2016

E-banking in Bangladesh: Vulnerabilities and Securities

Uddin, Md. Nokib

University of Rajshahi

E-banking in Bangladesh:

Vulnerabilities and Securities

PhD Dissertation

By

Md. Nokib Uddin

A Dissertation

Submitted to the Institute of Bangladesh Studies (IBS), University of Rajshahi

in Partial Fulfillment of the Requirement for the Degree of

Doctor of Philosophy
in
Finance and Banking

INSTITUTE OF BANGLADESH STUDIES
UNIVERSITY OF RAJSHAHI, BANGLADESH

2016

E-banking in Bangladesh:

Vulnerabilities and Securities

PhD Dissertation

By

Md. Nokib Uddin
PhD Fellow
Institute of Bangladesh Studies
University of Rajshahi

Supervisor

Dr. AHM Ziaul Haq
Professor, Dept. of Finance,
University of Rajshahi.

INSTITUTE OF BANGLADESH STUDIES
UNIVERSITY OF RAJSHAHI, BANGLADESH

2016

Certificate

This is to certify that the dissertation entitled, **"E-banking in Bangladesh: Vulnerabilities and Securities"** submitted by Mr. Md. Nokib Uddin to the Institute of Bangladesh Studies (IBS) University of Rajshahi, for the award of Degree, of Doctor of Philosophy in Finance and Banking is a record of research work done under my supervision during the academic period 2013-16 and the dissertation has not designed or conducted the basis of the award of any Degree, Associate-ship, Fellowship or any other similar titles of any university or institution. It is also certified that the dissertation represents an independent work on the part of the candidate.

Rajshahi,
2016

Dr. AHM Ziaul Haq
Professor
Department of Finance
University of Rajshahi
and
Research Supervisor

Declaration

I, the undersigned, hereby declare that this dissertation entitled, **"E-banking in Bangladesh: Vulnerabilities and Securities"** submitted to the Institute of Bangladesh Studies, University of Rajshahi for the degree of Doctor of Philosophy in Finance and Banking is a record of independent research work carried out by me under the supervision and guidance of **Dr. AHM Ziaul Haq**, Professor Department of Finance, University of Rajshahi. This has not been submitted to any other University or institute for the award of any degree, associate-ship or other similar purposes.

Rajshahi,
2016

Md. Nokib Uddin
PhD Fellow
Session: 2013-14
Institute of Bangladesh Studies
University of Rajshahi
And
Programmer (Principal Officer)
Sonali Bank Ltd.

Acknowledgements

Completion of this doctoral dissertation was possible with the support of several people. I would like to express my sincere gratitude to all of them.

First of all, I am extremely grateful to my research supervisor, Dr. AHM Ziaul Haq, Professor, Department of Finance, University of Rajshahi for his valuable guidance, scholarly inputs and consistent encouragement, I received throughout the research work. This feat was possible only because of the unconditional support provided by Sir. A person with an amicable and positive disposition, Sir has always made himself available to clarify my concept despite his busy schedules and I consider it as a great opportunity to do my doctoral programme under his guidance and to learn from his research expertise.

I thank Dr. Swarochish Sarker, Professor and Director. Institute of Bangladesh Studies, University of Rajshahi, for the academic support and the facilities provided to carry out the research work at the Institute. I also express my gratitude to Dr. M. Zainul Abedin, Professor of Economics, Institute of Bangladesh Studies, University of Rajshahi, for his very encouraging and supportive role. I am equally thankful and humble to all the faculty members specially.

The dissertation would not have come to a successful completion, without the help I received from the staff of this institute. No research is possible without the Library, the centre of learning resources. I also take this time to express my gratitude to all the library staff for their services.

I thank to all the fellows of Institute of Bangladesh Studies from different session, for their friendship, collaboration, and cooperation in the past few years that made this dissertation a wonderful journey.

My dear colleagues and Excellence Afzal Hossain (GM), Hasanul Banna (DGM), Monwar Hossain (SPO), Md. Hafizur Rahman (SO) and many others of Sonali Bank Ltd. have all extended their support in a very special way, and I gained a lot from them, through their personal and scholarly interactions, their suggestions at various points of my research programme.

I wish to thank profusely to S. M. Mohosinur Rahman, Head of IT Security and other executives of Dutch Bangla Bank Ltd. and Bangladesh Bank for playing their significant role to my multi-tasked activities during the study.

I owe a lot to my parents, who encouraged and helped me at every stage of my personal and academic life, and longed to see this achievement come true.

I extend my gratitude to Dr. Md. Nasim Mahmud, Deputy Chief Technical officer, Department of Statistics, University of Rajshahi to give me an effective suggestion about statistical analysis.

I am very much indebted to my family, my wife, son and my daughter, who supported me in every possible way to see the completion of this work.

Above all, I owe it all to Almighty God for granting me the wisdom, health and strength to undertake the whole research task and enabling me to its completion.

