Security of Information Systems in Organization: A Bank Model

Peter Okpamen

Ambrose Alli University
Ekpoma-Edo State, Nigeria

Doi:10.5901/mjss.2013.v4n7p101

Abstract

Security of Information Systems concentrates on the collective efforts of all institutions to produce markedly secured Information systems to help deal with the threats or problems of Identity management within and outside the banking institution. Identity Management (IDM)" refers to the analysis of procedures of utilizing technologies, models/methods, standards/mechanisms in order to manage essential information in the institution's network about the identity of all users, and control access to Bank resources. In this project, apart from the design implementation and analysis, emphasis was also placed on the Identity Management(IDM), which guarantees the Identity and Integrity of every registered users in the Network in order to apply appropriate access policy, deliver visibility into Network activity, and secure the local, centralized, distributed, and web/globalizes management of remote devices, while providing Authentication, Authorization, and Accounting functionality across the institution's Network devices. The Security of information systems and the need to have an effective management system in any organization cannot be overemphasized, because any attempt to undermine this laudable objective in any organization could obviously lead to an array of conflicts/crises within the organization. Essentially, this project is focussed on a design of a security requirements, analysis, and policy formulation in organization with a bias in the banking industry. Availability of such model can help management to formulate policy in terms of the security of operations in the system. In particular, the policy spells out the various authentication and authorization actions to be carried out by clients and personnel in the bank. However, there are strings of threats such as identity theft, "phishing mail", false accounts, fraudulent loans, wire fraud, credit card fraud, etc associated to the system. In other to have effective system in place, the system must be such that is capable of detecting these threats before they are carried out.

1. Introduction

This project is focused on a design of Security requirements, analysis, and policy formulation in a Bank. The essence of this design is to enable the Bank to design an appropriate Security Network, which will help guarantee the security of Information Systems in the Bank. In the course of this project, the following were taken into consideration: Assets in the bank, the operations of each staff, customers and non customers in terms of authentication and authorization policy; role allocation policy, and threat policy. The confidentiality policy, as well as the availability of the system was also of paramount importance to the design. We also placed emphasis on the threats facing the security system; such as access by unauthorised persons either by way of identity theft or by obtaining someone else's password, and attempting to alter information that could create serious crisis in the institution; as well as the integrity of the security system. In view of this development, the design was built on the premise that Identity management is a key to the implementation design. Based on this scenario, this paper is adumbrated as follows: Apart from the introduction, Section II contains a brief literature review on the subject matter; Section III contains the Methodology used in this project, and a description of the various assets in the bank: personal details of customers, personal details of staff, non customers, account details, etc. In this section, the operations and roles with respect to the assets were clearly spelt out. Section IV discusses the potential threats to the security system, and the vulnerable spots in the system were identified. Section V contains highlights and discussion on

Authentication of users; while Section VI discusses the Authorization policy of the system. Section VII discusses the issue of confidentiality; section VIII discusses the integrity status of the system; while Section IX discusses the availability of the system; and section X explains the audit procedure of the system. And section XI contains an explanation on how the system detects and reacts to threats; while, Section XII brings the analysis to a close with a concluding remark.

2. Security Systems in Organizational Context

The performance of any security system in any organization depends highly on the level of care put in place during the design. Security of Information Systems has therefore culminated into tough web of technology concepts and standards. And there seems to be no end in sight in terms of standard or consistency, not even a single organization. At the moment the issue appears to be beyond software and system users. The errors are only discovered only after the damage has been done to the system. “The only true security system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards-and even then there are still doubts”-(Gene Spafford 2007 : 291). ISO 27001, an information security management standard and certification program encompasses a set of information security requirements and it helps to reassures customers, employees, and suppliers that information security is of paramount importance for the organization. The organization on its part owes it a point of duty to establish a standard security system to deal with information security threats and issues.

