Global Information Assurance Certification Paper

Case Study: Information Security Concerns in Moving to an In-House Data Center

Wallis McMath

August 18, 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

Abstract

The Bank that I work for is located in the United States and will be called the "Bank" in this paper. This paper details the plan used to move the core processing requirements for the Bank from a remote third party processor to an in-house system with emphasis on information security issues relating to establishing an in-house data center. Security related and operational issues had to be understood and existing policies modified to incorporate the move to an in-house system. The three primary goals of the project were: (1) to move the core processing of the Bank to a new in-house system over a weekend without impacting our customers or internal users, (2) receive positive results from the Federal Information Technology Examination which would occur only three months after the move to an in-house system and (3) Successfully conduct a full scale disaster recovery at a vendor's recovery facility five months after the conversion. To achieve positive results for the Federal Information Technology Examination a complete overhaul of the existing information security related documents would be required and a disaster recovery plan for the data center would also have to be written and implemented. The move to an in-house system would significantly increase the Bank's scrutiny by the Federal examiners during their annual Information Technology examination. In reviewing various information security literature, it was obvious that our existing information security policies, standards and procedures needed to be, in many places, created or updated to conform to federal and industry standards.

As the Chief Information Officer (CIO) of the Bank, I was responsible for the overall conversion plan. I chaired the weekly management meetings and personally made the decisions on all hardware, software, power system security system and I wrote the required information security policies and standards. I also wrote most of the disaster recovery plan.

Before

The Bank had multiple PC based servers, a wide area network (WAN) and outsourced its core data processing to a third party. Each year, federal examiners have conducted a Safety and Soundness examination of the Bank. The Information Technology examination was included as part of the overall

Safety and Soundness examination and not as a separate examination because the core processing was performed by a third party at their facility. The Federal examiners relied on a SAS70 report, an industry standard, for the third party as to the safety and soundness of their information security practices. The contract with the third party was due to expire in 2002 and required new terms to be provided a year in advance. As the new CIO for the Bank, I elected to examine three alternatives: (1) renew the contract with our third party vendor, (2) bring the software development staff in-house and out source the mainframe computer system and its operations staff or (3) bring the new mainframe system in-house with our own operations group and hire our own software development staff. Over a three month period a study was conducted to evaluate all three options. The result of the study indicated a significant savings for the Bank by bringing the total system in-house with our own operations and software development staff. However, the change from an outsourced environment to a totally in-house system would be very difficult and could cause irreparable harm to the Bank if it was not successful. The recommendation to proceed with the in-house option was approved by the COO and CEO of the Bank. This approval started a one year long planning process, the end of which, would culminate in a move from the remote third party processor to a new in-house system over a weekend and was to be transparent to both employees and customers.

The Bank already had in-house PC based servers, an IBM AS400 and a wide area network (WAN) consisting of over ninety remote branches. The Bank's WAN had a firewall and a DMZ, but there was no written policy in many areas such as a firewall standard that could be used to measure compliance of firewall settings. There was no formal change control policy for PC based servers or the network. An information security policy was in place, but had not had any significant updates in a considerable amount of time. There was no real disaster recovery plan, only a semblance of one. All customer data and financial data was stored on the computer system managed by the remote third party vendor and therefore the above issues were not considered to be required.

Overall availability of the system was not at the level that it should be primarily due to the mix of computer equipment being used. Winn Schwartau[1] explains how availability is effected by "Cyber (computer, network and information security), Physical (the wires, silicon, glass and structures) and People (employees, consultants, suppliers, partners and everyone in contact with your company)". Schwartau further states that these three areas should be dealt with in assuring availability of any computer system. The plan included steps to insure availability of the system and the cyber, physical and people aspects as described by Schwartau were included in the plan.

As part of the move to an in-house data center, the Bank would continue to run the same core application software that was used in the out-sourced environment, however, one of the loan applications was so out of date, that a conversion would have to be performed on it to bring it to a current release level

In addition, a customer information application was being replaced by another functional equivalent, but totally different application. There were twenty plus other applications that would have to be tested in the new environment. In the out-sourced environment, the vendor was running on an IBM platform running the VSE operating system. The in-house system would use the IBM MVS operating system, so all applications would have to be extensively tested and new Job Control Language (JCL) would have to be developed. All new operational procedures would have to be written and tested. All ATM network connectivity would have to be moved to terminate in our new data center instead of the vendor's remote facility in another city with minimal interruption of service.