Rajshahi,
2016

Md. Nokib Uddin
PhD Fellow
Institute of Bangladesh Studies,
University of Rajshahi,
and
Programmer (Principal Officer)
Sonali Bank Ltd. Bangladesh

Acronyms and Abbreviations

ABB	: Any Branch Banking
BCC	: Bangladesh Computer Council
BTRC	: Bangladesh Telecommunication Regulatory Commission
BEFTN	: Bangladesh electronic funds transfer network
BIBM	: Bangladesh Institute of Bank Management
CB	: Commercial Bank
CHIPS	: The Clearing House Inter-bank Payment Service
CBS	: Core Banking System
DNS	: Domain Name System
DRS	: Disaster Recovery Service
DBBL	: Dutch-Bangla Bank Limited
EFT	: Electronic Fund Transfer
HR	: Human Resource
IT	: Information Technology
ICT	: Information and Communication Technology
ISP	: Internet Service Provider
LAN	: Local Area Network
MFS	: Mobile Financial Services
OSI	: Open System Interconnection
POS	: Point of Sale
PKI	: Public Key Infrastructure
SWIFT	: Society for Worldwide Interbank Financial Telecommunication
SPSS	: Statistical Package for Social Science
SBL	: Sonali Bank Limited
TCP/IP	: Transport Control Protocol/ Internet Protocol
VPN	: Virtual Private Network
WWW	: World Wide Web

Abstract

Nowadays, e-banking security vulnerability is an inevitable part to operate digitized banking system. So, the area of e-banking vulnerability and security brings attention of bankers as well as its stakeholders during the last few years. Statistics show that banks business, image and its commercial success rather closely depend on proper security measures. On the contrary, reducing core risks, customer satisfaction and competitiveness are associated with e-banking vulnerabilities and securities.

In Bangladesh, e-bankers have been facing diverse challenges continuously to render its services to the customer. Quick service, error free transaction, never-ending networking and tech-savvy experienced people are needed to provide quality services what is an integral part of e-security.

The host study considers the above mentioned issues to keep the digital banking system safe and sustain. In order to do so, three major e-securities (i.e. technological, operational and legal frame or compliances) have fixed up for the population banks.

This study basically searched major issues that influenced CB's to adopt e-security to smooth banking operations. To meet the challenges, researcher used both qualitative and quantitative data. It is an evaluation research under applied social science research using survey method techniques. The logical process of the research investigation is inductive to move from the particular to general making decisions and is sometimes called a bottom-up approach. Collected data from the respondents were analyzed using the statistical tool SPSS software. Simple percentage method was used in the study to analysis security vulnerabilities and its relation with other parameters to clarify the results. Correlations and Pearson Chi-square tests were used for determining the association and relationship among the variables. Three divisional controlling

offices and branches including head office of both banks were purposively selected for collecting primary data. The total sample size for the study was 119 (One hundred and nineteen) which were divided into different strata. The study evaluated data collected from two potential CBs of Bangladesh up to January 2016 and also used purposive sampling techniques. It had almost been completed on the basis of both primary and secondary data.

The result of the study revealed that e-banking vulnerabilities and securities have significant association among the variables like core risks of bank, customer satisfaction and commercial success of bank. The study also found that systems of both sample banks (Sonali Bank Ltd. and Dutch-Bangla Bank Ltd.) are vulnerable in some context. But from security point of view one has better security system compare to another.

The study findings suggest that security relating to technology, operation and compliance (both internal and external) is required to reduce vulnerabilities and rendering effective service to valued stakeholders. Hence, central bank of Bangladesh has to play all most all possible and time demanding measures as a regulatory authority to keep CB's digital transactions safe and secure.

Contents

List of Tables

List of Figures

List of Charts

List of Appendices

Chapter I
Introduction

1.1 Background of the Study

Modern banking is merely impossible without proper digitization or automation. Nowadays, business and technology are interrelated and interconnected with each other. Even bank customers want low cost and inclusive financial transactions. Bank can easily ensure it through e-banking (electronic banking) by using digital devices. In the world of banking, it is a new trend and non-traditional financial channel to provide financial services to the customer. Moreover, it is also an alternative delivery channel to guarantee numerous innovative financial services to the clients using digital outfits. Even, it has already been familiarized as a state-of-the-art to the digitized banks. Today, e-banking experienced huge growth in many countries as well as in Bangladesh. But the new trend has turned out CBs a great risk. Today the main fences to e-banking are lack of security, vulnerabilities of the system, lack of customer's trust and possible legal requirements.

The banking sector has recently transformed its operational mode and traditional banking practice by Introducing e-banking. More than 95% of banks are offering e-banking services through centralized and distributed system. Instead of manual process, CBs have been providing services to their valued customer and are processing all these information (data) by using ICT. To do so, CBs have installed huge intelligent (digital) devices within their own scope and the devices are somehow connected with inside and outside resources (Intranet, Internet, or Extranet). According to IT experts and professionals, all these information are

treated as organizational assets as well as very important tool for internal and external users (i.e. data items on a computer are assets, too).[1] But that information and technology both sometime experience serious vulnerabilities and threats which can paralyze the whole system and invite risks. Automation can not only strengthen the operational activities of banks but also weaken their control over its system. So, security policy and mechanism both are major concern in this part. Security of IT systems for a financial institution has, therefore, gained much greater in importance, and it is vital that such risks should properly be identified and managed. Information assets are critical to the services provided by the banks to their customer. Protection and maintenance of these assets are critical to the organizations' sustainability. Banks must take the responsibility of protecting information from unauthorized access, modification; disclosure and destruction to protect customers' interest.[2] E-security is not only a considerable part for customers' satisfaction but it is much important for banks internal management. So, bank people need to understand the major vulnerabilities and security issues relating to e-banking in a versatile networked world.

Control over the security vulnerabilities ultimately mitigate core risks, attain customer satisfaction and gain bank's commercial success. Without commercial success bank cannot continue their business. So, in order to continue bank business and to make profitability in a certain level security vulnerabilities of e-banking obviously is an important determinant.

---

[1] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Analyzing Computer Security:* A *threat/Vulnerability/Countermeasures an approach (*New Jersey: Pearson Education Inc., 2011*), 8.*

[2] Bangladesh Bank, *Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions (version 2.0* April, 2010),1.

