Case Study in Information Security: Securing The Enterprise

Roger Benton

Case Study in Information Security
Securing The Enterprise

By: Roger Benton

GSEC Certification, Version 1.4c Option 2

March 8, 2005

Abstract

This practical is a case study of an Insurance Company's migration to an enterprise-wide security system. It is the intent of this practical to provide a path to follow when creating or migrating to a security system. Initially, a primitive online security system was the only mechanism to control access to corporate data. The exposures were severe - there were no integrity controls outside of the online environment. Anyone with basic programming skills could add, change and/or delete production data.

A project plan was developed to identify tasks, assign resources and ensure milestones were met. The scope of the security initiative included creating an inventory of information assets, creating new objects (data within datasets), constructing new groups and granting the appropriate permissions for access to the objects. Training documentation was created to instruct the users how to access the new system, both in an interactive and batch mode. Mini boot camps were conducted to train the trainers, who in turn, provided mentoring and tutoring for the user community.. Additional staff was recruited from other departments to provide user support for the rollout. D-Day arrived and the rollout experience only minor glitches. All the exposures were mitigated to the satisfaction of internal and external auditors

Before Snapshot – May 1998

The Bumper Insurance Company (BIC – not its real name) is operating in a 1980's technology environment. There are no LANs or WANs, just 3270 (dumb – green screen) terminals linked by coax to the mainframe. In addition, BIC had previously acquired another insurance company and runs the acquired company's applications on the BIC mainframe. A proprietary security system provides access control for the online applications; there is no provision for access controls outside of the online environment. What are our risks? How can we quantify the risks?

National Institute of Standards and Technology (NIST) has many documents dealing with information security:

> Consistent with OMB policy, each agency must implement and maintain a program to adequately secure its information and system assets. An agency program must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is one way to determine if the system and the information are adequately secured.[1]

---

[1] NIST, p.1.

In conducting a risk assessment, the exposures become enormous:

- There is no centralized security department nor are there any security policies, standards or procedures. Security is administered by a single person working in the systems support department.
- An in-house developed security system provides authentication and authorization services for only the online applications. There are no provisions for users to change their passwords and there is no facility to lock out accounts for unsuccessful password attempts. Additionally, account IDs and passwords are stored UNENCRYPED in the online security file – any programmer can create a printout of this file.
- There is no facility that discovers or records sign-on failure attempts.
- There is no protection for objects from access outside of the online applications. For example, anyone with programming experience has the ability to write programs to access/update/delete production data or to use utilities to access/update/delete production data.
- Numerous instances of production downtime occur when developers are "testing" but accidentally modify production data. The data has to be restored from the previous night's backups. Transactions that were overlaid by the restore jobs had to be resubmitted.
- Independent insurance agencies (licensed to conduct business with BIC) access the online application utilizing 3270 terminal emulation programs provided by a 3rd party business partner. (passwords don't expire)
- There is no security manual or documentation of security procedures, processes, standards or guidelines.
- Examinations conducted by both internal and external auditors bring the exposures to the attention of senior management.

A technology refresh initiative is developed to upgrade the mainframe platform. Included in this refresh is to utilize the most current mainframe hardware and operating system, including the most current mainframe security system.

During Snapshot – November 1998 through November 1999

The technology refresh is underway. The new mainframe has arrived and the operating system is being generated. Vendor personnel are on-site and begin to install the security system.

Centralized Security

A security manager is hired to coordinate the security aspects of the refresh.

An information security managerial infrastructure should:

- exist
- include a management forum
- provide security coordination across organization
- formally and clearly allocate responsibilities to specific parties
- include management process for authorizing new information processing facilities
- develop sources for specialist information security advice
- encourage cooperation between organizations
- include independent reviews of information security[2]

Security standards, procedures and guidelines are developed and documented. The newly-implemented LAN provides an intranet site, where the information security directives are published for employee awareness. Included are pages such as:

MISSION

To preserve the confidentiality, integrity and availability of information by minimizing the potential for the unauthorized addition, alteration, destruction, denial or disclosure of data, regardless whether the act be intentional or accidental.

