ISSN (Online): 2230-7893
www.IJCEM.org

Information Security in Banking and Financial Industry

Vishal R. Ambhire[1], Prakash S. Teltumde[2]

[1,2]Computer Department, V.J.T.I.,
Mumbai, Maharashtra, India
[1]vishalambhire@gmail.com

[2]pst205@gmail.com

Abstract

It summarizes the influence elements introducing the concept of information technologies in financial and banking industries and analysis the relationship of information technology risk factors. By using the case study, research design and methods, and investigative study is conducted. IT security management practice is discussed. The potential vulnerabilities that exist in the system with reference to data leak, suggestions to safeguard from such threats are presented. It explores why information security should be a priority for businesses and deals with how a security expert can model potential losses for their organization. This paper identifies four security issues (access to information system, secure communication, security management, development of secure information systems).

Keywords: *information; security; banking; finance; phishing; vulnerability; authentication.*

1. Introduction

Information security issue is the most important one in using Internet and it becomes more crucial while implementing the Internet in banking sectors. This research revealed a lot of risks and threats to the security of online banking information which are increasing day by day. The demand for high security in banking & financial services creates both challenges and new business opportunities. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations. Financial institutions and banks protect their information by instituting a security process that *identifies risks*, *forms* a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks.

Information security in finance and banking can be increased by striving certain objectives like availability, integrity, confidentiality, accountability and assurance. Security objectives can be achieved by Information Security Risk Assessment, Strategy, Controls Implementation, Monitoring & Process Monitoring and Updating. Monitoring and updating makes the process continuous instead of a one-time event. Security risk variables include threats, vulnerabilities, attack techniques, the expected zMumbai, India frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture. These standards provide systematic management approach to adopt the best practice controls, quantify the level of acceptable risk and implement the appropriate measures which protect the confidentiality, integrity and availability (CIA) of information. Technical control improves security by Identity Authentication Management, Access Control Technology, Firewall Technology & Encryption technology (key technology). Internal control reduces the harm caused by internal personnel morals risk, the system resources risk and the computer virus.

2. Literature Review

The history of online banking is not very ancient, but it has made its possession strongest within two decades which has been possible due to its characteristic features. Not very long ago, in the early 1990s Internet banking has sprayed its network following some barriers of ATM, ATM network, PC banking and home banking in 1970s and 1980s. Now Internet banking is increasing rapidly instead of having the possibility of some sort of fraudulent activities. In a study, in Singapore, researchers found that people who accepted Internet banking compared to those who did not, acknowledged Internet banking to be more convenient, less complex, and more compatible. Some researchers have argued that still ebanking technology is not matured enough.

However, by the end of 2002, some estimates proved that as many as 30 percent of Americans were doing banking online, which increased at 50 percent in 2003. Similarly, others forecasted that over 20 million people in the UK will adopt e-banking by the end of 2005. This trend is also apparent in Singapore, Sweden, Germany and Norway, and the more advanced service-providing

economies in the world, and also in India. Nevertheless, security played an important role in adopting Internet banking and the continuation of its use which indicates that the security concerns are directly linked with the adoption of online banking.

2.1 Technical

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The elements are confidentiality, possession, integrity, authenticity, availability, and utility.

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Integrity means that data cannot be modified undetectably.[citation needed] This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit.

For any information 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. Non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

2.2 Banking

With the wide-expansion of mobile telecommunication technology into the business world, mobile banking became the popular and promising banking method in bank industry recently. Mobile banking can provide customers with better quality and more cost-saving services. It refers to provision and availment of banking and financial services with the help of mobile telecommunication devices. The scope of provided services may include facilities to conduct bank and investment market transactions, to administer accounts and to access customized information. Most of the mobile banking researchers agreed that mobile banking consists of three parts: mobile accounting, mobile brokerage and mobile financial information services. For customer service sector including: balance checking, account transactions, payment, etc. conventional banking services. Increasingly, bank customers will expect real-time information and access 24 hours a day, seven days a week, wherever they are in the world. Services such as electronic account management, mobile brokerage and financial information and alerts enable banks and network operators to increase bank's competitive edge and strengthen customer loyalty.