E-banking is a service. This distribution channel covers all the banking service sections such as general banking, loan and advance, investment, foreign exchange transactions and other ancillary services of society. Even it works as an alternative advanced distribution channel delivering ATM service, POS, First Track, Switching software and so on. But it should be executed through secured and flaws free system. Bank cannot able to make profitability until or unless it is safe. There are three types of e-banking security flaws described in this study such as technological, operational and law related. However, risk minimization, customer satisfaction and business success is explicably depends on e-banking security vulnerabilities.

It is high time to the country like Bangladesh finding out the flaws relating to e-banking and taking security measures for frictionless or smooth operation of banking services. CBs cannot perform properly with electronic threats and risks. On the other hand, people trustworthiness on the systems and clientele of bank are not possible without e-security. The recent cue in banking sector has raised critical question about e-banking adoption. However, in order to fulfillment of sound business and customer satisfaction e-security is inevitable part for banks.

So the study basically focused on e-banking vulnerabilities and securities of CBs here in Bangladesh.

1.2 Problem Statement and Research Question

Electronic banking is a process that makes CBs cost effective, customer friendly and more informative. Electronic banking, first conceptualized in the mid-1970s, some banks offered customers electronic banking in 1980s. The Internet explosion

in the 1990s made people more comfortable with making transaction over the web.[3] Before that we found e-banking started in the early 1980s both in the United States and the United Kingdom sporadically not globally. Four major banks of USA- Citibank, Chase Manhattan, Chemical and Manufacturers Hanover--offered home banking services. It was the Nottingham Building Society that in 1983 introduced Britain's first electronic home banking service through a joint venture with Prestel, a computerized information service owned by British Telecom. In India electronic banking arrived in the late 1990s. ICICI was the first bank to champion its usage and introduced internet banking to its customers in 1996.[4] In Bangladesh, Dutch-Bangla Bank Ltd. a private commercial bank is the first bank to be fully automated and introduced e- banking but the automation was completed in 2003.[5]

It is said that invention of www (an internet-based hypermedia initiative for global information sharing) site by the father of internet Sir Tim Berners-Lee in 1989,[6] the revolutionary change has occurred in e-business and opening the new integrated virtual environment all over the world. Economy and business entity took e-shape within their operational area. Organization can easily transmit data by using networking and DNS server. Public and private IP over internet is conceptualized using TCP/IP communication. It is proved that information technology makes the operation easier than before. But finding some remarkable issues like e-security and sustainability are commonly ignored by the users sometime which can paralyze technology as well as operation of the whole system within any digitalized organization.

[3] http://www.ehow.com/about_5109945_history-ebanking.html (Accessed on: August 12, 2014).
[4] http://userindesign.com/Images/Papers/Online_Banking_Springer.pdf (Accessed on: August 12, 2014).
[5] http://www.dutchbanglabank.com/electronic_banking/introduction.html (Accessed on: August 12, 2014).
[6] http://inventors.about.com/od/bstartinventors/p/TimBernersLee.htm (Accessed on: October 24, 2013).

Despite the effort of banks to ensure that customers reap the benefits of e-banking, the bank is met with complaints from customers as regards, malfunctioning ATMs, network downtime, online theft and fraud, non-availability of financial service, payment of hidden cost of e-banking like SMS for sending alert, mandatory acquisition of ATM cards and so on.[7] So, customers' recognition heavily depends on safe and secured e-banking services.

E-banking is already proved itself a low cost delivery channel, minimize transaction time for clients and a path to growth sales, increase business performance for bank but it is merely possible when the system is endless in all aspects and comparatively flaws are minimum level in the service.

Risk is common phenomena to e-banking service. This service provides many opportunities to the bank as well as customer, adversely it bears very complex form of threats. So, controlling such threats or risks is indispensible part to the banks' management. E-risk is inherent segment to the services and it should be properly identified and managed. Even bank's board and senior management oversight, security controls, legal and reputational risk management process are very much concern matter to this system.

In Bangladesh, financial service industry is a huge sector. There are many financial institutions like banks, insurance companies and semi-financial organizations are operating within this particular industry and they have all been gradually changing their operational mode from conventional manual system into automation. In banking sector, we found some revolutionary change in recent

[7] Ogunlowore Akindele John and Oladele Rotimi, "Analysis of electronic banking and customer satisfaction in Nigeria." *European Journal of Business and Social Sciences* 3, no.3 (June 2014):14-27.

time. Most of the public and private sector banks in our country have already completed their automation both internally and externally. It can be said that this particular automated system (e-banking services) act as a complementary and contemporary towards financial service sector of Bangladesh. Banks have launched attractive e-products (i.e. PC banking for financial transaction, ATM for quick financial transactions, POS for mobile banking, CHIPS for clearing house for interbank payment system, EFT for fund transfer and using SWIFT for cross border transaction.) through e-banking to provide cost effective, time saving and customer friendly banking. But this particular new e-trend in banking sector without taking proper security could be appeared insecure. Because, risks like human errors or intention, malware, phishing, skimming or hacking is very much common phenomena (threats) for this particular area. Most of the CBs now transmit their data (information) through virtual channel which is connected with third party domain or server (internet).

Like other central banks, Bangladesh Bank has been playing potential role as a regulatory authority of financial sector here in Bangladesh. This central bank has given a clear guideline what to do in this regard and proclaimed that ICT security risk issue is very important core risk for bank industry.[8] On the contrary, internal parallel security policy for ICT by each of the CBs has already been designed in accordance of security policy and mechanisms. However, all those steps ensure proper e-banking facilities for stakeholders.