The plan also included a requirement that all information related policies be updated in all areas. Many policies, standards and procedures required by the federal examiners policies did not even exist. The examiners expect to everything to be documented to insure that appropriate controls are in place and being followed. We utilized Kevin Mitnick's book, The Art of Deception[2] and other books to assist us in deciding what additional security policies needed to be developed. The existing policies did not completely conform to the concept of policies, standards and procedures as noted in The CISSP Prep Guide[3]

As part of updating all of our policies to include standards and procedures, we also knew that we needed to include additional information about the "Triad of Information Security - Confidentiality, Integrity and Availability"[4].

Regulatory Background

Many companies use external auditors to conduct technical and/or financial audits of their business. Banks also undergo examinations by the Federal Government. The following is an overview of the Federal Government involvement with banks.

The Federal Financial Institutions Examination Council (FFIEC) is a formal federal interagency group comprised of the following federal agencies: Board of Governors of the Federal Reserve System (FRB), The Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS). The FFIEC web site is a very important site that the person in charge of information security (hereinafter referred to as the CIO) should know extremely well.

Financial institutions are examined on an annual basis by one of the five member agencies of the FFIEC. The examination guidelines are produced by the FFIEC and used by all member agencies in conducting their respective examinations of financial institutions. The FDIC performs more examinations than any of the other FFIEC member agencies.

Since 1996, the FFIEC has been using their FFIEC Information Technology Examination Handbook (Handbook) for all information technology examinations. In 2002, the FFIEC announced that it would be replacing the Handbook which consists of thirty chapters with a series of booklets that would introduce new topics and replace the existing examination chapters. As of July 2003, a New Information Security booklet, issued in January 2003, replaced all security related information in the thirty chapters of the 1996 Handbook, including chapters 12, 13 and 14. In May 2003, two additional booklets, Supervision of Technology Service Providers and Business Continuity Planning were published which replaced Chapters 2 through 7 and chapter 10 respectively from the 1996 Handbook. No dates have been published by the FFIEC as to availability of future booklets replacing the other chapters of the 1996 Handbook.

The 1996 Handbook can be found at the FDIC website[5] and the new revised edition Information Technology Examination Handbook containing booklets can be found at the FFIEC website[6]. The revised Handbook consists of a series of booklets, most of which at this time have not been published. The booklets are identified below:

Available Booklets
- Business Continuity Planning
- Information Security
- Supervision of Technology Service Providers

Un-Published Booklets
- Audit
- Development and Acquisition
- Electronic Banking
- Management
- Operations
- Outsourcing
- Payment Systems: Fedline
- Payment Systems: Retail
- Payment Systems: Wholesale

The FDIC has a scaled down Information Examination for Financial Institutions with low to moderate technology and will not be used or discussed in this paper. This paper will focus on all financial institutions with a greater technology risk that will continue to be examined based on the Federal Financial Institutions Examination Council Information Technology Handbook. (The term "Handbook" will be used to denote the 1996 Information Examination Handbook for financial institutions and the new booklets that are being announced to replace the 1996 edition.)

The FDIC also regularly publishes Financial Institution Letters[7] (FILs) which address many areas, including information technology issues. CIOs in financial institutions should regularly review the FDIC site for updates to the Information Technology Handbook and to newly released FILs. The FIL's are the FDIC's way to distribute timely information to financial institutions.

Associated with each chapter or booklet is a workprogram document that is a detailed procedure to be used by examiners in conducting their examination. The CIO of a financial institution and his senior staff should review each step in the workprogram for each of the areas to be examined with their staff. The results of the CIO's staff review of all of the workprograms should tell the CIO which areas they need to concentrate on to be prepared for their next examination. Some of the detailed steps that are followed by the examiners in their workprogram are quantitative in nature and are relatively easy to determine if an institution is in compliance with a given requirement. However, many areas of the examination are very subjective and while the CIO may think he is in compliance, the examiner may not agree. The CIO will normally have an opportunity to try to convince the examiner that their institution is in compliance on any given issue that is raised during an examination. If the CIO fails to convince the examiner that he has complied, the examiner will produce a "finding" which means that the organization did not meet an examination standard in a particular area. The examiners report is presented to the institutions Board of Directors and generally, the institution provides a management response back to the FDIC which indicates what corrective action will be taken by the institution.