A mobile banking system comprises a mobile banking unit and a data processing centre which may be the mainframe computer of the bank responsible for processing banking transactions and data storage. The mobile banking includes one or more banking terminals such as ATMs, deposit machines and multimedia enquiry stations.

Mobile banking system has provided a good foundation for providing personalized, customer- oriented, new model of financial services, which incorporates a number of wireless communication channels, integrate the merits of different technologies.

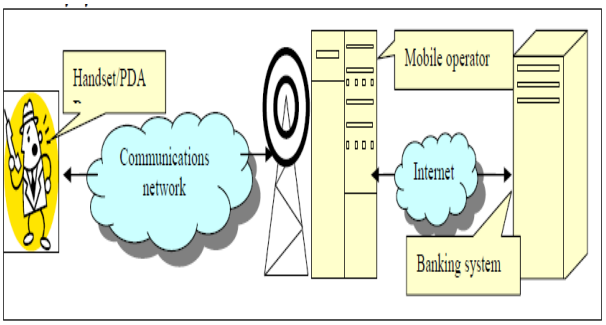

Fig. 1 Mobile Banking Operation System

2.3 Financial

The most important technologies include: Cryptography, Steganography, PKI (Public Key Infrastructure), Electronic Signature, Electronic Certification, Security Protocols, Authentication Protocols, Firewalls and Proxies, Access Control Models, Passwords,

ISSN (Online): 2230-7893
www.IJCEM.org

Digital Envelope, Biological Security technologies, Filtering, Intrusion Detection Systems.

3. Proposed Model: General

The Internet is radically transforming the provision of services and goods because of its immediacy, openness, ubiquity, and global reach. The financial and banking industry has not been aloof from the Internet but has fully embraced its new potentialities as demonstrated by a variegated set of new financial services offered to clients at competitive rates. The purpose of this research is to compare and test the success and failure of the possible strategies to counter the multiple risks facing online financial institutions in the experimental set up of Synthetic Environments for Simulation and Analysis (SEAS). This research intends to provide guidelines to the existing and future businesses for forming the information security policies and strategies to survive in a dynamic and hostile environment.

These statistics are not circumscribed to so-called "brick and mortar" financial institutions like American Express, BankOne, or Citigroup that have espoused the Internet to provide new services and products in order to exploit rapid growth of online users.

Table 1: Business model for Online Banks

Business Model	Features	Example
Vertical Portal	• Distribute information and financial solutions • Customers can access information and execute transactions (e.g., online bill payment)	Bank One Citibank American Express
Aggregator	• Visitors can compare products such as mortgages or insurance policies • Sell product prices and information, sometimes acting as intermediaries between online agents or brokers	InsWeb E-Loan QuickenMortgage InsureMarket
Specialty Manufacturer	• Provide a diverse array of ready-made services for Internet distribution points such as aggregators or vertical portals • Web presence is less important to these companies than producing a superior, low-cost, well-recognized brand name product	Capitol One MBNA Janus

The perpetrators of these security breaches may be classified in two groups: external agents and insiders. According to the 2000 CSI Computer Security Survey, almost three-quarters of the corporate respondents have suffered abuses from insiders. Motivations for these misuses vary from personal frustrations related to perceived lack of financial entailment for professional skills, computer dependency, and reduced loyalty to employers.

Table 2: Classification of Perpetrators

Perpetrators	Threat	Examples
External	Exploit Internet ubiquity and anonymity as advantageous feature to accomplish their objectives	• Hackers • Terrorist organizations • Business competitors • Organized crime • Foreign intelligence
Internal	Authorized users who exploit their system access to achieve specific objectives	• Employee • Contractor • Teleworker

4. Case Study

4.1 Banking: Phishing Attack in UAE

"Phishing" is a form of Internet fraud that aims at stealing valuable information such as credit cards, social security numbers, user IDs and passwords. The fraud starts by creating a fake website that looks exactly like that of a legitimate organization but with a slightly different URL address. In many cases, the organizations are financial institutions such as banks. An email is then sent to thousands of internet users requesting them to access the fake website, which is a replica of the trusted site, to update their records by entering their personal details, including security access codes. The page generally looks genuine. Note that the email has a FROM address that is identical to the original organization address, e.g. Human Resource or IT director, to make users believe that the email is authentic. However, the FROM field in an email can be easily faked by a hacker and the email is actually coming from the hacker's computer.

