GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Version 1.4b

Securing Data in a Financial Institution Environment

Eric A. Pulse
October 22, 2002

Overview

All too often in today's financial institutions, individual employee access to the core banking application, which houses and processes your bank account information (checking account, savings account, mortgage loan, etc.) is inconsistent at best and abysmal or nonexistent at worst. The problem? Duties are not adequately segregated at the application level and employees have more access to application functionality than is needed. Problems are accentuated by employee turnover, knowledge (or lack thereof) of the system, and inadequate passwords. Inadequate application security can affect the confidentiality, integrity and availability of institution data. Confidentiality of the data can be compromised by an insufficient authentication policy and enforcement, a compromised user ID and password, or core application functional security that grants access to an individual that does not possess the immediate need for such access. The integrity of the data can be compromised by unauthorized access to bank data due to inadequate application security. Availability of the data can be compromised by an unauthorized administration user denying access to others within the organization by altering their functional access.

This document addresses some Best Practices for improving application security within the financial institution. Topics that will be addressed are:

- Organizational and Operational Controls, including:
  - Management Directive (i.e. policies and procedures)
  - Job Descriptions
  - Segregation of Duties
  - Removal of User IDs
- Logical Controls, including:
  - Authentication
- Application Controls, including:
  - Input Controls
  - Processing Controls
  - Output Controls
  - Departmental Input
- Report Review
- Budgetary Considerations

Organizational and Operational Controls

© SANS Institute 2000 - 2005 Author retains full rights.

A thorough and up-to-date organization structure is important to provide a well-defined and orderly business environment, including formalized organization charts, current job descriptions for each position in the organization, and current operating policies and procedures. Additionally, proper levels of responsibilities should be clearly defined for adequate segregation of duties. This structure should not permit the perpetration and concealment of material errors or irregularities. Functions unique to processing should be divided within the organization to prevent or detect errors or irregularities in the normal course of business.

Policies

In any organization, financial institutions included, the best directives are those that come directly from the top. Management directives can be effectively defined and delivered through the utilization of board approved policies, standards and procedures. The financial institution industry has added incentive to develop adequate policies – federal regulation. A recent governmental directive, Section 501(b) of the GLBA of 1999, mandates standards for safeguarding customer information within financial institutions, of which application security is an integral part. Section 501(b) of the Act states, "The guidelines require each institution to implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities." [1]

Also, the Federal Financial Institutions Examination Council (FFIEC), which is comprised of the federal financial institution governing bodies (FDIC, FRB, NCUA, OCC, OTS) issued a statement of position, SP-3 relative to end-user computing risks. The issuance states that, "Control practices and responsibilities to manage these activities should be incorporated into an overall corporate information security policy. Such a policy should address areas such as: [2]

- management controls,
- data security,
- documentation,
- data/file storage and backup,
- systems and data integrity,
- contingency plans,
- audit responsibility, and
- training."

Job descriptions

Job descriptions should be developed to ensure they accurately reflect the

© SANS Institute 2000 - 2005 Author retains full rights.

current duties performed by employees. Job descriptions should also be prepared using a standard job description format. Job descriptions should be reviewed on a regular basis to ensure their completeness and accuracy. Written job descriptions can provide:

- Clearly defined responsibilities and accountabilities for all positions.
- Guidelines to measure performance for informal feedback when employee performance is evaluated.
- A method to ensure that all functions performed within the organization are assigned to an individual and duties are properly segregated between functions.
- Guidelines for developing or evaluating salary ranges.
- An orientation and training tool for employees new to a position.

A policy should be instituted where all position descriptions are reviewed annually for accuracy and to ensure that duties being performed are done so by the direction of management. Considerable analysis should be completed when developing the position descriptions. Local and regional markets and peer data centers can be contacted and studied during the development of appropriate position description.

Segregation of Duties

All too often security and functionality are granted to an individual without proper research as to specific job responsibilities. Every employee's functional access to the core banking application should be commensurate with his/her day-to-day job responsibilities. Many times employees are granted full access to the system because they transferred in from another department and their supervisor lobbied for additional access to the functions needed in that department. Obscurity is regularly often the excuse or reason. How many times have you heard, "John may be in possession of that access within the system but he wouldn't know what to do with it anyway." No one individual should have access to every function within the application. If that happens, you can throw accountability out the window.

