A Study on Risk Management Strategies in Electronic Banking Services

Zhang Y.W.
Department of Clinical Dermatology, Guangzhou Medical Academy, Guangzhou, China

Abstract– In this research one of the most affective factors on e-banking will be discussed, by accepting the use of information technology for the execution of the Traditional e-banking, As we know that e-banking is done online and the customers are considered the active element and the other party in e-banking operations. So in this paper we are analyzing the risk level of e-banking system, then highlight this points that professional in the execution of the traditional e-banking using IT , furthermore this create flaws in the security of e-banking by facilitating the sneaking into the personal information and distrust in customer confidence of the e-banking security.

I. INTRODUCTION

A Risk management is an important tool for Information Technology (IT) to use in evaluating the security of the IT systems, and in determining the potential for loss or harm to bank operations, mission, and stakeholders. The risk assessment provides management with the capability to:

- Provide an adequate level of security protection for e-banking systems.
- Meet Federal requirements for information and system security.
- Satisfy oversight e-banking.
- Establish an acceptable level of risk for e-banking.

Risk can never be totally eliminated, but can be minimized by the application of IT security controls. The decision as to what level risk will be accepted will be based on management review of the identified e-banking security controls needed to mitigate risk versus the potential impact of implementing those controls on available resources and system operations. The e-banking risk management identifies the current level of risk for the application and provides risk mitigation recommendations for management review.

The e-banking risk management serves as the primary access control function for numerous online banking applications and the loss of system availability and/or integrity that could have a debilitating impact on the organization's mission. The sensitivity level of the online banking and of the information stored within, processed by, or transmitted by the system reflects the value of the system to the bank. The sensitivity level has been used as the basis for implementing the necessary IT security controls for the system.

This risk management describes e-banking vulnerabilities and associated threats based on three major factors which are confidentiality, integrity and availability of the system.

I. Purpose

The purpose of this report is to provide the main e-banking system risk, threats, and analysis with an assessment of the adequacy of the management, operational and technical security controls that are currently in place to secure e-banking system. This risk assessment report identifies threats and vulnerabilities applicable to e-banking system. It also evaluates the likelihood that vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identifies the overall risk level.

II. Scope

The scope of this e-banking risk management report is to evaluate risks to online banking system in the areas of most recently threats and analyzing this threats and vulnerability.

III. Document Structure

This document is organized into five sections:

- Section 1.0 provides the introduction, purpose, and scope of this risk assessment.
- Section 2.0 provides an overview of the E-banking definition, risk, rules, mechanism and methodology.
- Section 3.0 provides a analyzing of system threats and vulnerabilities.
- Section 4.0 provides the risk calculate, which includes identifying threats, likelihood, impact, risk level and risk assessment results.
- Section 5.0 provides the cost benefits analysis, which includes SLE, ALE, ACS and NRRB.
- Section 6.0 provides the summary and conclusion.

II. ELECTRONIC BANKING DEFINITION

The term “Electronic Banking” or “e-banking” is defined as remote banking services provided by authorized banks, or their representatives through devices operated either under the bank's direct control and management or under the outsourcing agreement. In other words, e-banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a branch and includes the systems that enable customers of banks, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet.

A “remote banking service” is defined as a:

- Dedicated banking service for which the Customer has explicitly registered and authorized.
- Service supplied using devices that are not under the control of the Provider;
- Service which demands the authentication of the Customer.
-

Online Banking Risks Definition

The business risk is the risk of not being able to achieve the business targets due to inappropriate strategies, inadequate resources or changes in the economic or competitive environment. The big changes on the banking sector and the adoption of fast paced evolving technology also change the traditional strategic risks. A bank that will rush into the adoption of new technologies so that it is rendered pioneer is risking losing its investment as information systems lose their value in very short time interval. Moreover, there is the risk of extensive investment in particular products or services, which will not become acceptable by the end users. Internet banking may soon convert from a complementary to the main provider of financial services and products. Consequently, a possible failure of a bank entering this sector, can have various consequences on its future position in the market.