But taking those steps by the banks seems not to be sufficiently enough. Even it is found that branches are sometime careless to follow directions of their own central

[8] Bangladesh Bank, *Risk Management Guidelines for Banks* (February, 2012).

and controlling authority as well as the central bank. On the contrary, central bank exposed its weaknesses to regulate and supervise over banks effectively.

In recent time, robbery of ATM card information by using skimming device at six ATM booths from three private commercial banks (Eastern Bank Ltd., United Commercial Bank Ltd. and City Bank Ltd.) shocked Bangladeshi ATM card holders as well as stakeholders of bank.[9] Transactions over online system among inter-bank are demonstrated vulnerable. It is proved that internal compliance of CBs is not only weak but the surveillance and effective regulation by the central bank is also exposed imperfect. It is to inform people that all these booths are connected with central bank national payment switch. So the central bank cannot evade its responsibilities in this concern. Recommendation by central bank to install anti-skimming and pin shield device has come days after of the incident but it could be possible during installation of ATM by the CBs. Even the system of BB is not secured. Reserved account of central bank with Federal Reserve Bank of New York hacked by cyber attacker last February 2016 and lost about $100 million (around 800 crore local currencies) by issuing thirty fake online payment advice from BB end using applicable credentials hacked by intruders. Five of thirty is automatically paid by the system to the beneficiaries summed about $100m according to Federal Reserve Bank of New York.[10]

In the objectives of Bangladesh Payment and Settlement System Regulations, 2014 affirmed under 2(a), (b) and (e) that the central bank will regulate, and supervise payment systems that operate in Bangladesh and ensure secure and

[9] "Tin bank-er choai boothe jaliater jantra," *bdnews24.com,* February 14, 2016.
[10] "BB account hacked, back office-er aat karmokorta najardarite," *bdnews24.com,* February 9, 2016.

efficient arrangements for settlement of these transactions. Even in the provision of Bangladesh Bank's order, it is said under 7A (e) that Bangladesh Bank will have to promote, regulate and ensure a secured and efficient payment system.[11] From stated point of view, the central bank is far behind to realize its commitment at all.

Recently, a government-formed ad hoc committee headed by Dr Farashuddin, former governor of the central bank found involvement of global financial network SWIFT and BB officials to heist BB $100 million.

So, more innovative and effective measures with accountability is desired and implemented for banks' information system. Because, fraud and forgeries are common event by the computer and computer professionals willingly and unwillingly (lack of awareness) in some CBs. In addition, unauthorized access by outside hackers has already created problems in banking sector.

Around 30 percent of the banks in Bangladesh carry 'very high' risks of online fraud and security threats, found in a study conducted by the BIBM. "Ignorance of these banks may pose serious security threats for the entire sector,"[12] The study exposed tech-based banking fraud and forgeries through pie-chat area by area. It noticed that fraud and forgeries by ATM about 43%, Mobile banking 25%, Cheque processing and e-fund transfer 15%, Internet banking 12%, Banking application software 3%, SWIFT and others 2%. Nevertheless, banks of Bangladesh face up to 300 malicious software attacks a day.[13]

[11] Bangladesh Bank Order, 1972 (President's Order No. 127 of 1972)
[12] "30 pc banks exposed to high risks of online fraud: study," *The daily Star*, 24 December 2013, sec. B, 1.
[13] "BD banks face300 malware attacks every day," *The Financial Express*, 7 May 2016.

In this circumstance, the study addresses some general questions here that is- Do the e-bankers of Bangladesh face any technological and operational vulnerabilities or risks? Does the industry and as well as its customers protected from security risks in tolerance level? Do the banks have adequate security measures? Is it sufficient for their smooth and effective operation? Is it adequate for customer satisfaction or to attain commercial success of bank? How can security mitigate core risks? Are the existing laws relating to e-banking security in Bangladesh appropriate? Is existing e-banking system vulnerable or not? All these questions can be considered as a research question.

1.3 Aims and objectives of the Study

The common aim of the study is to investigate and examine existing e-banking vulnerabilities and security status of the CBs.

The following are the specific objectives of the study to:

- investigate the major e-banking security vulnerabilities;
- check existing laws and regulations relating to e-banking securities;
- examine the impact of e-banking vulnerabilities on banks' commercial success;
- evaluate the impact of e-banking security on bank customers' satisfaction;
- observe the impact of existing e-banking security system in reducing banks' core risks; and

1.4 Definition of key terms

1.4.1 Information and Communication Technology

Information and communications technology (ICT) refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. Although ICT is often considered an extended synonym for information technology (IT), its scope is broader. ICT has more recently been used to describe the convergence of several technologies and the use of common transmission lines carrying very diverse data and communication types and formats.[14] In e-banking operation, the acronym ICT is applicable basically for using intelligent devices (i.e. computer, cell phone, networking devices etc.) transmission systems, and network-based control and monitoring functions. In broad sense, "Information and Communication Technologies" (ICT) refers to technologies that provide access to information through telecommunication.[15]