Small financial institutions may lack adequate staffing to fully segregate duties and responsibilities. In such cases, additional precautions and controls should be established to ensure system integrity. These measures can consist of rotation of duties and additional audit coverage. Federal bank examiners pay particular attention to this. At a minimum, management should ensure that an adequate number of employees receive training on the system to minimize dependence on any one person. To facilitate communications with vendors, a primary and alternate contact should be designated to handle system problems.

Removal/Disabling of User IDs

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Upon termination or transfer of a bank employee, it is imperative that the IT staff responsible for maintaining user IDs and passwords be notified in a timely manner. There must be a formal process for notifying IT staff upon termination/transfer of an individual. A terminated user's access should be terminated or disabled and that access should include the local/wide area network, the operating system, core application, any remote access medium, and any physical access keys such as standard keys or card access keys. The Human Resources department should initiate the process and approvals should be validated by supervisory signatures. This notification should also be stored for future verification.

Logical Controls

Inadequate logical access security controls increases the potential for losses resulting from technical and business exposure. These exposures can result in minor inconveniences or total shutdown of the computer functions.

Computer files should be protected from unnecessary or unauthorized access by controls that reduce the risk of intentional or unintentional misuse, theft, alteration or destruction. Access controls apply to computer department personnel, users, management and hardware and software vendors.

Authentication

Financial institution employees should be required to authenticate to the core banking application using a unique user ID and password. Where possible, legal banners should be displayed warning that unauthorized access will be prosecuted to the fullest extent of the law. This can provide some legal recourse for prosecuting intruders.

In the aforementioned "Policies" section, it was noted that sound policies should be developed and approved by management and the board of directors in order to provide a management directive. Within those policies, a sound password policy should be developed.

Good passwords consist of a combination of case-sensitive alpha-, numeric, and special characters that are a minimum of six characters in length. According to Shriver and Wold, 1989, "...the number of possible random number combinations for various lengths of passwords are listed in the following table. The letters I and O are excluded to avoid confusion with the numbers 1 and 0, which leaves available 24 letters and 10 numbers."[3]

Password Length	Number of Combinations
1	34
2	1,156
3	39,304

© SANS Institute 2000 - 2005 Author retains full rights.

4	1,336,336
5	45,435,424
6	1,544,804,416
7	52,523,350,144
8	1,785,793,904,896

These statistics include passwords consisting of only alpha and/or numeric characters. Introduce case-sensitivity and special characters and the number of combinations would grow exponentially.

The best password policy is quickly rendered useless if users are sharing their unique passwords or if, more commonly they are posted at their workstation. Take a walk through any organization, financial institution or otherwise, and you are sure to find a fair number of passwords on the bright yellow Post-It notes hanging from many workstation monitors or keyboards. The password policy should strongly encourage users to keep their passwords private and to change them periodically. Systems can force password changes on a regular basis and password change intervals should depend on the sensitivity of systems and data accessible by each respective user. The more sensitive the system or data that is accessible by the user, the more frequent the password should change.

There are some operating systems that have the capability of effectively driving the password policy by providing system settings that allow institutions to more granularly define password composition. For example, IBM's OS/400 operating system or various versions of UNIX (AIX, HP-UX) provide such password composition granularity.

The following table is intended to show an example of some capabilities available in one operating environment for password definitions, in this case, OS/400, provided by IBM. [4]

Password system values:

Name in Operations Navigator	Description of system value	Name in command interface
Password level	Sets the password level for the system.	QPWDLVL
Minimum password length	Sets the minimum length for a password.	QPWDMINLEN
Maximum password length	Sets the maximum length for a password.	QPWDMAXLEN
Require at least one digit	Sets the passwords used on the system to use at least one digit.	QPWDRQDDGT

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Restrict consecutive digits	Sets the passwords on the system to restrict consecutive digits.	QPWDLMTAJC
Restricted characters	Specifies the characters to be restricted.	QPWDLMTCHR
Restrict repeating characters	Specifies whether or not to restrict repeating characters.	QPWDLMTREP
Require a new character in each position	Sets the passwords on the system to require a new character in each position.	QPWDPOSDIF
Password reuse cycle	Specifies when a password can be used again.	QPWDRQDDIF
Password expiration	Specifies when a password expires.	QPWDEXPITV

Various versions of UNIX provide the ability to define passwords using the following variables:

- Password length restrictions (minimum and maximum)
- Minimum password history
- Password age restrictions (minimum and maximum)
- Minimum # of alphabetic characters
- Minimum # of non-alphabetic characters
- Minimum # of repeated characters
- System generated passwords (although these passwords are often written down because they are usually difficult to remember)

Common verbiage from a board approved password policy might read as follows:

> All user-chosen passwords for computers and networks must be difficult to guess. **Words in a dictionary, a derivative of user-IDs, and common character sequences such as "123456" must not be employed.** Likewise, personal details such as spouse's name, license plate, social security number, phone number, pet name, child name, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locat6ions, common acronyms, and slang must not be employed. An example of an excellent password would be "Mu2DbyU2."