I- E-Banking system mechanism

Online banking is a series of processes that the client logs into the bank’s website through the web-browser installed on the PC or smart phones and carries out various online transactions by using a private username and password. Online banking is carried out in four main phases:

1. The computer’s user runs on the installed operating system.
2. After the web-browser opened, users can access the bank’s website and then enters the personal identifying number (PIN) and the password by using the keyboard.
3. The data input is encrypted by SSL (secure socket layer) and transmitted to the bank’s server.
4. The bank’s server decrypts the transmitted information and processes of the user’s authentication.

II- Risk Assessment Methodology

Risk analysis methodology is structured as four distinct phases:

- Risk analysis of resources, controls, threats, and vulnerabilities.
- Management decisions to implement security countermeasures and to accept residual risk.
- Implementation of countermeasures.
- Periodic review of the risk management program.

This document addresses the first phase, which provides the foundation for the remaining three phases. The detailed analysis of threat, vulnerabilities, and risks includes:

- Asset Identification: e-banking resources within the system boundary that require protection.
- Threat Sources and Vulnerability Identification: Weaknesses in the e-banking system design, system security procedures, implementation, and internal controls that could be exploited by authorized operators or intruders.
- Threat Identification: Known and projected threats that are applicable to the e-banking system under review.

III- Identifying System Assets

Identification of e-banking system assets is necessary for determining system threats, vulnerabilities, and risks, and the appropriate level of security to apply to the system and related system components. System asset identification includes the following:

- Identifying and documenting the system architecture.
- Identifying system and subsystem assets, including all hardware, software, and ancillary equipment.
- Identifying system interfaces (external and internal).
- Identifying system boundaries.

Based on identification of the system assets, a system description is developed and documented in the Security Plan or Technical Architecture Document for complex systems. Once assets have been determined, system security needs are identified by first determining system sensitivity requirements and severity (impact of system loss) related to system information confidentiality, integrity, and availability. Federal IT security standards define the following three basic protection requirements in order to determine the information sensitivity:

1. Confidentiality: Protection from unauthorized disclosure.
2. Integrity: Protection from unauthorized, unanticipated, or unintentional modification. Also includes:
    a. Non-repudiation: Verification of the origin or receipt of a message.
    b. Authenticity: Verification that the content of a message has not changed in transit.

3. Availability: Available on a timely basis to meet mission requirements or to avoid substantial losses.

IV- Analyzing System Threats

Threat sources are any event, process, activity, or action with the potential to cause harm to a system or that exploits a vulnerability to attack an asset. It is any force or phenomenon that could degrade the confidentiality, integrity, or availability of an asset. The capabilities, intentions, and attack methods of hostile entities that have a potential to cause harm to the e-banking system must be identified and evaluated. A threat source is normally known, includes physical, natural, environmental, and human sources, and normally impacts most networks and computer systems when adequate safeguards have not been implemented. A threat source is defined as any circumstance or event with the potential to cause harm to an IT system or that exploits a vulnerability to attack an asset. It is any force or phenomenon that could degrade the confidentiality, integrity, or availability of an asset. The common threat-sources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment.

V- System Threats

Electronic banking creates new risk management challenges for Banks. Typically, all risks associated with traditional banking and products may be impacted with the introduction of e-banking services. However, there are seven major categories of risk specifically associated with e-banking. The associated risks are strategic, operational/transaction, technology, business, online fraud, reputation and legal.