Accordingly, ISO27001 is deeply associated to all classes of organizations, and is generally applied for certification purposes. Once the organization meets the standard of ISO 27001 requirements, the security features is often certified by an external registrar. Broadly speaking, a lot of IT managers do not have the required coherent platform and genuine methodology for achieving enterprise security. A security plan that includes technology, personnel, and policies would be a much better approach to developing an organization security strategy (Hazari, 2005). Essentially, the building of a security model requires a clear understanding of the security functional requirements of the organization, and a standard security policy strategy (FIP Standard, 2004; FIP Standard, 2006; NIS Special publication, 2002; NIS Bulletin, 2003). Accordingly, the literature suggests that different levels were adopted by researchers to examine access control requirements. Foremost in their approach is the threat analysis-based approach; and it has been found to be very essential as studied intensively by researchers (Debar et al., 2006; Thomson and Von Solms, 1998; ; Whitman, 2004). The second approach is the evaluation-criteria based. The emergence of this approach over time gained immense popularity among researchers. And this framework has also been adopted by the US department of defence; as well as the European Union. As a result of this development, it is widely known as the common criteria (ISO/IEC, 20050). Consequently, this school of thought have recommended that this become a basis for every security model. However, to formally evaluate any security system, an evaluation methodology with a set of security requirements is required in order to define the functionality of the security system. Adequate care for the existing technology expertise may well overwhelm an information company, irrespective of position and size. The bottom line therefore should be a regular assessment of risk in order to ensure that the goal of achieving a genuine security system is not a mirage.

3. Methodology

The methodology in this project involves a design of a set of potential security procedures and polices within the Banking environment. Thereafter, the project will discuss the potential threats to its operations and unauthorised access to the customer’s information and electronic funds

3.1 Assets of the bank

In this section, we shall discuss in brief about the assets we have identified within the bank with respect to security issues.

Table 1 Assets: Customer Authentication Table

Customer- ID	Password
C0001	abcdefgh
C0002	Robinson

This table is used to authenticate the customers when they login via the Internet, using the customer ID and its associated password.

Table 2 Assets: Customer Details Table

Customer ID	Name	Address	Telephone	Status	Security Question
C0001	Mr S. Robinson	Epson	123456789	Active	Dog = Feed

This table contains customer details associated with the customer ID. The status field identified above is used to mark the customer's entry and inform the bank as to how to interact with the customer.

Table 3 Assets: Account – Holder Table

Customer ID	Account ID
C0001	A1001
C0001	A0002

This table contains entries for all the actual accounts a customer has with the bank. It maps both customers to accounts and to customer.

Table 4 Assets: Account Authentication Table

Account ID	PIN
A1001	1234

This table is used to authenticate a customer as he/she interacts with a specific account that he/she own, using both the account ID and its associated PIN

Table 5 Assets: Accounts Table

Account ID	Account Type	Date Opened	Balance	Status
A1001	Visa	01/01/06	-200.00	Active
A0002	Loan	01/02/06	-7000.00	Active

This table contains account details associated with the account ID, which then maps a specific customer.

Table 6 Asset: Account Transaction Table

Account- ID	Transaction-ID
A0001	710
A0002	711

The table maps transactions to accounts and accounts to transactions.

Table 7 Assets: Transaction Table

Transaction- ID	Date	Amount	Location	Status
710	25/03/2006	100.00/-	Stratford	Active
712	10/12/2006	500.00/-	Forest Gate	Monitored

This table contains all transactions made with respect to an account within the bank. The Possible states for this field are:

- Active: Normal customer interaction
- Monitored: All interactions with the customer need to be monitored.

Table 8 Assets: Personnel Authenticate Table

Personnel- ID	Password
P00126	James67Robins

The table is used to authenticate a bank employee when they login into the bank computer network, using the personnel ID and its associated password.

Table 9 Asset: Operation Table

Operation ID	Table- Assets	Operation on Assets	Time- Frame
OP0001	Customer Details	Customer	(Mon- Fri= 0900-1700) (Sat = 0900-1230)
OP0002	Personnel Details	Bank HR	(Mon- Fri= 0900-1700)
OP0003	Transaction Details	Bank Admin	(Wed- Fri= 0900-1700)
OP0004	Personnel Authenticate	Bank HR	(Mon- Fri= 0900-1700)
OP0005	Security Log	Bank security	(Mon- Fri= 0900-1700) (Sat = 0900-1230)
OP0006	Accounts	Bank Manager	(Mon- Wed= 0900-1700)

This table is used to define operations on assets

Table 10 Assets: Role Table

Role- ID	Operation- ID
R0001	OP0001

This table is used to define operations on assets to specific roles.