The 1996 version of the FFIEC Information Technology Examination Handbook is extremely outdated because of the rapid changes in information technology since 1996. The newly released booklets on Information Security and Business Continuity Planning are much more in line with current information security related literature.

The FFIEC examiners produce a summary report at the end of their examination for senior management which includes a summary of any findings (e.g. non-compliance) and they give the bank they examined a composite rating of 1 to 5 (with 1 being the best). The FFIEC defines a composite rating of 1 as "Data centers in this group are sound in almost every respect. If deficiencies are noted, they are minor and can be handled routinely and without further supervisory involvement." A composite rating of 2 is defined as "Data centers in this group are fundamentally sound, but may reflect modest weakness. Deficiencies are generally corrected in the normal course of business. Therefore, the need for supervisory response is usually limited." Senior management, with good reason, always wants a 1 rating. A rating of 3 or higher is unacceptable.

The FFIEC also oversees bank compliance with the federal Gramm-Leach-Bliley Act which deals with protecting the confidentiality of consumer information. It

was imperative that the Bank develop policies and standards to address and protect the confidentiality of our customer data. The FFIEC will also oversee compliance with the Patriot Act (which becomes effective on October 1, 2003) and, among other things, requires financial institutions to authenticate their customers when establishing new customer relationships.

The purpose of including the above information on the FFIEC is to underscore the importance that the CIO of a bank must know and understand what the FFIEC expects from their bank in terms of complying with their information security related regulatory requirements for Information Technology. CIO's are responsible for providing information security for their respective institutions using industry standard guidelines and also making sure they are complying with the FFIEC requirements. In general, most sound financial institutions will exceed the federal requirements for information technology.

During

Once the decision to move to an in-house system was approved, work began immediately to develop a detailed plan of all steps required to accomplish the move along with the other issues identified above. The majority of the plan detail was developed over the following two months. Three committees were formed and each committee met once a week throughout the entire conversion period of one year. A committee was formed for the loan application conversion, a second committee was formed for the customer information application conversion, and a third management committee was formed of managers to oversee the overall plan. A significant amount of attention was placed on developing both the physical and data security requirements early in the process instead of adding them at the end of the conversion. The participants of the management team included managers from our Information Technology Department (which includes data security), Retail Operations, Loan Operations, Finance and Internal Audit. Written minutes of each meeting were recorded. From start to finish, the plan covered a period of twelve months.

The plan to move to an in-house data center included the following major areas:

- Physical Security
- Application and Data Access Security
- Data Center Hardware
- Power, UPS, Generator and HVAC Requirements
- Incident Reporting
- Ancillary System Software Requirements (i.e. Security, disk management, tape management, etc.)
- Installation and Testing of New Operating System
- Hiring and Training New Data Center and Development Employees
- Testing All Applications
- ATM network Security and Connectivity
- Change Control

Turnover
Business Continuity Planning
Mock Conversions
Contingency Plan

Physical Security

One of the first decisions to be made was the location of the new data center. Initial thoughts were to locate the data center at another facility across town, but we realized that we would have the same type of problems we had when the data center was in another state. By performing some employee office consolidation, we were able to create enough space for the new equipment. Physical security had not been a concern in the past and the IT department was open to anyone. Prior to installation of the data center equipment, electronic locks were installed on entrances to the IT department. In addition, electronic locks were installed within the IT area for the data center room, the server room and the print room. Physical access was built on a role based model tied to a separation of duties matrix. The CIO is the owner of physical access and defines access rights based on employee job descriptions. The data security officer built the access profiles and assigned access rights accordingly. Proximity badges were selected that includes the employee's photograph, name and department. A reception desk was established at the entrance to the IT department and visitors to the IT department must present themselves at a door with a camera and telephone into the receptionist to be allowed entrance to the area. All visitors are assigned a visitor's badge and are escorted at all times. The IT department went from no physical security to significant security in one step. The physical security rules were put in place nine months prior to going live.

Application and Data Access Security

The data owners for each application are the senior managers of the Bank. They have discretionary control over who can access their respective applications, however, virtually all access rights are granted using a nondiscretionary role based access model. A default access list has been approved for each major job function in the Bank. Only the data owner for a particular application can change the access rights for a given role and they can also make exceptions to access rights based on individual exceptions. All requests must be in writing and signed by the data owner before security changes will be made. Actual granting of the access rights is accomplished by the Data Security Administrator.