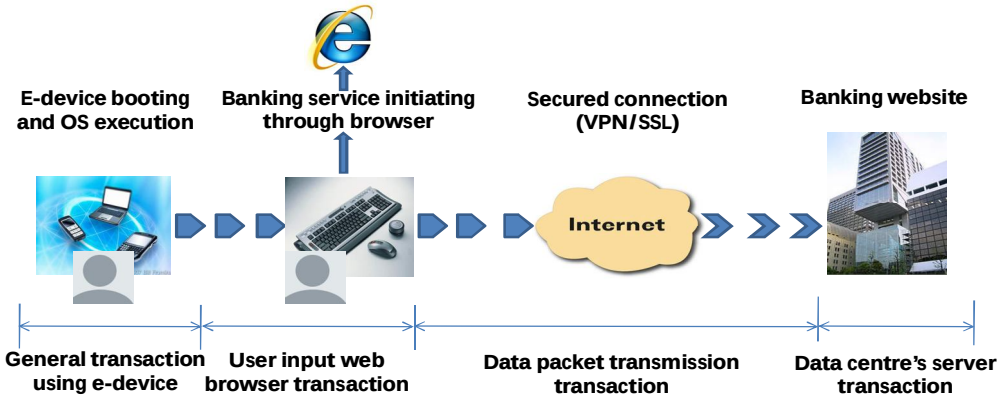
1.4.2 E-banking

The term electronic banking is derived from e-finance. There are two part of e-finance. One is e-banking (i.e. internet banking, telephone banking, other electronic delivery channel etc.) another is other financial services and products (i.e. insurance, online brokering etc.). E-banking addresses banking through internet and the internet banking system refers to the hardware, software,

[14] http://www.techopedia.com/definition/24152/information-and-communications-technology-ict (Accessed on: August 16, 2014).

[15] http://www.techterms.com/definition/ict (Accessed on: December 15, 2013).

networks or inter networks (internet) that make internet banking possible.[16] It is the use of electronic means to deliver banking services, mainly through the internet. The term is also used to refer to ATMs, telephone banking, use of plastic money, mobile phone banking, and electronic funds transfers.[17] E-banking may be understood as term that covers all these ways of banking business electronically.[18] So, financial services delivery by the bank using electronic devices or electronic means is called e-banking service. It is said that financial services delivery using electronic means or devices without internet technology can also be called e-banking (i.e. a distributed system with LAN). But at the advance level, bank carries out e-banking using internet.



E-banking process
Figure- 1.1

1.4.3 E-banker

In this study "e-banker" denotes the commercial banks here in Bangladesh who has been providing services through electronic devices using network or internet.

[16] Frimpong Twum and Kwaku Ahenkora, "Internet Banking Security Strategy: Securing Customer Trust," *Journal of Management and Strategy* 3, no. 4 (September 2012): 79.
[17] Zachary B. Omariba, Nelson B. Masese and G. Wanyembi "Security and privacy of electronic banking," *International Journal of Computer Science Issues (IJCSI)* 9, no. 3 (July 2012): 433.
[18] Md. Mohiuddin, "Trend and Development of E-Banking: A Study on Bangladesh," *IOSR Journal of Business and Management, (IOSR-JBM)* 16, no. 5 (May 2014): 16-24.

1.4.4 IT security threats and vulnerabilities in e-banking

Threat means a possibility of harm or risk which has the possibility of something adverse happening.[19] IT security threat denotes that possible chance to breach computer rules or information security.

In computer security (also known as cyber security or IT security) a threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. It might be denial of service, illegitimate use, disclosure of information, information alteration, and repudiation. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.[20] Threat like session hijacking or cookie hijacking is another serious threat for cyber users. So in banking operation security vulnerabilities and threats both can be explained or exposed in the form of technological, operational and compliance related issues.

According to Charles P. Pfleeger and Shari Lawrence P. Pfleeger, there are four types of security threats to be considered.[21] These are:

i) interception (unauthorized party has gained access to a service or data);

ii) interruption (a file is corrupted of lost);

[19] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, *An Introduction to Computer Security* (USA: National Institute of Standards and Technology Special Publication, 1995), 59.

[20] http://en.wikipedia.org/wiki/Computer_security (Accessed on: December 27, 2013).

[21] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing* (New Jersey: Pearson Education Inc., 2003),414.

iii) modification (unauthorized changing of data or tampering); and

iv) fabrication (additional data or activities are generated that would normally not exist).

The particular local and cyber threats for electronic banking are physical security threats, hardware and network failure/service loss, software defects, unauthorized access or changing, customer data loss, data exposure/loss, access control and human error, malicious attack, virus infection, faulty internet connection, spoofing, phishing, man in the middle attack, social engineering, etc. which cover all of the above categories defined by the security experts.

On the other hand, vulnerability refers to a deficiencies and weaknesses of an entire system. That means vulnerability is a condition of an electronic system which is ready for inviting threats. So, security vulnerability is anything that offers a potential avenue of attack against a system, including things like malware, incorrectly configured systems, passwords written on sticky pads, and so on. It's true that issues like these do increase the risk to a system.[22] So, vulnerabilities mean incorrectly configured systems, faulty internet connection, interception, interruption, weak access control, system without antivirus software, slow response system, lack of legal support, chance of customer's data loss, system ready for attack, non tech-savvy employees and so on.

1.4.5 IT security (e-security)

IT Security (also known as computer security or cyber security) is information security as applied to computers and networks.[23] Here information (data) security means the practice of defending information from unauthorized access, use,

[22] http://technet.microsoft.com/en-us/library/cc751383.aspx (Accessed on: August 16, 2014).
[23] http://en.wikipedia.org/wiki/Information_security (Accessed on: December 27, 2013).

disclosure, disruption, modification, perusal, inspection, recording or destruction. On the other hand, the meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons to:

- prevent theft of or damage to the hardware;
- prevent theft of or damage to the information; and
- prevent disruption of service.[24]

Broadly speaking, electronic security is any tool, technique, or process used to protect a system's information assets. Electronic security enhances or adds value to a naked network and is composed of soft and hard infrastructure. The soft infrastructure components are the policies, processes, protocols, and guidelines that protect the system and the data from compromise. The hard infrastructure consists of hardware and software needed to protect the system and data from threats to security from inside or outside the organization.[25]

So in the e-banking part, e-security system means system secure from all possible vulnerabilities or threats, such as system authorization, authentication, access control, configured network, firewall, VPN and encryption mechanisms, quality internet connections in branch level, error free and timely response system, no communication failure routine backup & restore and disaster recovery service (DRS), legal support and so on which is hooked up with technology, operation and compliance related security issues.