- Strategic Risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. Ideally, an e-banking service should be consistent with the bank's overall financial strategy. The planning and decision making process should focus on how specific business needs are met or enhanced by e-banking, rather than focusing on the product as an independent business objective. Strategic vision should determine how e-banking is designed, implemented, and monitored.
- Operational/Transaction Risk arises from fraud, processing errors, system disruptions, and the inability to deliver products or services, maintain a competitive position, and manage information. In the provision of e-banking services, banks may rely on outsourced software companies. They require the proper management of information systems and the right capacity to service their customers. Contingency and business resumption planning is necessary for Banks to ensure that they can deliver products and services in the event of adverse circumstances.
- Technology Risks are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks, and telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities. Banks have to control every single component and process related of their e-banking systems. Each component represents a control point to consider. This is also valid for potential components; they have to be assessed in appropriate ways before being implemented in the e-banking environment. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.
- Business Risk: In some circumstances, due to the more savvy nature of the e-banking consumer who is more focused on costs and rates, traditional banking risks, such as credit risks, interest rate risk, liquidity risk, and foreign exchange risk are elevated.
- Online Fraud Risk: With online trade, it is essential to take online fraud risks into consideration. Scams such as Phishing and Harming attacks, Identity theft and faulty corporate representation pose a serious risk to the bank itself and to the banks customers. The bank must take the appropriate measures to prevent the occurrence of losses due to online fraud and take the appropriate action to protect the bank's clients globally once an incident occurs.
- Reputation Risk arises from negative public opinion. A bank's reputation can be damaged by e-banking services that are poorly executed or otherwise alienate customers and the public. It is important that customers understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using them. Customer education along with formal incident response and management procedures can help lessen a bank's reputational risk. Banks are required to communicate in a transparent and clear way and to meet their obligations in this regard. The Board of Directors or the management has to agree on the communication strategy and content.

-
- Legal Risk is the risk to earnings or capital arising from violations of, or non- conformance with, laws, rules, regulations, or ethic standards. The need to ensure consistency between paper and electronic advertisements, disclosures, and notices increases the potential for legal violations. Regular monitoring of the bank's websites will help ensure compliance with applicable laws, rules, and regulations.

The Board of Directors and senior management are responsible for managing the above risks and must ensure that the risk management of e-banking is an integral part of the bank's overall risk management. As a result, the applicable risk management policies and processes, and the relevant internal controls and audits as required in the institution's risk management system should be enforced and carried out as appropriate for the e-banking services.
In addition, the Board or its designated committee should ensure that the bank's risk management controls and systems are modified and enhanced as necessary to cope with the risk management issues associated with e-banking.

III. ANALYZING E-BANKING SYSTEM VULNERABILITIES

Vulnerabilities are weaknesses in the environment, system architecture, design, or implementation; the organizational policies, procedures, or practices; and the management or administration of hardware, software, data, facility, or personnel resources. Vulnerabilities that are exploited may cause harm to the system or information processed, transported, or stored by the system. The vulnerability analysis encompasses the following three security control areas:

- Management Controls are safeguards related to the management of security of the system and management of the risk for a system. Examples of management vulnerabilities include lack of risk management, life cycle activities, system security plans, certification and accreditation activities, and security control reviews.

- Operational Controls comprise the operational procedures that are performed with respect to an information system. More often than not, these vulnerabilities stem from the lack of (or an insufficiency in) the various practices and procedures that are critical to the secure operation of a system. Examples of operational vulnerabilities include the lack of (adequate) security awareness and training, security monitoring and detection provisions, personnel and physical security controls and security auditing, and the absence of some or all of the procedural documentation critical to an effectively applied and managed security program.

- Technical Controls are countermeasures related to the protection of hardware, software, system architecture, and modes of communication. Examples of technical vulnerabilities include insufficient security software controls and mechanisms, faulty operating system code, lack of virus controls and procedures, and lack of authentication and access controls. Normally, vulnerabilities are identified during the risk assessment or during security testing and evaluation.

After analyzing online banking system management, operational and technical security controls for the system in its fielded environment, system vulnerabilities are then identified as below:
Confidentiality: In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes". Confidentiality ensures that only authorized parties can view information.

- It is the protection of the transmitted data from passive attacks.
- The other aspect of confidentiality is the protection of traffic flow from any analysis.
- This required that an attacker not be able to observe the:
    - Source
    - Destination
    - Frequency
    - Length
    - And the other characteristics of the traffic on a communications facility.