© SANS Institute 2000 - 2005,

Clearly defined policies help the everyday user to better understand the importance of sound password practices.

Application Controls

Application controls in a financial institution environment are designed to protect the accuracy and integrity of the data residing on the system. According to Webopaedia, data integrity refers to the validity of the data. Data integrity can be compromised in a number of ways, including data entry error or errors during transmission from one computer to another.[5]

Application controls are safeguards that protect the integrity of system information. According to Shriver and Wold, "Application controls are methods of insuring that only complete, accurate, and valid data are entered and updated in a computer system; that processing accomplishes the correct task; that processing results meet expectations; and that data are maintained." [6] Application controls can consist of:

- Controls that are designed to ensure that transactions are properly authorized and approved
- Forms that properly document transactions
- User controls over regular data, file maintenance, inquiry and error correction transactions
- Authorizations, segregation of duties, audit trails, logs, data edits performed and balancing and verification procedures
- Error detection, correction and resubmission procedures

Application controls commonly consist of input, processing, and output controls. Warren, Edelson, and Parker indicate that "**input** is considered to be the initial recording of a transaction and the subsequent activity until that transaction is recorded in the computer records and update files." [7] Controls over input can include dual control, segregation of duties, sequentially numbered documents, transmittal documents, batch dollar totals and item counts, supervisory review, authorization, safekeeping, documentation, data edits, and error handling.

"Processing includes all of the functions performed within the computer, including editing, calculating, summarizing, categorizing, and updating," [8] state Warren, Edelson, and Parker. Processing controls can include sequence checks, batch dollar totals and item counts, run-to-run control totals, data edits, field checks, record checks, matching, internally generated transactions, rejects, file completion checks, reconciliation, balancing and settlement.

Output is the result of processing the input data. Output controls can include report scheduling, distribution lists, controlled pick-up, and sensitive document procedures.

© SANS Institute 2000 - 2005, Author retains full rights.

Departmental input

One of the first steps to adequate application security is departmental input. The individual or committee responsible for the development and maintenance of application security should assemble meetings with key departmental management and supervisors who are intimately familiar with the functions performed within their respective department. A listing of all available transaction codes within the application should be distributed to each manager/supervisor. These meetings are usually (or should be) the site of heated debate over the need for certain access. Departmental managers/supervisors typically request more access than is needed. Internal auditors and information security specialists typically err on the side of caution and recommend very restricted access. Executive management should play the role of intermediary or arbitrator. Typically, executive management makes the decision based on the level of risk the institution is willing to accept.

Application security, like all other security in the organization should be based on the principle of least privilege. As Chris Hare noted, “Like its counterpart in the function role, the concept of least privilege means that a process/user has no more privilege than what it really needs in order to perform its functions.”[9]

Report Review

Each core banking application provides the institution with various file maintenance and transactional activity reports. The key is to ensure that the appropriate file maintenance and transactional activity reports are reviewed on a regular basis to ensure the accuracy and integrity of the maintenance and transactions being processed. It is important to remember that each individual responsible for reviewing file maintenance should not possess the functional access within the application to perform the maintenance that is being reviewed. Therefore, management should consider implementing a report review procedure where the individual responsible for reviewing a particular report does not have functional access within the application allowing them to make changes that are reflected in the particular report being reviewed. This will provide for more adequate separation of duties and reduce the risk that unauthorized system or account changes may go undetected. An example of this, a kind of quasi-Salami attack (a series of minor crimes that are part of a much larger crime, ie. when large amounts of money can be skimmed from an account(s) in very small amounts), follows:

> A bank employee, a departmental manager, is responsible for the monitor and review of certain monetary maintenance transactions (i.e. refund of NSF fees). This employee also has the functional authority within the application to perform the same monetary maintenance transactions that she is responsible for reviewing. The employee hatches a scheme to embezzle funds from the institution by refunding NSF fees to her account. Oh, by the

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

way, this individual is also responsible for monitoring employee account activity, a practice common in the financial institution industry. Since this employee is responsible for monitoring and reviewing the particular NSF fee refund transactions, she quickly realizes that NSF refunds to her account are unnoticed since the NSF fee general ledger account is debited while her account, not the customer's account, is credited. The customer is unaware that the refund even happened because, after all, it was legitimate in his eyes.