Table 11 Assets: Personnel Table

Personnel ID	Role ID	Name	Address	Telephone	Location	Status	Date
P00126	R0001	Stephen	121 Road	1112221	Waterloo	Active	03/03/2012
P00127	R0002	Ray	121 Road	1112222	Waterloo	Retired	03/03/2012

Table 12 Assets: Security Log Table

Security ID	Time Stamp	Location	Type	ID	Activity
S00150	03/02/2012 at 3:00pm	Stratford	Customer	A10001	Logged in Accounts table
S00151	03/02/2012 at 3:00pm	Waterloo	Account	A10002	Changed password

3.2 Roles

Figure 1: Bank Hierarchy structure

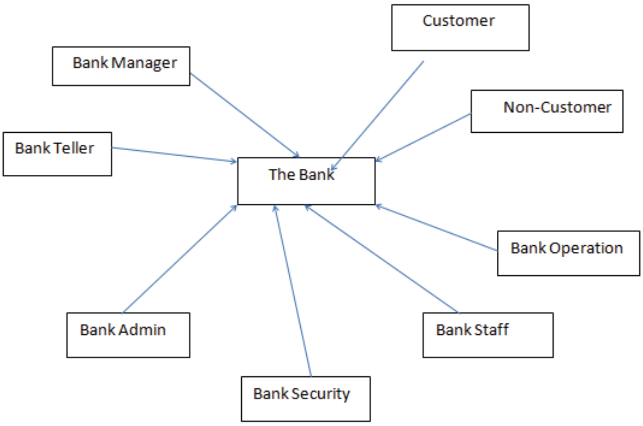

Table 13: Bank Roles

In our analysis of the security issues with respect to the bank model, we have identified a number of key roles which must be taken into account.

Role	Description
Customer	A customer is the one who has an account in the bank and is authorised to view personal details of his own transaction.
Bank Manager	• A bank manager is manager of a branch office of a bank. His/her main responsibilities are: • Implementing the delivery of sales strategies and targets and motivating employees to meet these. • Processing data to produce accurate facts, figures and reports; • Managing and supporting staff and facilitating appropriate continuing

	professional development (CPD)
Bank Teller	• A bank teller is an employee of the bank who deals directly with most customers. His main responsibilities are; • Cashing cheques • Accepting deposits and loan payments • Handling foreign currencies or commercial or business accounts.
Bank Security	• Bank Security is responsible for the IT infrastructure of the bank
Bank Operations	• Bank operations are employees who ensure a smooth activity of work on a daily basis. • They are responsible for the verifications of customer's details.
Bank HR	• Bank Human Resource is responsible for recruiting new employee • Pay roll, appraisal etc.
Bank Admin	• Bank admin is responsible for all the clerical work. • They will create all the accounts for the customers, as well as employee. • The will store essential records of customers in the database. • Mainly responsible for paperwork
Non Customer	A Non customer is one who does not have any rights or privileges to look into anyone's account. He or she does not have an account with the bank and is only allowed to get public information. It may include the procedures to open a bank account, etc.

3.3 Operation on Assets

Table 14: Access Control Matrix

Assets Role	Customer_Authenticate	Customer_Details	Account _Holder
Customer	Authenticate, Change password	View, Update	View
Bank Manager		View, Update, Change Status	View
Bank Teller		View	View
Bank Security	Reset	View, Change Status	View
Bank Operations			
Bank Admin	Create, Reset, Delete	Create, Reset, View, update, Change status, Delete	Delete, Append, View
Bank HR			
Non Customer			

3.4 Operations on Assets for Access Control Matrix (ACM).

Table 15 Asset: Customer Authenticate

Assets Fields	Customer ID = CACID; Password = CAPwd;
Operation Inputs	Customer ID = ID; Password = PWD;
Operation	Authenticate
Description	Authenticate a customer using their customer ID and password
Precondition	None
Event	If (ID = CACID and Pwd = CAPwd) then customer authenticated
Post event	Security->Append(ID)

4. Potential Threats to the System

We have classified the threats as, internal threats and external threats. The internal threats emanates from someone working inside the bank, whereas the external threats emanates from an outside person.