Integrity: (remains identical to its state) : Integrity ensures that the information is correct and that no unauthorized person or malicious software program can or has altered that data . As with confidentiality, integrity can apply to a stream of messages to protect it. A Connection-oriented Integrity Service assures that messages are received as sent with:

- No duplication
- No insertion
- No modification
- No reordering
- No replay

The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both:

- Message stream modification
- Daniel of Service

3- The Connectionless Integrity Service, provides protection against message modification only.
4- The integrity services relates to active attacks, so we are concerned with their detection instead of prevention.
5- When a violation of integrity is detected, then the service may report this violation.
6- Some other portion of software or human intervention is required to recover from the violation.

Availability: For e-banking system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Availability (Always available) Although a secure computer must restrict access attempts by unauthorized users, it must still make the data available to allow authorized users immediate access.A variety of attacks can result in the loss of or reduction in availability. – Some of these attacks are menable to automated countermeasures such as:

- Authentication
- Encryption

Whereas others require some sort of physical action to prevent or recover from the loss of availability of elements of a distributed system.

Access Control – It is the ability to limit and control the access to host systems and applications via communication links. To achieve this control, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Non-repudiation – It prevents either sender or receiver from denying a transmitted message.

When a message is sent, the receiver can prove that the message was in fact send by the alleged sender. When a message is received, the sender can prove that the message was in fact received by the alleged receiver.

Access Control and Non-repudiation it will be part of the integrity.

ANALYSIS OF THE RISK LEVEL FACTORS

The analysis of the e-banking vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation resulted in a risk rating for each missing or partially implemented control. The risk level was determined on the following two factors:

Below make it as table and then insert it as picture NO plagiarism

- Likelihood of Occurrence - The likelihood to which the threat can exploit a vulnerability given the system environment and other mitigating controls that are in place.
- Impact – The impact of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation or interest.

To determine overall risk levels, we look at how important the availability, integrity, and confidentiality of the e-banking system is in relation to it being able to perform its function, and the types of damage that could be caused by the exercise of each threat-vulnerability pair. Exploitation of vulnerability may result in one or more of the following types of damage to a system or its data:

- Loss of Availability/Denial of Service – Access to the system, specific system functionality or data is not available (Asset is not destroyed).
- Loss of Integrity/Destruction and/or Modification – Total loss of the asset either by complete destruction of the asset or irreparable damage, or unauthorized change, repairable damage to the asset, or change to asset functionality.
- Loss of Confidentiality/Disclosure – Release of sensitive data to individuals or to the public who do not have a "need to know."

The analysis of the e-banking systems vulnerabilities and risk determination will be further discussed in Section Risk Calculation.

Each protection requirement is rated on a scale of High, Moderate, or Low, using the guidance from NIST Guide for Developing Security Plans for Information Technology Systems, SP 800-18, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

The information sensitivity for Online Banking is as follows:

- High: The consequences of unauthorized disclosure or compromise of data or information in the system are unacceptable. Loss of confidentiality could be expected to cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- Moderate: The consequences of unauthorized disclosure or compromise of data or information in the system are only marginally acceptable. Loss of confidentiality could be expected to cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of

the functions is significantly reduced; result in significant damage to organizational assets; result in significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

- Low: The consequences of unauthorized disclosure or compromise of data or information in the system are generally acceptable. Loss of confidentiality could be expected to cause degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; result in minor financial loss; or result in minor harm to individuals.

IV. RISK CALCULATION

This section discusses vulnerabilities, the threats that can exploit those vulnerabilities, and the probable impact of that vulnerability exploited. System vulnerabilities are identified as required security controls that are not fully implemented. These are classified as vulnerabilities because the lack of required controls result in vulnerability that a threat can be exploited successfully.

The analysis of system vulnerabilities, the threats that can exploit those vulnerabilities, and the probable impact of that vulnerability exploitation resulted in a risk rating for each missing or partially implemented control. The risk level was determined based on the following two factors1:

- Impact of the threat exploiting the vulnerability in terms of loss of tangible assets or resources and impact on the organization's mission, reputation, or interest.
- Likelihood to which the threat can exploit a vulnerability given the system environment, threat frequencies, and other mitigating controls in place.