In the Middle East, cyber criminals are increasingly targeting UAE residents with advanced hacking methods, one of which is phishing scams. Such scams have caused UAE banks to raise their IT security services in recent years. One of the detected attacks involved a duplicate website of the UAE's Ministry of Labor which had a URL of: http://www. uaeministryoflabour.tk. among the students, faculty, and staff of the American University of Sharjah (AUS) in UAE. The university consists of 10,000 students and alumni in addition to 1,000 faculty and staff. The students come from 70+ nationalities. Note that the authentic URL of the Ministry is http://www.mo/.gov.ae. The fake website was cheating people who wanted to find a job in the UAB. In order to study the vulnerability of users to phishing attacks in the Middle East, a controlled phishing experiment was conducted The university was founded in 1997 and offers 26 majors and 42 minors at the undergraduate's level and 13 master's degrees programs through four colleges (Arts and Science; Engineering;

Architecture, Art and Design; Business and Management). The language of instruction at the University is English.

A fake website was setup to look identical to an AUS website that is accessed by the users to change their AUS passwords. The domain name (http://www.myaus.irifo) was used to host the fake phishing website. Note that the phishing domain is different than the original website domain (https://passwords. aus.edu). An email was sent to all AUS users asking them to urgently change their passwords due to a security breach. The AUS FROM address was faked to look identical to the AUS IT Department email address. Once the email was received by the users, they were requested to click on a link https:llpasswords. aus.edu which redirected the users to the fake phishing website http://www.myaus.info. The users were asked to enter their usemames and click on the continue button. They were supposed to be taken to a second page to enter their old and new passwords; however, to ensure that no passwords were entered, the users were directed to a second page with a timeout error and a message asking them to try again after an hour due to heavy system usage. A database was used to log all entered usernames with the corresponding date and time. User anonymity was ensured and no usernames were revealed. The goal was only to count the number of potential victims. The phishing website was left online for 10 days. The AUS IT Department typically sends a warning email to all AUS users whenever similar phishing emails are sent to AUS users. The Department also sends periodical emails alerting users to the latest IT security threats. In the experiment's case, the IT Department sent a warning email a few hours after the original phishing email. Despite the warning emails, 954 users out of the 11,000 AUS users entered their usernames to the phishing website. Of those, 96% were students.

As users, today, are becoming familiar with phishing attacks, hackers are launching more
sophisticated phishing attacks known as Spear Phishing. The idea is to send a phishing email targeting specific names in governments or financial enterprises. The emails typically belong to senior executives and include personally identifiable information that is collected of public websites or social pages, e.g. facebook. Only a limited number of emails are sent to make the emails look credible and avoid publicizing the attack. Such attacks usually end up with the victim passing his or her personal information and passwords.

4.2 Financial: Data Security in Finance Industry

See how PrimeRevenue Inc. uses FileAssurity OpenPGP Command Line to: protect customer financial and personal information verify files that have been transferred save time and money PrimeRevenue chose FileAssurity PGP Command Line over McAfee Ebusiness Server.

PrimeRevenue, Inc. is a leading supplier of Financial Supply Chain managed service software. PrimeRevenue, Inc. bridges the supply chain with financial services to optimize the total relationship between buyers and suppliers to return immediate bottom line benefit to each. This case study shows how PrimeRevenue saved time and money implementing FileAssurity PGP Command Line to protect large volumes of sensitive financial information being sent to partner banks.

PrimeRevenue realised that an SSL solution would not be secure enough and looked for a standards based solution using digital signature and encryption technology that would satisfy their demanding requirements. They identified the OpenPGP standard as being the most widely implemented technology for file encryption and digital signatures and searched for a suitable product to work with.