4.1 Internal threats:

False Accounts: The bank authorities might open false accounts in the names of fictitious customers and allow privileges to that account. They may provide such accounts with loans and credits. Later, they might convert this money to personal use.

Fraudulent loans: One way to remove money from the bank is to take out a loan. A fraudulent loan however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; "the burrower" could then declares bankruptcy or vanishes. Eventually the money is gone. The borrower might even be a non-existing entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank.

Wire fraud: Wire transfer networks such as the international SWIFT interbank fund transfer are often targets because if a transfer is made, it is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that the insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

Forged or fraudulent documents: Forged documents are often used to conceal other thefts. Banks tend to count their money meticulously, so every penny must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested, can therefore be valuable to a banker who wishes to conceal the minor detail, and assumed that the money has been stolen and is now gone.

Theft of Identity: Dishonest bank personnel have been known to disclose depositor's personal information for use in theft of identity frauds. The perpetrators then use the information to obtain identity cards and credit cards, using the victim's name and personal information.

Demand Draft Fraud: This fraud is usually done by one or more of the bank's dishonest employees. They remove few demand draft (DD) leaves or DD books from stock and write them like a regular DD. Since they are insiders they know the coding and punching of a demand draft. These Demand Drafts will be issued payable at a distant town/city without debiting an account, and will be cashed at the payable branch. For the paying branch it is just another Demand Draft. This kind of fraud will be discovered only when the head office does the branch- wise reconciliation, which normally takes 6 months. By that time the money is unrecoverable.

External threats: These are the threats from outsiders, and can be done by thefts or hackers. Someone using the internet banking for transactions has to be careful of hackers. The security number and password are vital information for your online transaction. We have listed some of the threats below:

Credit card Fraud: Typically the fraudster uses the credit card of another person to be charged for the purchase. Some of the credit card frauds are stolen card frauds, Account Takeover Fraud, Credit Card Mail Order Fraud, and Skimming.

***Stolen Credit card fraud**:* When a customer losses a card it is possible for the thief to make unauthorised payments on the card until the card is cancelled.

***Account Takeover Fraud**:* Fraudsters call and impersonate actual card holders using their stolen personal information. They have the address and other information of the card holder changed to an address they control. Additional cards and possibly PIN mailers are requested and issued to the new address and used by the fraudsters to make purchases or obtain cash advances.

***Credit Card Mail Order Fraud**:* Using a stolen credit card number, or computer generated number, a thief will order stolen goods.

***Skimming**:* Skimming is the theft of credit card and information by a dishonest employee; it is usually done at bars or restaurants. These people either copy the numbers manually or they use a magnetic stripe reader to get the card security code.

Phishing or fraudulent mail: Phishing is a fraud technique used to make people to give their security numbers and password to fraudsters. The hacker sends a fraudulent mail which is specifically designed to reveal the security details to the intended person. This mail is designed in such a way that it looks like it has come from a responsible source e.g; your bank. This mail might also provide you with a hyperlink with your bank home address URL which is again a fraud site. You might find this fake site exactly same as the original one where you can easily end up giving your security details to the hacker or fraudster. How phishing could be avoided is listed below:

First of all, no bank will ever send a mail asking about your security number and password. If you do receive a mail from your bank, no matter how urgent it is never ever put security information on it. Always call the bank phone number to verify whether they want this information. Secondly, if you suspect that it is a fraud mail forward it to the bank reporting about this fraud.

Check the security Bank sites: You should never click on a hyperlink or follow a link to go to your bank home address on internet. Always type the whole address of your bank URL in the browser. Check whether the bank site starts with 'https' and whether there is a padlock icon at the bottom section of your browser. When you double click on the padlock icon it brings the information about the lock which will help you confirm whether this site is genuine. If the lock is not valid or has been issued to a website that you do not recognise, do not enter your security information.

Login and Logout: Do not provide your security ID and password to anyone to avoid scams. Do not leave your computer or laptop unattended while you are still logged into your internet banking. Always logout when the session is over. Avoid saving the security ID and password on your computer and always keep it in a safe place. Also, do not change your security details when you are using a computer in a public place.