The following sections discuss the areas of potential impact and how the values for the above two factors, magnitude of impact and likelihood of occurrence, and the level of risk were determined. The factors used in these sections are derived from NIST Risk Management Guide for Information Technology Systems, SP 800-30.

Impact

An impact analysis prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. The system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. To determine overall risk levels, the analysis first looked at how important the availability, integrity, and confidentiality of the system and/or its data are to the ability of the system to perform its function and the types of damage that could be caused by the exercise of each threat-vulnerability pair. Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any of the three security goals: integrity, availability, and confidentiality.

To determine overall risk levels, the analysis first looked at how important the security goals (availability, integrity, and confidentiality) of the system and/or its data are to the mission's ability to function as intended. The system sensitivity values of this report were mapped to the magnitude of impact qualitative values of high (100), moderate (50), and low (10) as defined in the NIST guidelines.

Exploitation of vulnerability by any of threats defined in section 2.2 may result in one or more of the following types of damage/impact to a system or its data as documented in Table 2.1 (Threats and Potential Damage):

- Loss of Availability/Denial of Service: Access to the system, specific system functionality, or data is not available (asset is not destroyed).
- Loss of Integrity/Destruction and/or Modification: Total loss of the asset either by complete destruction of the asset or irreparable damage, and/or unauthorized change, repairable damage to the asset, or change to asset functionality.
- Loss of Confidentiality/Disclosure: Release of sensitive data to individuals or to the public who do not have a "need to know."

The impact of a specific threat exploiting vulnerability is determined by adding all applicable impact values for the given threat. The formula for Threat Impact is as follows:

Impact = A + I + C

Given the security sensitivity values for the environment, the total possible Impact value for the environment is 300.

Likelihood of Occurrence

The likelihood that a threat will exploit a vulnerability and cause damage for each of the four areas listed above was determined based on the following factors: the frequency of the threat and the existence of mitigating controls. Likelihood of occurrence was determined qualitatively to be high, moderate, or low using the following Table:

Table 4.1. Likelihood of Occurrence Values Criteria

Value	Risk	Likelihood of Occurrence Description
Moderate (50)	Strategic Risk	The threat-source is motivated and capable, but controls are in place that may impede successful exploitation of the vulnerability.
High (100)	Operational/ Transaction Risk	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.

High (100)	Technology Risks	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
Moderate (50)	Business Risk	The threat-source is motivated and capable, but controls are in place that may impede successful exploitation of the vulnerability.
High (100)	Online Fraud Risk:	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
Low (10)	Reputation Risk	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.
Low (10)	Legal Risk	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited.

In accordance with NIST guidelines, a numerical value was assigned for likelihood of occurrence as High = 1, Moderate = 0.5 and Low = 0.1

Based on the threat frequency documented in previous section and the value entered in the vulnerability questionnaire of "I" (Implemented), "P" (partial), "NI" (Not Implemented), and "N/A" (Not Applicable) a likelihood value is assigned to the threat-vulnerability pairs listed in the RA table using the mappings shown in below Table

Table 4.2. Assignment of Likelihood Values

Countermeasure Implementation Status	**Threat Frequency**		
	High (3)	**Moderate (2)**	**Low (1)**
I (Implemented)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1
P (Partially Implemented)	Likelihood = 0.5	Likelihood = 0.5	Likelihood = 0.1
NI (Not Implemented)	Likelihood = 1.0	Likelihood = 1.0	Likelihood = 0.5
NA (Not Applicable)	Likelihood = 0.1	Likelihood = 0.1	Likelihood = 0.1

Table 4.3. Assignment of Likelihood Values

Countermeasure Implementation Status	**Level**	**Value**	**Risk**
I (Implemented)	Moderate (50)	10%	Strategic Risk
I (Implemented)	High (100)	10%	Operational/Transaction Risk
P (Partially Implemented)	High (100)	50%	Technology Risks
P (Partially Implemented)	Moderate (50)	50%	Business Risk
I (Implemented)	High (100)	10%	Online Fraud Risk:
NI (Not Implemented)	Low (10)	50%	Reputation Risk
NA (Not Applicable)	Low (10)	10%	Legal Risk

Risk Level

A relative risk level was determined for each vulnerability. The purpose in defining this risk level is to determine both the overall level of risk for the system as well as the degree to which each vulnerability contributes to that risk. The risk level for each control also serves as the basis for prioritizing controls for implementation.