Data Center Hardware

New mainframe hardware was selected based on the hardware used by the third party vendor. The new hardware was installed and was operational nine months

prior to the conversion for use during the testing phases. Maintenance contracts were put in place for all hardware and system software.

Power, UPS, Generator and HVAC Requirements

Once all of the hardware requirements had been determined, an un-interruptible power system (UPS) and an external generator were ordered and installed. The UPS and external generator provide emergency power to all computer systems and to the air conditioning equipment for the computer area. The generator automatically starts in the event of loss of commercial utility power and is online within eight seconds. Standards and procedures were written to manage maintenance and testing of the UPS and emergency power system which includes a weekly generator test and a monthly test of the full system where commercial utility power is disconnected.

Incident Reporting

Prior to the move to an in-house system, there was no type of formal incident reporting procedure. An incident reporting system standard was defined and implemented to report, log and resolve all incidents. The Bank defines an incident as any event that disrupts or threatens to disrupt normal operations. Hardware failures and power outages are two examples of an incident. Attempts to break a password or password sharing are two examples of a threatening incident.

Ancillary system software requirements

Once the IBM MVS operating system was chosen, attention was shifted to determining the vendor(s) to use to provide all of the ancillary system software such as security, tape and storage management, backups, reporting and monitoring. Information security was a prime concern and after looking at several security applications, we choose IBM's RACF product. The security officer attended two RACF education classes to prepare for the establishment of the required profiles. The security officer will continue to attend periodic RACF training. Most of the other ancillary software is from Computer Associates.

Installation and Testing the New Operating System

The out-sourced facility used by the Bank used IBM's VSE operating system. Due to the age of VSE and its pending loss of support by IBM it was decided to install the MVS operating system with the new in-house system. We used outside consultants to assist us with setting up the new MVS operating

environment. The new operating system environment was installed and operational seven months prior to the conversion date.

Hiring and Training New Data Center and Development Employees

Hiring of new data center employees started seven months in advance of the conversion date. This included application developers, system programmers and data center operators. It was imperative that operational and development personnel were hired and trained in advance of the conversion.

Testing All Applications

Testing of all applications started as soon as the hardware and operating system were in place seven months prior to the conversion. Thorough testing was necessary due to the change in operating systems and due to the upgraded loan application and the new customer information application. The single biggest change for the applications was creating new job control language (JCL) job streams for each application in the MVS operating system environment.

ATM Network Security and Connectivity

The ATMs on the network are a combination of older binary synchronous based devices and TCP/IP devices. The binary synchronous data is encapsulated on our TCP/IP WAN using Cisco's BSTUN protocol. Some of the ATM's are connected to the network with wireless connectivity using Wired Equivalent Privacy (WEP). We do not consider WEP 802.11 as a secure transmission standard so routers using IPSec are used on both ends of every wireless circuit to ensure confidentiality of all data. In addition, some measure of protection is also provided by using line of sight transmission.

Change Control

Prior to bringing the data center in house, there was no real change control in place for network changes or for changes to the PC server environment. Everyone knew we would need a formal change control process for the data center. When the conversion occurred and change control was implemented for the data center, we also required that all changes to any other production environment such as PC servers, network, and power system would also be required to go through the formal change control process.

A change control standard was added to our Information Security Policy which requires all production related changes to go through the change control process

regardless of what was changing. The formal change control process implemented requires the attendance of the data center manager, the development manager, the network manager, the MIS director (who runs the daily operations), and the CIO. All changes must be documented and signed off by every manager. Involving all managers in the change control process all of the time helps ensure that each manager is aware of changes in other areas and can therefore evaluate if any change in another area could affect their area.

A key component of change control was to add a business continuity check to all production changes. Every change is evaluated to see if it has an effect on the business continuity plan. If so, the required changes to the business continuity plan are identified and a specific person is assigned as being responsible for documenting the required changes to the business continuity plan.

Turnover

Turnover, as defined, by the Bank is a review each morning of the activities of the previous day and night processing. All incidents are logged in an incident reporting system. Senior management of the Information Technology Department attend the morning review where any and all incidents are reviewed. Any incident that requires follow up activity is assigned to someone who is responsible for resolving the specific issues and recording the results in the incident reporting system. Incidents are logged according to the type of pre-defined incidents. The incident log provides a means to research and look for any trends that may develop.