5. Authentication

5.1 Security policies

A Security policy is a high level definition of a specific or set of behaviours, defining what is and what is not permitted with respect to the policy. It will correspond to a specific purpose within the bank's security model. From detailed study of our model, we have identified a number of specific security policies, which describe and relate to activities. They include:

5.2 Authentication Policies

Authentication is the process that is used to establish and confirm the identification of a valid entry. This identification allows for this entity to provide such information that their identity is no longer in doubt, allowing them to perform some authorised function or action. With the above statement in mind, in this section, we will discuss the different authentication tables we have identified above for our model, specifically in the asset section and the operations on the assets identified in the Access Control Matrix, specifying their purpose, their inter-action and procedure.

5.3 'Customer_Authentication' Table

This table is used to authenticate a customer who wants to access and manage his/her personal information and overall account information over the internet. In order to do this, using a secure communication link, he/she will be asked to enter both his/her customer ID and password as proof of identity. This information is then compared using the 'Authentication' operation table; with the customer entered password encoded using that defined in the 'password Security' policy. The customer is allowed three failed attempts at the authentication process, before the 'Failed Login Attempt' policy is enforced and his/her 'Customer Details' table entry marked as 'Blocked' and recorded in the 'Security Log' table. The bank will then contact the specific customer to inform him of this incident and investigate i.e., to find out if the customer forgot his/her password, or someone trying to impersonate him/her or an opportune hacker.

In conclusion of this specific event, whether or not the bank security become involved due to a security violation, Bank admin gets the customer to activate it again so that he/she can manage the account again. In order to do this, the bank admin will perform the 'Re-Authentication' policy to authenticate the customer again, which on successful resolution of this issue, the customer will be able to login again and manage his/her account.

5.4 'Account_Authentication' Table

This is the table to authenticate a customer attempting to manage a specific bank account held within the bank using an account card encoded with the account's details. This access is usually in one of two ways; using an Automated Teller Machine (ATM) or from the front desk with a human tiller; both uses the 'Authentication' operation policy. The use of the ATM requires the customer to go through an extra level of authentication, a personal identification number (PIN). This is the number originally assigned to the customer by the bank admin, and must be entered along with the account card. It is this information that is used by the 'Authentication' operation table.

The customer is allowed three failed attempts at the authentication process at the ATM, before the 'Failed Login Attempt' policy is enforced and the relevant account in the 'Account' table entry is marked 'Blocked' and recorded in the 'Security Log' table. The bank admin will then contact the specific customer to inform him/her of this incident and thereafter investigate to see if there was any security implications i.e; was it the customer that forgot his/her PIN or someone trying to impersonate them.

At the end of the investigation, Bank security may or not be involved depending on the outcome, the bank admin will perform the 'Re-Authentication' policy in order to authenticate the customer, and subsequently make the account 'Active' again. The use of the front desk within the bank with the Tiller: the customer here does not have his/her PIN to gain access to the account. Here, the only authentication is that the customer has the account card and seeks for reasonable transactions on the account. Apart from scrutiny to identify any unusual behaviour in the customer, there may be further identification from the customer by the Tiller, as well as the fact that the entire incident will be recorded on CCTV for potential analysis if something wrong is later identified. If the Tiller is unhappy or believes something is wrong, he is able to mark that account as 'Blocked' and the incident recorded in the 'security Log' table. Bank admin will then request the customer to come into the bank for further talks, where the customer may have to go through the 'Re-Authentication' policy

5.5 'Personnel_Authentication' Table

This is the table used to authenticate bank employees so that they can carry out their employment objectives and interact with the equipment within the bank's network. Here employees will have to prove their identity in two different ways. The first request is to ask them to enter their personnel ID and password as proof of identity, and is eventually compared with information in the 'Authentication' operation table, using the entered password encoded in the 'Password security Policy'. The employee is allowed three attempts in one day during the authentication process, before the 'Failed login Attempt' policy is enforced and his/her 'personnel' table entry is marked as 'Blocked'. It is then up to the employee to contact the bank security and request for a reset of his/her password, while the 'Personnel' table entry is made 'Active' again. Bank Security will undertake the 'Re –Authentication' policy with the employee, and if successful it re-enables that employee's login. The second authentication way is more of a visual approach, in that the employee must display his/her personnel ID card. This will enable other members of the bank to have some idea with respect to internal bank information.