The determination of risk for a particular threat/vulnerability pair can be expressed as a function of the likelihood of occurrence and magnitude of impact. The overall level of risk for each control was determined by the following formula:

Risk = Likelihood x Impact.

Table 4.4. Indicates the range of possible risk values

Risk Level Range of Values						
Availability/Denial of Service		**Integrity/Destruction and/or Modification**		**Confidentiality/Unauth. Disclosure**		**Risk**
Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	Level
High = 1	High = 100	High = 1	High = 100	High = 1	High = 100	
Med = .5	Med = 50	Med = .5	Med = 50	Med = .5	Med = 50	
Low = .1	Low = 10	Low = .1	Low = 10	Low = .1	Low = 10	
1	100	1	100	1	100	300
0.5	50	0.5	50	0.5	50	75

0	1	0	1	0.1	10	3

Table 4.5. Risk Level Matrix

Risk Level Range of Values							
	Availability /Denial of Service		Integrity/Destruction and/or Modification		Confidentiality/ Unauth. Disclosure		
	Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	Likelihood of Occurrence	Impact	
	High = 1	High = 100	High = 1	High = 100	High = 1	High = 100	
	Med = .5	Med = 50	Med = .5	Med = 50	Med = .5	Med = 50	
Risk	Low = .1	Low = 10	Low = .1	Low = 10	Low = .1	Low = 10	Risk Level
Strategic Risk	0.1	50	0.1	50	0.1	50	15
Operational/ Transaction Risk	0.1	100	0.5	100	0.5	100	110
Technology Risks	0.5	100	1	100	1	100	250
Business Risk	0.5	50	0.1	50	0.1	50	35
Online Fraud Risk:	0.1	100	1	100	1	100	210
Reputation Risk	0.5	10	0.1	50	0.5	50	35
Legal Risk	0.1	10	0.1	10	0.1	50	7

As illustrated in the table 4.5 above, three is the lowest possible value for risk, 75 is the median value, and 300 is the highest possible value using this methodology.

Table 4.6 below shows the possible risk ranges for the system. Given the sensitivity values for the environment, the maximum possible risk value is 300, which falls in the high level of risk.

Table 4.6. Risk Value Matrix

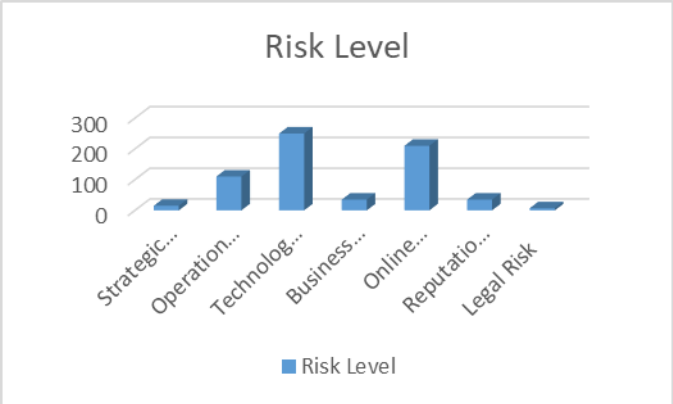
Risk	Impact Value	Likelihood value	Risk = Likelihood x Impact
Strategic Risk	50	0.1	5
Operational/Transaction Risk	100	0.1	10
Technology Risks	100	0.5	50
Business Risk	50	0.5	25
Online Fraud Risk:	100	0.1	10
Reputation Risk	10	0.5	5
Legal Risk	10	0.1	1

Table 4.7. Risk Value Matrix

Risk Type	Risk Level
Strategic Risk	15
Operational/Transaction Risk	110
Technology Risks	250
Business Risk	35
Online Fraud Risk:	210
Reputation Risk	35
Legal Risk	7

Risk Summary

The following figure summarizes risk assessment findings as documented in Table 5.1:



The results of the risk assessment of e-banking system indicated that the primary risks to system resources technology risks, online fraud risk and operational and transaction risk.