In this example, you can see the importance of maintaining adequate segregation of duties and a thorough maintenance transaction review process.

As a guide, management should perform the following as a first step on the road to improving application security/securing data:

- Identify individual user job function(s) and assigned application security privileges;
- Compare individual user application security privileges to the appropriate security template;
- Identify any non-compliance with institution policies and procedures;
- Identify discrepancies between templates and assigned user security privileges; and
- Document reasons for security discrepancies.

Budgetary Considerations

As with anything, money matters. Chris Cunningham notes that, "in a world where budgetary constraints are often the norm, information security managers could be finding difficulty adequately securing their company's data. Some guidance for information security managers whose bosses have tightened the purse strings includes:"[10]

- Developing a corporate security policy
- Use of secure shredding procedures for sensitive documents
- Lockdown of desktop configurations
- Tightening configurations on all border routers
- Ensuring all systems are up to date on patches
- Ensuring all systems are running only necessary services
- Maintaining a detailed network map
- Learning TCP/IP
- Maintaining anti-virus updates
- Maintaining strong passwords throughout the organization

Other Controls

There are, of course, many other things to consider when securing data in a

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

financial institution. Institutions should ensure the protection of files containing sensitive information on the local/wide area network. Institutions should also eliminate any unnecessary modems that allow remote access to/from the network that don't pass through a firewall. Institutions should also refer to any application vendor's SAS 70 "User Control Considerations" for guidance on security data.

Conclusion

The appropriate security controls will obviously vary from institution to institution based on a variety of factors from staff size to management philosophy. Bank management should ensure that the appropriate Defense in Depth (DiD) mechanisms, of which application security is one, are in place to insure the confidentiality, accuracy, and integrity of system data. Common DiD mechanisms include:

- Policies and procedures
- Physical security (door locks, etc.)
- Segregation of duties
- Application security
- Network security
- Firewalls
- Network/firewall monitoring
- Intrusion detection systems
- Report reviews
- Auditing

By implementing effective controls to secure data in a financial institution, organizations can rely on the confidentiality, integrity and availability of their customers' information.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. FDIC. “Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information.” 2001. URL: http://www.fdic.gov/news/news/financial/2001/fil0168a.html

2. Federal Financial Institutions Examination Council. SP-3. “Joint Interagency Issuance on End-User Computing Risks.” January 1988.

3. Shriver, Robert F. and Wold, Geoffrey H., Computer Crime, Techniques for Preventing and Detecting Crime in Financial Institutions, Rolling Meadows, Illinois, Bankers Publishing Company, 1989. 107-108. ISBN: 1-55520-161-X.

4. IBM iSeries Information Center. “Password Overview.” URL: http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm?info/rzakz/rzakzpasswordoverview.htm

5. Webopaedia. “Data Integrity.” 31 October 2001. URL: http://www.webopaedia.com/TERM/d/data_integrity.html

6. Shriver, Robert F. and Wold, Geoffrey H., Computer Crime, Techniques for Preventing and Detecting Crime in Financial Institutions, Rolling Meadows, Illinois, Bankers Publishing Company, 1989. 247. ISBN: 1-55520-161-X.

7. Warren, J. Donald, Jr., Edelson, Lynn W., Parker, Xenia Ley, Handbook of IT Auditing, Boston, Massachusetts, WG&S/RIA Group,1995, B1.02[1], B1-3

8. Warren, J. Donald, Jr., Edelson, Lynn W., Parker, Xenia Ley, Handbook of IT Auditing, Boston, Massachusetts, WG&S/RIA Group,1995, B1.02[1], B1-5

9. Hare, Chris. “Security Architecture Domain.” April 1999. URL: http://www.in-focusnet.com/resources/Study/cissp/10Domains/Domain_6.htm

10. Cunningham, Chris, “Cheap Tricks for Information Security.” SC Magazine, April 2002 (2002): 27

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.