6. Authorization

Authorisation will always follow after successful authentication. Authorisation is the process of allowing an authenticated person, to access a function or action that is allowed to do. It is the access control, the guardian, who performs this function. In the bank model, I have identified a number of specific roles which have specific functions or operations associated with them. These roles have been defined in the 'Roles' table, each being made up of a number of operations which have been defined in the 'operations' table in order to achieve the role's functionality. These roles cover both the employees of the bank and its customers. It is a declaration of the activities both can perform on bank assets. The main difference between employees and customer's roles is that all customers have the same default role of a 'Customer' and its associated operations. Whilst employees cannot be pigeon holed into a single role, they can be spread over many roles, each with a number of common and unique operations associated to him/her. Note that in the design of our authorisation process, we have added a dynamic capability to its planning and operation. This means if an operation is changed or if a role requires a new operation, this can be implemented very easily with immediate effect. This entire process of authorisation can be seen quite clearly in the 'Access Control Matrix, where operations on assets can be clearly identified to specific roles. One additional important facility associated with this authorisation process, is the ability for each operation to have a 'Time-Frame' component associated with it. This means that even though an operation can be carried out by a specific role, it must also meet the criteria of the timing element. It adds a little more control over when an operation can be started.

7. Confidentiality

In this section, we will argue about the generic principle of data protection procedure and its importance in connection with the bank model we have designed. Confidentiality is about ensuring that information is accessible only to those authorised to have access. Confidentiality is one of the keystones of "data protection or information security". Confidentiality is one of the design goals for many Cryptosystems made possible in practice by the techniques of modern cryptography.

7.1 Types of Confidentiality

Client Confidentiality: In relation to the bank Model we have designed, client confidentiality is the principle that have been implemented and suggest that the bank (as an institution or employees), should not reveal information about their clients both at individual level or otherwise, to a third party without the consent of the client or a clear legal reason.

Bank secrecy or Bank Privacy: With regard to the Bank Model developed above, we have introduced Bank privacy, which implies legal principle under which banks are allowed to protect personal information about their customers.

Introducing Access Control Matrix for data protection: Access Control Matrix is an abstract, formal security model introduced in the bank model that characterises the right of each subject with respect to every object in the system. It is a scheme through which we have specified and enforced security policies (what is to be secured for a system of the Bank and its' entity). It also addresses the constraints on behaviour of its members and constraints imposed on adversaries by the help of mechanism developed in the bank model, which means the system controls on functions and flows amongst them, including external system and adversaries, and access to customer data by internal people. Therefore, we have designed the authorisation as been granted on the basis of role hierarchy, which defines the degree of access to any objects.

8. Integrity

In this section of the bank model, we will discuss about data (Bank Assets/Services) and information being provided against any data for the purpose of getting access. The degree of accuracy on information provided against the data will be the source to create authentic data integrity. Integrity is an assurance of data non-alteration. Data integrity is having assurance that the information has not been altered in transmission from origin to reception.

8.1 Data Integrity assurance in Bank Model

An application or mechanism was introduced into the security systems to ensure that there is data integrity in the bank model. This section concerns about cryptographic signature, which includes digital signature or digital signature scheme.

Table 16: Table of Implementation procedure of mechanism

1. Mechanism type	• Asymmetric cryptography
2. Property of mechanism	• Signature in digital rather than in written form
3. Digital signature scheme gives two algorithms	• One for signing user's secrets or Private Key • One for verifying Public signature
4. Purpose of mechanism	• Authentication (verification of user's identity)
5. Process of authentication	• Through electronic mail to contact (sending, storing and receiving message over electronic communication system).
6. Contents of electronic mail	• Customer – ID • Customer – Password • Pin No. • Personal –ID (when login – out) • Pre-arranged questions etc.
7. Use of digital signature	• To create public key infrastructures
8. How does PKI work?	• It works with the help of public key encryption (a message encrypted onto a user's public key cannot be decrypted by another one, except the user possessing corresponding private key).
9. How a user is joined with PKI system	• By digital identifying certificate issued by certificate authority.