To facilitate secure connectivity and access by anyone, anywhere, anyhow, and anytime to anything: ANY-5

SECURITY STANDARDS

Practices:

"Practices" is a common approach, a standard, a level of requirement or a control objective that allows BIC to maintain reasonable and responsible levels of protection for computer information, assets and resources. Common mechanisms, procedures and tools are developed or selected by BIC to meet the standards set forth in the practices. These practices embody:
Software, hardware and/or physical devices are employed to protect information from the unauthorized addition, modification, deletion, denial or disclosure regardless whether the act is accidental or intentional. Technologies such as digital certificates, firewalls, intrusion detection systems and access control/logging processes are utilized.

- Grant access to company information based only upon job-related functions and a need-to-know basis, in compliance with the established procedure for requesting access to computer systems/networks. All requests must be submitted in electronic form.

[2]Newstaff

- Critical computing resources are afforded physical protection.
- All remote access to BIC networks and a supplemental security layer are protected by computer systems. Personnel must use the secure access server to access the network. At no time is a modem to be directly connected to a computer/PC that is directly connected to either the local or wide area network, except via the secure access server, unless so authorized by the manager, network services.

Protection:

Information is afforded protection both while being stored in computer systems and while being transmitted over private and/or public networks. The levels of protection increases with the sensitivity of the information.

User Accounts:

- Each user of a platform (mainframe, NT, UNIX, etc.) has a user ID and associated password for their individual use. The user ID and password are the authentication mechanisms for access to the latform/applications.
- Only one user account is assigned to an individual, unless so authorized by the manager, systems security.
- Upon separation of the individual assigned to the user account, all account access is granted to the individual's manager/supervisor. (The password is changed and given to the manager/supervisor, who accesses the account(s) to delete obsolete/unneeded data, forward e-mail to the appropriate individuals, copies data to other folders/libraries and performs other requisite clean up of files, prior to the deletion of the user account and its associated data.

Event Logging:

Certain events are recorded to provide an audit trail of system activity. The following table defines the minimum standards for event recording.

Event	Logging
All failed attempts to access resources	Required
Password violations	Required
Logon/Logoff activity	Recommended
Specific users	When applicable
Special/Adminstrator activity	Required
Operator Activity	Recommended.

The event logs are maintained for a minimum of 1 year.

Unattended Workstations:

To minimize the potential for the unauthorized use of terminals and personal computers, it is recommended that personnel protect their input/display devices:

- For terminals (327x) devices:
  If so equipped, disable the terminal by locking the terminal and removing the key.
  If not equipped with a key/lock, log off from the system.
- For personal computers:
  Manually activate the password-enabled screen saver.

Default time-out for periods of inactivity:

- TSO
- 30 minutes
- Windows/NT screen saver
- 10 minutes

Encryption:

There exists a number of technologies that provide assurance for the integrity and confidentiality of information. They include but are not limited to:

Encryption
Digital signature
Digital certificates
S/MIME e-mail

It is the responsibility of the service requestor to coordinate all requests with the managers of systems services, network services and systems security to assure the appropriateness of the protective measures to be employed.
It is absolutely essential that no encryption mechanism be deployed without the express written consent of the manager of systems security. Failure to properly implement the encryption process can result in the unrecoverable loss of data.

Resource Access Control Facility: RACF

What Is RACF?

> In 1976, IBM set the standard for security products when RACF was introduced! From the beginning, the RACF Development Team has proudly brought you RACF, the premier product for securing your most valuable corporate data. Working closely with your operating system's existing features, IBM's award-winning Resource Access Control Facility (RACF) licensed program provides improved security for an installation's data. RACF protects your vital system resources and controls what users can do on the operating system. As a key component of the z/OS Security Server, RACF supports both OS/390 and z/OS.[3]

[3]IBM
RACF provides security by:

- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

How does RACF identify and verify users?