[24] Morrie Gasser, "*Building a secure computer system,"* (New York: Van Nostrand Reinhold, 1988), 3.
[25] The World Bank, *Electronic Security: Risk Mitigation In Financial Transactions* (June, 2002), 4.

1.4.6 Information security risk (IT risk)

In general, risk is a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities.[26] On the other hand, IT risk is loss of service, data loss or theft, processes made unnecessarily complex by systems interfaces and limitations, inaccurate information from redundant or "buggy" and a myriad of the other ills.[27] So in IT related field, risk pooled both security threats and vulnerabilities. So, minimize the IT risk in e-banking operation is a considerable part for bank business. Risk = Assets (information) x Threats x Vulnerabilities[28].

1.4.7 Information (assets) security management

Information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction," according to U.S. law (1). In essence, it means people want to protect their data and systems from those who would seek to misuse it.[29] On the other hand, risk management means coordinated activities to direct and control an organization with regard to risk.[30] In other word, risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.[31]

---

[26] http://www.businessdictionary.com/definition/risk.html (Accessed on: August 4, 2014).

[27] George Westerman and Richard Hunter, *IT Risk, Turning Business Threats into Competitive Advantage* (Boston: Harvard Business School Press, 2007), 2.

[28] Symantec Corporation, *Assets, Threats and Vulnerabilities: Discovery and Analysis, A comprehensive approach to Enterprise Risk Management* (California: Symantec Corporation), 6.

[29] Jason Andress, *The Basics of Information Security, Understanding the fundamentals of InfoSec in Theory and Practice* (New York: John Wiley & Sons, 1998), 2.

[30] BCC, Ministry of ICT, *Information Security Policy Guideline, Bangladesh* (Draft), 11.

[31] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, *An Introduction to Computer Security* (USA: National Institute of Standards and Technology Special Publication, 1995), 59.

Organization nowadays and their IT systems are exposed to ever growing security threats that endanger not only their technological segment, but also their overall business activity. These threats have their sources in many places like computer frauds, industrial espionage, system hack-ins, information leaks, resource withholding, viruses and other malicious codes. Threats can also originate from sources that are not so obvious; like vaguely defined rights of information ownership, non-existent line of responsibility, non-defined incident recognition and response procedures, non-existent change management policy or other security policies.[32] So that complete shielded system should be needed to protect one's valued system (including information and device) and organization from any harm.

Managing the risks and implementing controls for internet banking initiatives follow the same principles as other risk management processes. The most dangerous thing is to consider risk management as a technical problem and leave it to IT management to manage. As the previous enumeration of the risks has shown, risk management in IT is a general management issue which needs particular attention from senior management. A general framework of risk management is set by the Electronic Banking Group of the Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking.[33] In Bangladesh banks basically face seven core risks (i.e. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk.) in which ICT security risk is

[32] http://www.king-ict.com/en/Default.aspx?tabid=615 (Accessed on: January 3, 2014).

[33] Asli Yuksel Mermod, "Customer's Perspectives and Risk Issues on E-Banking in Turkey; Should We Still be Online?," *Journal of Internet Banking and Commerce* 16, no.1 (April, 2011)

vital and have linked with other six risks. On the other hand, e-bankers maintain all of its information (assets) in electronic form in its own database and risks are arise from storage information. So, eventually all risks are related with information assets in database. So, it can easily be mitigated by information security risk management process to an acceptable level.

1.4.8 Commercial banks

A commercial bank is a type of bank that provides services, such as accepting deposits, giving business loans and basic investment products.[34] But today's bank provides different sort of services like agency arrangement, ancillary services and e-banking services such as core banking, cluster banking, any branch banking, doorstep banking, ATM, EFT mobile banking, etc. It is said that all these functions are rendered today through the help of information and communication technology. E-banking process used alternative distribution channel to provide above banking services to the customer. It is an e-trend paradigm using most advance technology for the CBs here in Bangladesh.

1.4.9 Bank Customer

For a bank, a customer is a person who is utilizing one or more of the services provided by the bank. A customer is a person through whom the bank gets an opportunity to make an earning in return to the service it can provide the customer with. For instance, an individual who has a checking account with a bank or an individual who has a mortgage or a loan with the bank or an individual who has a deposit with the bank are all customers of the bank.[35]

[34] http://en.wikipedia.org/wiki/Commercial_bank (Accessed on: January 4, 2014).

[35] http://www.answers.com/Q/Who_is_a_customer_as_per_bank_definition (Accessed on: February 10, 2015).

So, a customer is a person or organization (entity) that is using any or all of the services offered by the bank. The task could be anything like:

- holding accounts;
- depositing cash in the bank;
- taken a loan from the bank;
- withdrawing cash or transfer fund;
- taking electronic banking services (i.e. EFT, ATM, MFS, etc.)

So, different types of depositors and borrowers are the main customer of bank. Depositor is an individual or company (entity) that places money in bank. On the other hand, "Borrower" means any person to whom any credit limit has been sanctioned by any banking company."36 So, borrower is an individual or company (entity) that takes money from bank. This study prefers regular bank depositors and borrowers that involve in financial transaction with bank for long time.