9. Availability

In this section of the bank model, we will discuss how to obtain availability and accessibility of information or resources. This section also contains a discussion on some factors that causes resources to become less available than required or not available at all. Availability is assurance to timely and reliable access to data services for authorized users. It ensures that the information or resources are available when required. It implies that the resources are available at a rate, which is fast enough for the wider system to perform its task as intended by the bank customer's satisfaction. But there are still some constraints we considered in the bank model which can cause delay and unavailability of resources or services. Factors that we have outlined in the bank model which could lead to unavailability of resources are as follow:

In relation to the bank model developed above, confidentiality and integrity were built-in to protect the system. However, a third party e.g. an attacker or a hacker can make the bank resources and services least and sometime unavailable

Table 17: Polices introduced in the Bank Model

1. Identification and awareness of computer crime in relation to individual and secrete data	• E.g. Illegal access: [unauthorised access]. • Illegal interception: [by means of non-public transmission of computer data to, from or within the computer system]. • Data interface: [unauthorised damaging, deletion, deterioration and altering or suppressing computer data]. • Misuses of devices: [forgery, ID-theft]. • Electronic fraud
2. Identification of access factor	• Customer –ID. • Account – ID • Account –PIN • Customer Password. • Prearranged Questions for security check etc.
3. Use of the identification factors	• Access will be granted upon if insertion of PIN or Password was done within standard time frame and procedure. Else • If until third time pin number or password use is not correct then the access factor and account will be locked for security check
4. Eventually, assuming that it could be due to computer security reason caused by the hacker	• DOS attack [Denial of service] will take place to make sure resources are unavailable for intended users.

10. Auditing

In this section of the bank model, we will discuss about identifying the who, where and when, with respect to information access carried out, which as a record remains recorded in a chronological order in the security Log system of the bank. In addition, we will also discuss about the computer – generated records and the process of creating such record called data logging. Auditing in relation to the bank model (data, access, communication, transaction etc.) is a chronological sequence of audits records, each of which contains evidence directly linked to, and resulting from the execution of business process or system function into the security log system of the bank. In order words, an audit records from activities such as transactions, communication by individual, people, systems, accounts or entities.

Table 18: Function of auditing in relation to the bank

By whom	Activities	Result
Bank Manager	- View Customer details - Update, Change Status	- All the activities carried out will be recorded in the bank security log with time in and out in chronological order
Customer	- Change of password. - Viewing balance and carrying out Dr Transaction.	- All the activities carried out by the manager will be recorded in the bank security log with time in and out in chronological order.
Third Party [Hacker]	- Impersonate the details of customer	- The activity will be recorded and log system will not authenticate in the absence of accurate identification.

Any individual bank employee or customer carrying out any activity relating to authorization, authentication for any purpose will be automatically recorded in the security log system. The data recorded in the security log can be found in chronological order, which enable us to find out when a particular activity was carried out. It can be enabled to reconstruct and examine the starter/end of data, and can also reconstruct the intermediate states the data went through before the final state was established

11. Detection and Reaction

Detection is the ability to identify some trends, patterns or activities hidden or excluded within the normal operating flow of the system, which should not be there. The goal is to do this as close to real-time as possible, and to limit damage and exposure. Reaction is the activity that will follow the detection of an abnormal event and there is a procedure in place to deal with such occurrences. Most detection would probably come from customer noticing abnormal activities on his/her account, usually via transactions made on them. At this point the bank will carry out investigation, if not 'Blocking' but certainly 'Monitoring' the account and subsequent transactions for clues or trial in order to trace the culprit(s).Usually, the bank does have a wide range of tools it can use to help in its detection process, which includes:

Intruder Detection System: *Software which monitors network traffic for patterns and certain types of behaviour.

Trend analysis and Data Mining: Constantly analysing customers' activities, identifying their habits and forming a classification of their type; watching for when this classification drastically alters, and then investigating the change to see if any action is required.

False application: New applications from customers are investigated to see if their details are correct (address is registered with council, name is registered to address, etc) and that they exist and have a credit value.