> RACF identifies you when you log on to the mainframe system. It does so by requiring user identification, your user ID - a unique identification string. RACF then verifies that you are the user you say you are by requesting and checking a password. Each RACF user ID has a unique password.
>
> You should be the only one who knows your password. That way, RACF can ensure personal accountability. (No one can log on with your user ID.)
> When the security administrators define you to RACF, they assign you a user ID and an initial password. Your initial password will allow you to log on to the system the first time. As soon as you log on, RACF requires you to supply a new password of your choice. This password must be between 6 and 8 characters long: both numbers and letters are required. Your password will expire after 60 days. RACF also maintains a history of your 12 most recently used passwords, so you cannot re-use any of your 12 prior passwords.
>
> RACF enables the systems security department to define individuals and groups who use the system RACF protects. For example, for a secretary in our company, the security administrator uses RACF to define a user profile that defines the secretary's user ID, initial password, and other information, which will allow them to access information.

What else does RACF do?

> Besides uniquely identifying and authorizing you, RACF records what you do on the system. It keeps track of what happens on the system so that systems security can monitor who is logged on the system at any given time. RACF reports if persons have attempted to perform unauthorized actions. For example, RACF can record when someone who does not have the proper authority tries to use or change company data.

Additionally, all procedures are being documented. The content has outgrown a 3 inch binder. Topics include:

- Overview of the security program

- Request Processing
- Legacy Online Security
- RACF Processing
- Violation Reporting

User Accounts

A naming convention needs to be created to identify users.

By creating a naming convention for usernames, you can save yourself a great deal of trouble. Instead of making up names as you go along (and finding it harder and harder to come up with a reasonable name), you do some work up-front and devise a convention that will be used for all subsequent user accounts. Your naming convention can be very simple, or the description alone could take several pages to document. The exact nature of your naming convention should take several factors into account:

- The size of your organization
- The structure of your organization
- The nature of your organization

The size of your organization matters, as it dictates how many users your naming convention must support. For example, a very small organization might be able to have everyone use their first name. For a much larger organization this naming convention would not work.

An organization's structure can also have a bearing on the most appropriate naming convention. For organizations with a strictly-defined structure it might be appropriate to include elements of that structure in the naming convention. For example, you could include your organization's departmental codes as part of each username.

The overall nature of your organization may also mean that some naming conventions are more appropriate than others. An organization that deals with highly-classified data might choose a naming convention that does away with any personally-identifiable ties between the individual and their name. In such an organization, Maggie McOmie's username might be LUH3417.

Here are some naming conventions that other organizations have used:

- First name (john, paul, george, etc.)
- Last name (smith, jones, brown, etc.)
- First initial, followed by last name (jsmith, pjones, gbrown, etc.

- Department code followed by user's last name (029smith, 454jones, 191brown, etc.)[4]

[4] Red Hat

It is hoped to develop a naming convention that ensures that no functionality is associated with the account ID, so that the account owner could have access privileges changes without having to assign a new account – for example, the geographic location of the individual will not be included in the user name. The current convention uses the first initial and last name – with a total length of 8 characters. Security suggests to change the convention to avoid having to create new accounts when name changes take place. The enormity of the impact of this suggestion to the corporate users overshadows the amount of work to process name changes. Hence JSMITH remains.

Password parameters that exceed the standards suggested by the National Association of Insurance Commissioners (NAIC) baseline are applied to the security system:

- 6-8 characters in length
- Must contain both numbers and letters.
- Must expire at the initial sign on.
- Expire every 60 days.
- History of 12 prior passwords before a password could be reused.
- The security system did not recognize lower case letters, so requiring both upper- and lower-case letters is not an option.

Demographic groups are developed to identify the account owner. The groups have no functionality associated with them:

- Agents – for employees of the independent insurance agencies.
- Employee – for employee accounts (Human Resources advises security when an employee is separated)
- Services – for services running on the mainframe.
- Temps – for temporary, consultants and contractors. (Since these owners are not in the personnel system, the accounts expire every 90 days. The sponsor of the owner must submit the Move-Add-Change (MAC) form to extend the owner's access)
- Test – for accounts used for testing purposes.