1.5 Delimitation and Gap of the study

As a background of the research topic "E-banking in Bangladesh: Vulnerabilities and Securities" generally represent all those issues which influence Bangladeshi CBs to adopt automation to minimize business costs and provide quick or quality services to satisfy customers and the security issues relate to the customers as well as CBs, but because of limited time frame of the research, researcher attempts to narrow down the study. So, the study has focused mainly on the "Security vulnerabilities of e-banking" which is associated with bank's core risks, customer satisfaction and bank's e-security management perspective rather than other related issues.

[36] Article 42 (b), Bangladesh Bank Order, 1972

Researcher believes that the result of the research can be generalized with all other related issues simultaneously for CB's and their valued customers.

After reviewed a number of literature on this particular issue, researcher found that e-security measures taken by the CBs in different countries focused frequently on customer's satisfaction issue rather than e-banking system vulnerability, risks or e-security management issue of CBs which is closely related with bank business as well as other stakeholder's interest. This is the research gap and that's why researcher is going to study further the security vulnerabilities issue from CBs risk mitigation point of view which can simultaneously minimize risk both for banks and customers.

1.6 Justification of the Study

It is obvious that information systems and technologies significantly influence business processes in the banking industry. The information system or information technology both represents as an important factor for banks' competitiveness and commercial success. Information system or information technology both affects e-banking as equally as the banking business and customer's interest. But to ensure the success of the bank, information systems and technologies both should be secured because loss of information means loss of customer satisfaction, loss of reputation, loss of return and finally loss of bank business. Today, information security management and vulnerabilities management both are vital issues for CBs. Whereas recent trend of local and cyber heist in the banking industry categorically emphasized on conducting this particular study. Considering these factors, the research is planned and this is very much important for banks' policy makers and other stakeholders. However, recently some special type of difficulties

regarding e-banking vulnerabilities and securities in branch level have seriously occurred which usually affect e-banking operation and raised different questions. The organization like bank cannot run properly and effectively without taking necessary security measures to minimize the core risks. That's why the study is very much rationale on this particular ground.

1.7 Utility of the Study

Some category of stakeholders will hopefully be benefited from the findings of this particular research work. These are the as follows:

i) Financial service industry:

The study could profoundly be helpful for the members of the financial service industry like banks, financial institutions, etc. The study has provided major security solutions for this particular sector.

ii) Regulatory authority:

As a regulatory authority Bangladesh Bank could be benefited from findings of the study.

iii) Bank customers and Investors:

Customers will be safe and secured from major vulnerabilities regarding their transactions, information and other bank related matters. On the other hand, investors could be secured in terms of their investment. Save investment and financial transaction for both parties can be ensured by the findings of research.

iv) Concern officials and policy makers:

The study may help the concern bank personnel and e-banking policy makers to take proper measures and development of e-security.

v) Academicians, scholars and researchers:

The research work could also be a good reference for future researchers, scholars as well as academicians regarding vulnerabilities and security of e-banking.

1.8 Research Hypothesis

E-banking security (e-security) system and all possible e-banking vulnerabilities are the major variables for this research. After detailed review of related studies, the below hypothesis are formulated for testing:

H1: E-security system has significant impact on e-banking vulnerabilities.

H2: There is a positive correlation between e-security system and vulnerabilities.

H3: Bankers' commercial success significantly depends on e-security system.

H4: Relationship between e-security system and bank core risks are significant.

H5: There is a positive correlation between e-security system and customer satisfaction.

1.9 The Layout of Dissertation

This particular chapter, section and sub-sections of the study are expected to contain the following elements:

[42] Uma Sekaran, "*Research Methods for Business, A Skill Building Approach*," (New Delhi: Shakti Packers, 2009),18.

Chapter 1: Introduction

Background of the Study

Problem Statement and Research Question

Aims and objectives of the Study

Definition of key terms

Delimitation and Gap of the study

Justification of the Study

Utility of the Study

Research Hypothesis

The Layout of Dissertation

Ethical Consideration

Chapter 2: Literature Review

E-banking Vulnerabilities

E-banking Securities

E- Banking and Risk Management

E-banking and Customer Satisfaction

E-banking and Banks' Commercial Success

Chapter 3: Research Approach

Methodology

Data and Collection Techniques

Study Area

Study Population

Sample size and Sampling method

Questionnaire Design

Adequacy of laws and regulations in Bangladesh

Conclusion

Chapter 6: Data Analysis, Interpretation and Findings

Frequency Tables

Frequency Tables for SBL

Frequency Tables for DBBL

Testing of Hypothesis

Findings of the study

Chapter 7: Summary, Recommendations and Conclusion

Summary

Recommendations

Final Remarks

Suggestions for further research

Appendices

Bibliography

1.10 Ethical Consideration

Ethical guidelines and principles for conducting research with human participants (and non-human ones as well) are clearly needed. Risks of harm of participants (respondents), privacy and confidentiality, anonymity and other related principles rigorously maintain by the researcher. The researcher has followed 'the code of conduct or expected norms of behavior while conducting the research.'[42] On the contrary, plagiarism, fabrication and falsification, no publication of data, faulty data has been avoided in this study. However all ethical standards were considered by the researcher during conducting this particular study.

Chapter II
Literature Review

Introduction

A review of the literature is an essential part of any academic research. In research, literature review is a collection of published information (data) relevant to a research question. There are a few numbers of literatures available regarding electronic banking vulnerabilities and security measures. Some are theoretical and some other empirical. Both findings, in the subject matter of the research e-banking vulnerabilities and securities were reviewed in order to find out research gap and, to follow effective method and design particular models for this study. It is worth noting that some important affluence relating to e-banking service vulnerabilities and securities were studied and reviewed meticulously to enrich the research work for the present context.