11.1 Detection and Reaction by the system

The sort of 'Detection and Reaction' events we could foresee in our model's assets are as follow:

11.1.1 'Customer_Authentication' / 'Account-Authentication' Table

Detection: Repeated attempts to login and failure to a customer account. Perhaps an attempt to permanently block a customer's account, a form of Denial of Service (DOS)

Reaction: 'Monitor' account, if not blocked; Detailed investigation of events.

11.1.2 'Customer_Authentication' / 'Account-Authentication' Table

Detection: Account logged in twice at the same time at different IP addresses
Reaction: 'Block' account; detailed investigation of events; and inform the customer.

11.1.3 'Customer_Authentication' / 'Account-Authentication' Table

Detection: An attempt using IP address from a foreign site to login to as a customer's account.
Reaction: 'Monitor' account; investigate IP; and inform the customer.

11.1.4 'Customer_Authentication' / 'Account-Authentication' Table

Detection: Unusual hours of accessing account from the norm
Reaction: 'Monitor' account; investigate IP; and inform the customer.

11.1.5 'Account, / 'Transaction' Table

Detection: Unusual account activities from the norm, lots of debits, high values
Reaction: 'Monitor' account, possibly 'Blocking' if high values are recorded, investigate IP; and inform the customer.

11.1.6 'Personnel_Auhentication; Table

Detection: Account logged in twice at the same time at a difference IP address
Reaction: 'Block' account; detailed information/investigation of events follows.

11.1.7 'Operation' Table

Detection: An employee attempting to run an outside operation beyond its 'Time-Frame'
Reaction: 'Monitor account; disallow operation; investigate event.

12. Concluding Remark

By and large, the need for effective and efficient security system in the banking industry cannot be overemphasised, in order to guarantee confidence amongst clients and other users. Although, the desire to protect security systems is increasingly difficult because of the fact that hackers are becoming more skilful due to sophisticated attack technologies available. Therefore, eliminating all kinds of threats to the security systems is one of the bank's foremost challenges. Apart from being a moral imperative, it is also an essential step in reducing crisis in the banking industry. As long as large numbers of users are faced with frequent threats occasioned from instability of the present security system, the response to opportunities for the bank to create confidence amongst clients/users is bound to be muted, and little progress would be made in the fight against threats to security systems. But reducing potential threats to security systems is not an exorbitant endeavour as it is achievable to a large extent through this bank model designed above, which combine measures for dealing with Information security problems, coupled with investments in security systems.

The lesson to be learnt is that challenges to security systems cannot be eliminated without first ensuring that the security systems in the banks are markedly secure. This can be achieved through the reversal of the declining trend in investments in security systems. Only with dynamic security system would there be any hope of dealing with the problems associated to the system.

Common sense is always the voice of reason and in the Bank's case, the deadlock over frequent or failure in security systems need to be broken for the users in the society to enjoy the benefits of doing business with the banking industry.

References

Debar, et al; (2006) Using contextual security policies for threat response, Lecture notes in computer science, 109-128.

Hazari, S (2005) Perceptions of end-users on the requirements in personal firewall software: an exploratory study, Journal of organizational and end user computing, July-September.

International Organization for Standardization {ISO/IEC} (2005 ;) Information technology-Security techniques-Information Security Management Systems Requirements. Geneva: ISA.

Whitman, M.E (2004) In defence of the realm: Understanding the threat to Information Security. International Journal of Information Management, 24: 43-57.

Internet Reference

(Webopedia, 2007) retrieved from http://www/webopedia.com/TERM/A/authentication.html
(Webopedia, 2007) retrieved from http://www.webopedia.com/TERM/A/authorization.html
Online banking safety retrieved on March 3rd, 2013 from http://www.rbs.co.uk/security/online_banking _safety.htm
Phishing mails retrieved on March 6, 2013 from http://www.antespam.co.uk/bank
Bank frauds retrieved on the March 6, 2013 from http://en.wikipedia.org/wiki/Bank_fraud
Credit card fraud retrieve on March 6, 2007 http://en.wikipedia.org/wiki/credit_card
Fraud$Credit_Card crime profits.2 C_Loses-26_punishment