The assessment found that identified risks could be fully mitigated through the implementation of security controls specified in the e-banking Security Plan and in the accompanying Plan of Action and Milestones.

V. Cost-Benefit Analysis

Single-loss expectancy

Single-loss expectancy (SLE) is the monetary value expected from the occurrence of a risk on an asset. It is related to risk management and risk assessment.

Single-loss expectancy is mathematically expressed as:
Single loss expectancy (SLE) = Asset Value (AV) * Exposure factor (EF).
Where the exposure factor is represented in the impact of the risk over the asset, or percentage of asset lost. The result is a monetary value in the same unit as the single-loss expectancy is expressed (Euros, dollars, yens, etc.): exposure factor is the subjective, potential percentage of loss to a specific asset if a specific threat is realized. The exposure factor is a subjective value that the person assessing risk must define.

The annualized loss expectancy (ALE): is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as:
ALE = ARO x SLE
The annualized loss expectancy is the product of the annual rate of occurrence (ARO) and the single loss expectancy. ALE = ARO * SLE

Cost-Benefit Analysis

Determines whether a particular control is worth its cost (Money saved – net reduction benefits) NET risk reduction benefits (NRRB)= NRRB = [ALE(prior) -ALE(post)]–ACS.
ALE(prior) –ALE before implementing control
ALE(post) –ALE after implementing control
ACS –annual cost of safeguard

The results of the cost benefit analysis of e-banking system indicated that the primary cost benefits for the bank will be by implemented the countermeasure of business threats, technology threats, operational and transaction threats, online fraud threats, reputation threats and all it has to be on the accepted level. For strategic assets it can be and legal assets it can be avoid.

Summary

The impact of e-banking on risk management is complex and dynamic. Management should constantly reassess and update its risk control and mitigation approaches to take into account varying circumstances and changes to its risk profile in the internet environment.

VI. CONCLUSIONS

With the explosive spread of the Internet and electronic financial transactions such as online banking has become a universally accepted common practice. The online security service has become an essential requirement and a new directive critical in the evaluation of the competitiveness of an online banking service and other financial institutions. Therefore, the providers of online banking services should be more responsive to security requirements, and makes the online transaction have a layered protection against security threats. The necessity for a strong authentication solution became inevitable in banking services because of the growing pace of the transition technology adoption along with the unfortunate rise in fraud and security breaches. The strong authentication such as two factor authentication, usage of biometrics and quantum cryptology along with a proper way of customer sensitization are important to increase security and reduce the stealing of customer data. Banks should take the security considerations as part of their service offerings. Accordingly, it is obligated to provide a safe banking online environment based on the advanced security procedures.

REFERENCES

1- E-BANKING – IMPACT, RISKS, SECURITY
2- Universitatea Româno American_, B-dul Lacul Tei, nr 71, bl 18, sc B, et. 2, ap. 55, sector 2, Bucuresti, Tel : 0762985187, e-mail: cristina_titrade@yahoo.com
3- International Journal of Marketing, Financial Services & Management Research Vol.1 Issue 9, September 2012, ISSN 2277 3622 www.indianresearchjournals.com 164 RISKS IN E-BANKING AND THEIR MANAGEMENT
4- Security Risk Management Cost-Benefit Analysis book/ Instrutor: N. Vlajic, Winter 2015.
5- RISK AND INOVATION IN E-BANKING Cezar MIHALCESCU, Beatrice CIOLACU, Florentina PAVEL, Cristina TITRADE / Romanian – American University, Bucharest, Romania
6- The Risks &Advantages of Online Banking http://smallbusiness.chron.com/risks-advantages-online-banking-2249.html