Business Continuity Planning

Prior to moving to an in-house system, there was no formal business continuity plan (BCP) for the IT department. During the planning stages of the conversion plan, a Business Continuity Plan was developed and put in place for every department. A full time position was created and filled for BCP documentation. A BCP committee was formed to create, implement and test the plan. Early in the process, it was stressed to all involved and reflected in the plan that the first and foremost priority of the BCP was the safety of our employees and customers.

The committee is comprised of senior managers and representatives of every department. A business impact assessment was made which included prioritization of business processes, maximum downtime interruption by business process and resource requirements.

A third party vendor was chosen to provide an alternative data center capability for all of the different types of computers used by the Bank. The bank's contract with the vendor provides for a warm site containing all required hardware. The

warm site also includes network connectivity to our state wide network of branches. The plan requires that all systems must be operational within seventy-two hours of a disaster. A successful test of all applications was completed at the alternate data center site three months after the conversion

Mock Conversions

Two mock conversions were conducted prior to the conversion weekend. The purpose of the mock conversion was to test all steps to be executed during the conversion weekend. During the two mock conversions, minor changes were made to the plan.

Contingency Plan

The overall plan included a contingency plan so that if the weekend conversion was not successful, normal operations would still be in effect the following Monday morning. The basis of the contingency plan was that Friday night processing would occur at both the in-house system and the out-sourced system so that either system could be used on Monday morning. Most of the plan detail was in the communications area and involved routing employees and customers to the appropriate system on Monday morning.

Policies, Standards and procedures had to be developed for many of the above listed major areas of the conversion. I spent a considerable amount of time reading the sample policies listed on the SANS website. Some of the SANS sample policies were used as templates and modified to suit the Bank's particular needs. The sample policies used were very beneficial and helped to reduce the time required in writing the policies.

After

The conversion was completed on schedule twelve months after the plan was started. The conversion was very successful. The actual conversion to the in-house system started on a Friday morning without affecting normal operations. The conversion activity lasted through the weekend. Employees from all major departments tested their respective applications on Sunday and verified that their applications were in balance and ready for use. Monday morning the new system was operational without our employees and customers knowing a change to the in-house system had occurred which accomplished our first primary goal of a successful conversion.

Three months after the conversion, the FDIC conducted their first Information Technology examination which was, in effect, an independent evaluation and grading of how well we did in accomplishing our information security

requirements to insure that our Bank was operating in a safe and sound manner in relation to information security. The results of the FDIC Information Technology were positive. The FDIC did not find any major security concerns. All issues found were minor in substance and were resolved in a timely manner.

The positive results of the conversion and the subsequent FDIC Information Technology examination was accomplished by establishing the overall plan and then monitoring it on a daily basis to resolve any issues that would occur.

Six months after the conversion, a full scale disaster recovery test was conducted for the data center with the IBM mainframe and AS400 computers and selected PC based servers at our vendor's facility in another state. Selected users from all departments entered data into their respective systems. A full night's batch was completed and all applications balanced. Full network connectivity was also successfully tested. Several days after the test a final meeting was held to re-cap the disaster recovery test. The items noted were documented and action taken to update the disaster recovery plan. All data used during the test was deleted by formatting all disk drives used during the test. In addition, the vendor is contractually required to ensure all data from testing at their facility is deleted.

The success of the test was attributed to the detailed plan that was developed and refined during the conversion plan. Having a full time person dedicated to disaster recovery documentations was very significant and played a large role in the successful test.

References

1. Schwartau, Winn, What's happened to availability?
   URL: http://www.nwfusion.com/columnists/2003/0106schwartau.html

2. Mitnick, Kevin. The Art of Deception, Indianapolis: Wiley Publishing, Inc., 2002. 259 – 329.

3. Krutz, Ronald; Vines, Russell. The CISSP Prep Guide. New York: Wiley Publishing, Inc., 2001. 10 – 14.

4. King, Christopher; Dalton, Curtis; Osmanoglu, Ertem, Security Architecture:
   Design, Deployment and Operations. Berkeley:Osborne/McGraw-Hill, 2001. 48 – 53.

5. Federal Deposit Insurance Corporation, System Examination Handbook.
   URL: http://www.fdic.gov/regulations/information/information/index.html

6. Federal Financial Institutions Examination Council, Information Technology Examination Handbook.
   URL: http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

7. Federal Deposit Insurance Corporation, Financial Institution Letters
   URL: http://www.fdic.gov/news/news/financial/2003/index.html