exceptions. The scope section should outline the purpose of the policy, and it should be located at the beginning of the document; The High-Level Policy Statement should be a paragraph stating the goal of the policy; the accountability section should identify the personnel involved in enforcing the policy; the Non-Compliance section should state the consequence of not complying with the policy; the monitoring section should describe how the policy will be kept validated and updated; and, the exceptions section states how variances to the policy are granted if for any reason a rule should be bent.

The policy should include a section discussing how to handle breaches in security (i.e. who to contact, steps to take), and it should discuss the different areas managed by the IT organization (i.e. Internet, Network, hardware, Passwords, and E-mails. In addition, it is recommended that all members of the organization sign a statement to say that they read and understood the policy. This statement should be filed, if possible as part of the Human Resources file.

A password policy must discuss password expiration times and lengths. The password policy should also discuss the management of passwords for the Internet, E-mail, administrators, and database custodians.

An Internet usage policy should discuss the filtering and software used to monitor Internet usage, as well as those tasks that are allowed and those that are not. The e-mail policy should cover the acceptable use for e-mail and any filtering or tools used for handling e-mail traffic.

The network security policy will need to cover all access to computing and information resources. This policy may include sections to cover firewall security, intrusion detection, and security event monitoring. It should also cover the physical security measures that should be considered in order to protect network elements.

A section regarding external access to the systems should clearly explain methods to be used for allowing and approving access into the networks remotely form outside, and it should also describe the events that are not accepted.

Desktop guidelines should outline what is expected from the users and support in order to maintain an appropriate security structure for the organization. It should also outline desktop and server access controls, administration, anti-virus software and other compensating controls.

It is also important to the controls surrounding an application. An application security policy should describe how the applications used by the organization meet specific regulations. In short, the Information Security Policy will set the rules of the game.

Information Classification

Today's organizations compete to have competitive advantage over information. In a rush to capitalize, organizations have developed many Internet-enabled applications such as Intranets, Customer service Applications, Order Entry Systems, and E-market places. Many organizations do not thoroughly evaluate the risks that these applications bring to their business and data. Through an Information Classification Process ("ICP"), companies can develop effective and efficient controls to mitigate such risks.

The starting point for an effective ICP should be the organizations Information Security Policy. Here the organization, as mentioned in the policy section, defines corporate information as an asset that need to be protected and also defines the sensitivity of risks and consequences for breaches into each of the classifications of data. This policy should also define how the information should be protected.

In order to be successful, the ICP should have full support of the organization's senior management. This will be an important factor for funding and implementation of the process.

The ICP should be a set of guidelines and requirements designed to protect corporate confidential information. It should support business practices, and it should cover all classifications of data within the organization.

The criteria that an organization should consider to create its classifications are the following:

- Confidentiality – risk that sensitive data could be accessed

- Data Integrity – risk that unauthorized modifications to information could occur
- Availability – risk that critical systems cannot be accessed in a timely manner
- Risk to repudiation – accountability
- Privacy – risk related to corporate unauthorized use, or gathering of user information.

An ICP targets the application level data. The development and implementation of operational procedures to protect data at the application layer are more effective than using firewalls and proxy servers. Firewalls are very effective protecting the infrastructure, however, they lack the complex logic that would be required to protect different classifications of data.

Once the classifications are established, the ICP should address the different types of controls that will be required. These controls should mitigate damages when unauthorized actions are detected and alert the appropriate personnel when these actions occur. Other controls such as audit trails should be in place to trace any unauthorized activity.

The controls needed for an ICP should not focus on single points of failure within the control architecture, and it is important to develop redundant controls in order to lower the risk if a control fails. Also, different types of groupings should not be mixed with one another. However, when this is unavoidable, these groupings should be categorized as sensitive.

Authentication and identification should also be part of the ICP. Authentication is the process of validating a users identity. The failure to authenticate a user's identity reduces the system integrity and accountability causing privacy, confidentiality, and integrity issues. The bottom line is that authentication is done to ensure that only authorized users are accessing protected systems or data.

Authorization is another important part of the ICP. This will permit or restrict users access to databases, functionalities or applications. Therefore, after a user is authenticated in a system, the systems and applications should ensure that the user has enough rights to perform a specific function or operation. The authorization mechanism should be implemented in a way that it is never bypassed.