PrimeRevenue had to support a number of business processes in the secure operations they deliver to their business partners, including: encrypting and digitally signing files for the recipient bank(s) using FTP to send files to their partner banks verifying those files with the banks being able to archive files by re-encrypting them with their own key securely deleting original files to ensure they cannot be recovered and compromised providing an audit log of the whole process for accountability reasons. PrimeRevenue evaluated a number of products before deciding to purchase FileAssurity PGP Command Line as the best of the competition.

Jeff Simizon of PrimeRevenue said 'The main reasons we selected ArticSoft was cost and ease of use. With the economy the way it is today we look to save money, but at the same time are not willing to sacrifice functionality in a product. After evaluating McAfee E-Business Server and similar (they did not have the equivalent of the functionality of CLS ' so to implement their solutions we would have had to do some programming ourselves) we determined that ArticSoft had more to offer at a fraction of the price. Some of our partner banks are using McAfee E-Business Server or similar, and we have not had any compatibility issues. So it was a win win situation for us ' full interoperability, lower cost, greater functionality and greater ease of use all in one package'

Implementation was quick and easy. After the download it was all up and running in 15 minutes. Other products we tested were somewhat more time consuming. We have not had to call ArticSoft support yet, but have used their email support, and they have been very responsive. I think one reason we have not used support much is due to the products ease of use, and that it does what it says.

" Our customers find that they get more from our solutions," says Steve Mathews, CEO of ArticSoft. " More savings, more ROI, more features and more capability. And that is what we aim to provide with all our FileAssurity products. FileAssurity PGP Command Line is an out of the box, setup and forget product that runs each time and every time."

5. Conclusion

It summarizes the influence elements introducing the concept of information technologies in financial and banking industries and analyze the relationship of information technology risk factors. It explores why information security should be a priority for businesses and deals with how a security expert can model potential losses for their organization. It also provides guidelines for professionals to make well informed decisions.

This paper also provides investigation information system security in the context of internet banking. Overall study proves that attention to the importance of security in financial transactions is significant, mobile technologies had been discussed and studied for their usage in financial transactions.

1. Acknowledgement

I would like to thank all those people whose support and cooperation has been an invaluable asset during the course of this Seminar. I would also like to thank my Guide Dr. B.B.Meshram for guiding us throughout this Seminar and giving it the present shape. It would have been impossible to complete the seminar without their support, valuable suggestions, criticism, encouragement and guidance.

I am grateful for all other teaching and non-teaching staff members of the Computer Technology for directly or indirectly helping us for the completion of this seminar and the resources provided.

References

[1] Computer Security Institute. 2000 Computer Crime and Security Survey, 2000 (available from http://www.gocsi.com; accessed March 2000).

[2] Information Security Industry Survey. Information Security Magazine, July 1999 (available at http://www.infosecuritymag.com; accessed September 1999).

[3] Online Banking Report. The Online Banking Report, 1999 (available from http://www.onlinebankingreport.com; accessed September 1999).

[4] "Leading UAE newspaper's website hacked", Arabian Business, 2008. Available at: http://www.arabianbusiness.com1519982-leading-uae-newspapers-website-hacked.

[5] "UAE cybercrime squad gunning forward", Arabian Business, 2009. Available at: http://www.Arabianbusiness.coml553470-uae-cybercrime-squad-gunning-forward.

[6] "UAE bank targeted in major phishing attacks", ITP,2010. Available at: http://www.itp.netl579059-uae-banktargeted-in-major-phishing-attack.

[7] Rajnish Tiwari，Stephan Buse and Cornelius Herstatt ： Customer on the move ： Strategic Implication of MobileBanking for Banks and Financial Enterprises. E-Commerce Technology, 2006.

[8] Tiwari, and Buse, 2007: The mobile Commerce prospects: A strategic Analysis of Opportunities in the Banking Sector, Hamburger University Press.

[9] APWG, Phishing Activity Trends Report, Q4 2009. Available at: http://www.antiphishing.org/reportslapwg_ report_Q4 2009.pdf

[10] "NBK online banking customers targeted b! Phishing attacks", Arabian Business, 2008. Available at: http://www.arabianbusiness.coml522781-nbk-onlinebanking-customers-targeted-by-phishing-attack

[11] UAE-CERT, http://www.aecert.ael