Data Objects

The existing information objects (datasets) are inventoried – over 129,000 are enumerated. A naming convention is developed, categorizing the objects in terms of lines of business: Policy, Claims, Billing, Accounting and Actuarial

applications. Additional naming conventions are developed to segregate objects based upon company number and to identify test data from production data:

The mask for the objects' name is AAAANNPX.SECD.othernodes

- AAAA – to define the business line; BILL for billing, FINA for accounting, etc.
- NN – to identify the company number: 00 for BIC, 01 for the acquired company
- P – to define the data status: P for production; D for development.
- X – to define the data structure: V for VSAM; N for Non-VSAM
- SECD – the secondary line of business; DRCT for Direct Bill (in the billings line of business), for example.
- Othernodes – descriptive identifiers, such as MASTERFIL.

Hence an object might be named FINA00PN.CKWR.WEEKLY for the weekly production checkwriter file for the BIC accounting application.

The creations of the object mask is critical – it is used to provide "inheritance" of access privileges, thus avoiding having to construct specific access control lists for each data object. For example if we want the billing department group to have read access to all billing production data objects, we set the permissions as follows (asterisk are wild cards):

```
PERMIT BILL00PN.**   ID(billing group) ACCESS(READ)
PERMIT BILL01PN.**   ID(billing group) ACCESS(READ)
```

Note: this will allow read access to both BIC and the acquired company billing objects.

At the end of this task, there are access control lists for 344 development masks and 439 production masks.

Groups

The next task is to identify the individuals who need access (and what type of access) to the data objects. Then, construct functional groups (as opposed to demographic group described above) and connect user accounts to the appropriate groups.

Some of the groups are:

- ONLINE – this group has access to the online applications. The proprietary online security system (not RACF) determines the specific application-level access to be granted. However, an account must be

connected to this group to even get to the online applications.

- PRODUCTION – this group's sole member is the automated scheduler systems. It is the only group that can update production information. (Except for the objects that are updated by the ONLINE group.)
- Developer (programming) Groups are segregated so that one programming team can not add/delete/modify test data "owned" by another programming team:
  - ACCOUNTING
  - ACTUARIAL
  - BILLINGS
  - CLAIMS
  - POLICIES
- BUS ANALYSTS – this group has the responsibility for User Acceptance Testing of changes, prior to being moved into production.
- REPORTS – this group has the ability to generate periodic and ad hoc reports, using production data.

At the end of this task, 490 functional groups are constructed. Initially, there is only one user account in many of the groups – this is fundamental process: don't permit user accounts access; all access is by group membership. As additional personnel need access, they will be added to the appropriate group.

The labor-intensive task of linking the groups (with the appropriate access authority) to the various groups is begun. Two week later, the task is completed.

User Training

Online Applications:

The users sign on the online main menu by starting an online session, then being prompted for a user ID and password. Prior to the migration, the user ID and password was authenticated by the online security system. The sign-on modules will be changed to use RACF as the authentication mechanism, in lieu of the proprietary user ID – password file. The proprietary user IDs are used to populate the RACF database:

- 12,000 Agents accounts
- 2,500 Employee accounts
- 500 Services account
- 300 Temps accounts
- 50 Test accounts

Passwords are "harvested" from the proprietary file and input to the RACF database (where they are hashed), with the option that would force the user to select a new password at sign-on time.

The procedures for signing on and selecting a new password are communicated to the employees and agents a week prior to the migration.

Programming Staff:

The programmers sign onto the new mainframe to begin testing the existing inventory of programs, to ensure that they will function properly with the new operating system. The time-sharing environment that they are using is significantly different than the one they had been using – no passwords were required in the old one. There are over 9,000 programs to be tested – a daunting task, but fortunately it is not a security responsibility.

A training document is created (complete with screen prints) and hands-on training is conducted for the team leads – approximated 20 personnel. The team leads then conduct hands-on training for the rest of their team – approximately 200 personnel in all. This process continues without any major glitches.