The user authorizations define the type of access that a user will have to data or programs (ie. READ, WRITE, EXECUTE, CHANGE, and CREATE). When implementing the access controls, it is important to follow the least of privileges, which means that the user should be granted the minimum set of permissions to perform a job. People who only need to read reports should not have access to update or change databases.

Access Control Systems are categorized into discretionary or mandatory. Discretionary access controls enable users to set the rights and permissions to their own data or application. The mandatory access control requires that all elements within the system are properly identified, and the governing system controls all the elements within the system.

Confidentiality requires the protection of private or personal information. Applying the proper access controls and using encryption when the information is transmitted through un-secured networks achieve confidentiality.

Keep in mind that all encryption can be broken given enough time and resources. Confidentiality also includes how a corporation manages certain types of information, and how the company's users manage the information.

As important as it is to keep data confidential, data integrity should also be protected to ensure that it has not been illegitimately changed. The integrity of data faces many threats such as data entry errors, malicious users, transmission errors, and application processing errors.

Maintaining systems with high integrity goes beyond authenticating and authorizing users. Good applications will perform validation checking to ensure that data inputs are adequate. This meaning that the formats are correct and that the defined validation rules for the data entered is correct.

Users always attempt to use systems in ways never anticipated (intentionally or unintentionally). Applications should always log events that are successful as well as unsuccessful. Administrator should monitor these logs to detect any suspicious activities before a serious security breach occurs.

Audit logs should be efficient and sufficient to review, and examine transactions from creation to output. Also records can be reviewed to track the system usage and detect intruders. However most audit logs will not reach the integrity of databases.

Database Beacon Scoring (Data Integrity)

Data Integrity controls are the hardest to implement, especially if users have direct access to the organization's databases.

Organizations will always have users who will have update capabilities to information assets. A good example is a customer service department of a bank, credit services company, or insurance company. These organizations hold private information (i.e. account numbers, social security numbers, automobile VIN numbers, policy numbers, addresses, etc) that may require at any moment to be updated. Updates can be done by sharing data records with other organizations via FTP, customer data tapes, or by direct intervention of a customer service representative.

Consider the following scenarios:

- A customer service agent is approached by an individual who will pay a sum of money to modify records in a database
- An employee has access to sensitive data, and uses it for his privately owned business
- An employee from a credit services organization who accesses his own records in order to modify data to reflect better credit information

How can organizations protect from these kinds of threats? The following are examples of controls that could help mitigate the scenarios mentioned above:

- Ensure that a Database Management Policy exists. This policy should address information classification, the types of changes or updates that are permitted, and the process that should be followed in order to make such changes.
- Designate database custodians to guard and approve the access and changes to data.
- Develop scripts around databases that will detect and write to an audit log every time an employee accesses or attempts to access his own data records. If possible, set up alerts that will notify the data owners as soon as this type of events occurs.
- Develop scripts to monitor the changes that occur inside the database using a scoring technique.

As part of the Database Management Policy, a section should be included discussing the responsibilities of data custodians. Data custodians should authorize all access to the organization's databases.

Some operating systems or security packages will have audit tools that are capable of monitoring the activity surrounding databases. These tools can document any time a user accesses any file, directory or database, and also will detect when a user is not able to access a database. The security administrators can then review the reports generated by these tools.

Even though these tools can detect unauthorized access to databases or company's information assets, they cannot detect changes made to specific fields within databases. This is where the concept of database scoring comes into play. This technique allows data custodians to ensure that changes made to databases are authorized. It is still a detective control, but with periodic reviews it is possible to prevent serious damages to databases.

This control works by developing scripts that will monitor changes inside the databases. When a user accesses a database, the script will give the user id an initial score. Each record and activity within the database and activity is assigned a value that is added to the initial score every time a change is made. Once the user exits the database, the final score is logged.

For example, if a user accesses an insurance database to modify a customer address. the script gives an initial score of 100 points just for accessing the database. When the user modifies the address, the script adds 50 points, which means that when the user exits the database, a score of 150 points is recorded in the log. The more sensitive the data changed, and the more records modified, the higher the score should be.

With this type of information, the data custodians can determine if a user is making unauthorized changes. The users should be able to justify any changes made to a database, especially if the user is from a customer service function.

Software Configuration Management

Occasionally programmers will download or copy databases, source code or portions of data into their hard drives to perform testing. By doing this corporate information assets are put at risk. IT organizations normally should have test environments for programmers to test their programs.

It is recommended that organizations do not allow users to copy source code or data into their hard drives.

A very important part of an organization's information assets, is the program source code. In many cases management forgets just how important it is to protect the applications' source code. Well, it is as important as any database and it must be treated with the same level of importance. To protect application's source code a discipline called "Software Configuration Management is used.

Computer Associates defines Software configuration management ("SCM") as **"*the discipline whose objective is the identification of the configuration of software at discrete points in time and the systematic control of changes to the identified configuration for the purpose of maintaining software integrity, traceability and accountability throughout the software life cycle.*"** In simple words, SCM is the process to protect, trace, and control changes made to application source code.

There are four SCM functions that are needed in order to accomplish this. They are identification, control, status accounting and audits. In the Identification function, the SCM tool will keep track of the users and portion of the source code that is to be changed. It will describe the program being generated, the processor used to generate or change the source code, the user-defined symbols, their version and level.

The Control function, used to protect the source code, will cross-reference the low-level components of the source with all of its high-level owners. This way it is ensured that the original source code is not affected unless approved by the appropriate authority.

The Accounting function keeps track of the versions. It stores and remembers the components used to create the outputs for a particular program, date and time, version, and level of a typical program.

The Audit function, by using the information stored in the Root and Cross-reference Databases, it is possible to generate logs that provide historical audit trail of source code changes that serves as the foundation for all software configuration analysis and management activities.

Practicing configuration management in a software project has many benefits including increased development productivity, better control over the project, better project management, reduction in errors and bugs, faster problem identification and bug fixes, and improved customer goodwill.

The major challenge is ensuring that the relationship between a program and its related components is accurate and up-to-date, at any given point in time. This synchronization is typically accomplished by retranslating a program each time one of its subordinate components is changed. A problem arises, however, when a component is changed but that modification is not propagated to all affected programs.

Below, find a list of configuration management tools that are available and the operating systems that these tools support:
"AllChange" by Intasoft Ltd.
"Endevor" and "CCC/Harvest" by Computer Associates International
"ClearCase" and "ClearGuide" by Rational Software Corporation
"CMVision" by Expertware
"PVCS Dimensions" by MERANT
Continuus/PT, Continuus/Web Synergy, and Continuus CM by Continuus Software Corporation
VisualAge and TeamConnection Enterprise Server by IBM Corp.
EChange Man by SERENA Software Inc.

These are not the only SCM tools that can be found out there, but they are the most popular and considered the high-end SCM tools that cover all the SCM functionality. These are also process-oriented tools.

Conclusion

Protecting information assets is not an easy task. Organizations have to consider all kinds of threats, and all scenarios. The Information Security teams, in many cases, will need to think like an intruder or put themselves in the place of someone who would want to cause harm to the organization's information assets. The constant growth of technology creates more challenges for intruders, and they like that. However, by keeping in mind basic controls and having a broad scope in security that considers both internal and external threats, organizations can accomplish the mission of protecting their Information assets.

References:

[1] Andre Pretorius. "Information Security Awareness Policy" April 10, 2001
URL: http://rr.sans.org/policy/infosec_awareness.php

[2] Cisco World, Web Papers
URL: http://www.ciscoworldmagazine.com/webpapers/2001/12_cryptek.shtml

[3] NCipher Security Insights
URL: http://www.ncipher.com/insights/databases.html

[4] FDIC, Financial Institution Letters
URL: http://www.fdic.gov/news/news/financial/2000/fil0067.html

[5] Sygate Secure Enterprise Solutions for Internal Threats White Paper
URL: http://www.sygate.com/products/sse/sse_internal_threats.htm

[6] CA-Endevor Administrator's Guide

[7] CISSP Certification, Data Classification, Page 100 Exam Guide Harris, McGraw-Hill Osbourne.

[8] Information Security Management Handbook 4th Edition, Tipton Krause.