The War Room

Prior to the migration, a conference room is outfitted with 10 PC's and telephones. (We are making progress – replacing dumb terminals with PC's that run a terminal emulation program to communicate to the mainframe via the LAN) This will serve as the Help Desk during and after the migration. Volunteers are recruited from the various programming teams to staff the war room. Training is provided on how to guide a caller through the password reset process. A problem tracking mechanism is implemented to document issues and to ensure that all issues are resolved.

Event Monitoring

Reports are created using the RACF report writer to monitor unusual and/or suspicious activity:

- ALL RACF COMMANDS – records all activity conducted by individuals with administrator authority. This is an audit trail of activities of all RACF administrative personnel, used to ensure only authorized changes are performed.
- DATASET VIOLATIONS – records all unsuccessful attempts to access the data objects.
- SELECT IDs – records the use of all emergency (FIRE AXE) account IDs, used to fix production problems. These are used to make "quick fixes" to erroneous data, thereby ensuring that the online applications are available at 7:30 a.m. each morning.
- SIGN-ON VIOLATION – records all unsuccessful sign-on attempts and

identifies if the attempt was denied due to a bad password or an undefined account ID.

Security Analyst of the Week (SAW) duties are documented and a checklist is created for the daily review of the various reports. Instructions are documented for the escalation of any significant, unusual or suspicious event. The SAW duties are rotated weekly among the security administrators.

After Snapshot – November 1999

Well, D-Day has arrived. The new mainframe, operating systems and security system have replaced the old platform. It is 7:30 Monday morning and the War Room is ready for action.

We are pleasantly surprised. Only 100 phone calls the first day, easily handled by our 10 volunteers. The level drops to about 50 calls per day for the rest of the week. No nightmares to be found. A trickle of calls are received the following week. The War Room is decommissioned and calls are routed to the "normal" help desk for resolution.

A Pending Crisis

On D-Day, all users select new passwords. Sixty days hence, they will all be prompted to select new passwords on/about the same day. What will the phone volume be? To spread out the expiration day, password intervals (default is 60 days) are shortened by:

- 8 days for 20% of the user base;
- 6 days for 20% of the user base;
- 4 days for 20% of the user base;
- 2 days for 20% of the user base.

As the expiration periods occur, the password interval is re-set to 60 days. The crisis is avoided.

Impact

The migration to the new security systems provides significant benefits to BIC:

- A centralized security department now exists, with appropriate standards, procedures and guidelines documented.
- Access to the systems is password-controlled, which have the appropriate functionality, e.g, expiration, limited re-use, lockout, hashing.
- Data objects are protected by default.

- Suspicious and/or unusual activity is recorded and reviewed.
- Data objects are protected by default.
- Production downtime due to accidental testing parameters has been eliminated.

In December 1999, internal audit conducted an exhaustive review of the security system, standards, procedures and guidelines. Their final report did not identify any significant defects or material weaknesses associated with the security system. A subsequent review by external auditors confirmed the findings of the internal audit department.

The work has just begun. The new challenge will be to address the new issues:

"Businesses that successfully lead in the information age will be those that efficiently find the balance between protecting corporate and customer information, and making sure good ideas and creativity are not "pent up" and made ineffective." [5]

[5] Ramana

References

IBM. “Resource Access Control Facility”. November 2003. <http://www-1.ibm.com/servers/eserver/zseries/zos/racf/>

Newstaff Inc. “ISO 17799 Security Organization, 1995-2005 <http://newstaff.com/criteria/iso17799/2.htmlIS0 17799>

Red Hat, Inc. Red Hat Linux System Administration Primer, 2003. <http://linux-rep.fnal.gov/rhl-sap-en-9/ch-acctsgrps.html> (From the Fermilab Linux Repository)

Ramana, S. V., “Securing the Enterprise” Network Magazine, January 2003. <http://www.networkmagazineindia.com/200301/cover9.shtml>

United States. National Institute of Standards and Technology. Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26. November 2001. <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>