The topic is very burning issue for the CBs here in Bangladesh. Because, the recent trends of digitization with insufficient security has fallen CBs a great risk. Although very few surveys have been conducted on this particular subject. Yet no complete research on this topic has been seen in Bangladesh. Even there are no much articles, journals or books on this particular subject here. There are some books, journals, research papers written by foreign writers or experts and very few articles on news daily written by local experts. Furthermore major publications or guideline by the banks (both central and commercial banks) are also developed security risk management process for e-banking. All these materials helped to conduct the study easier. Some major books, journals, research papers, articles, organizational publications, electronic form and articles news daily that have been reviewed which are as follows:

2.1 E-banking Vulnerabilities

2.1.1 Peotta Laerte, et al.[43] focused on electronic attacks and vulnerabilities associated by internet banking. The author designed an attack tree model for common attacks against online banking systems. This model represents the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (engineering social and phishing) then to gain control of device (malware) and credential theft of legitimate user (fake Web pages and malware).

2.1.2 Brar, Sharma, and Khurmi[44] basically depicted on the nature of frauds and other cyber criminal activities through ICT in Indian banking sector. The increase in the use of ICT facilities result in increase of criminal activities like spamming, credit card frauds, ATM frauds, Phishing, identity theft, denial of service and most of others has lend credence to the view that ICT is contributing crime in banking sector. The challenges that oppose electronic banking are the concerns of security and privacy of information. This paper aims at investigating various risks and whether these risks can be totally eradicated or not. Based on the findings this study, the paper concludes that with the help of various tools total eradication of risks is not possible but can be highly reduced if internal control measure techniques are adequately put in place.

[43] Laerte Peotta, et al. "A formal classification of internet banking attacks and vulnerabilities," *International Journal of Computer Science & Information Technology* 3, no. 1 (Feb 2011): 186.

[44] Tejinder Pal Singh Brar, Dr. Dhiraj Sharma and Dr. Sawtantar Singh Khurmi, "Vulnerabilities in e-banking: A study of various security aspects in e-banking," *International Journal of Computing & Business Research* (2012): 2229-6166.

2.1.3 Singh N. P. [45] analyzed the reasons for increase in fishing activities, types of phishing techniques, and process of phishing. Further author has presented recent cases of phishing specifically in banking or financial sector. Towards the end it author has studied the measures to combat the fishing in online banking.

2.1.4 Espelid Yngve, et al.[46] emphasized on man-in-the-middle vulnerability (MitM) in online banking applications using Bank ID.

2.1.5 Jassal, and Sehgal[47] mainly illustrated online banking security flaws. Billions of financial data transactions occur online every day and bank cyber crimes take place every day when bank information is compromised by skilled criminal hackers by manipulating a financial institutions online information system. This cause huge financial loses to the banks and customers.

2.1.6 Klingsheim, et al.[48] described a man-in-the-middle vulnerability in online banking applications using BankID. Authors outlined the details of the flawed BankID authentication protocol and the MitM attack. An exploit has been implemented and successfully run against two randomly chosen online banking systems to demonstrate the seriousness of the attack. BankID is Norwegian customized software developed for conducting commerce on the Internet. BankID relies on two-factor authentication with One-Time Passwords (OTPs).

---

[45] N. P. Singh, "Online Frauds in Banks with Phishing," *Journal of Internet Banking and Commerce* 12, no.2 (2007): 1.

[46] Espelid, Y., et al., 2008, in IFIP International Federation for Information Processing, Volume 278; Proceedings of the IFIP TC 11 23rd International Information Security Conference; Sushil Jajodia, Pierangela Samarati, Stelvio Cimato; (Boston: Springer): 63–77.

[47] Rajpreet Kaur Jassal and Ravinder Kumar Sehgal, *"Online Banking Security Flaws: A Study," International Journal of Advanced Research in Computer Science and Software Engineering* 3, no.8 (2013): 1017-1020.

[48] Andre N. Klingsheim, et al. "Robbing Banks with Their Own Software—an Exploit against Norwegian Online Banks," *Risks in Networked Computer Systems,* paper IV (2008): 49.

2.1.7 Jassal, and Sehgal[49] mostly described different sorts of vulnerabilities and security threats and the online banking security system of various Indian banks such as Oriental Bank of Commerce (OBC), ICICI Bank, HSBC Bank. Bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system, spreading malicious bank Trojan viruses, corrupt data, and impedes the quality of an information system's performance. So at present customers can do banking online which is easy and time saving and at the same time they are vulnerable to threats. So one of the major concerns of people with respect to internet banking is the safety related to data of bank account, transactional information and also the access path of their accounts.

2.2 E-banking Securities

2.2.1 French[50] concentrated on types of vulnerabilities and security threats faced by the commercial organizations. All commercial operating systems have vulnerabilities, also known as weaknesses in the computer system. These vulnerabilities create opportunities for possible threats to the information housed on these systems. Security threats can be classified into several categories from internal to external, human or non-human, and intentional or non-intentional. These threats can lead to the possibilities of disclosure, modification, destruction, or denial of use of that information. There are various threats to information security that protectors of information must be aware of and account for. On the other hand author focused on security measures. He said that organizations must

[49] Rajpreet Kaur Jassal and Dr. Ravinder Kumar Sehgal, "Comparitive Study of Online Banking Security System of various Banks in India*," International Association of Scientific Innovation and Research* 6, no.1 (2013): 90.

[50] Aaron M. French, "Case Study on E-Banking Security – When security becomes too sophisticated for the user to access their information, *"Journal of Internet Banking and Commerce 17, no.2 (2012):1-6.*

take preventative measures to protect their sensitive corporate information. This includes information about the company's strategy, financial information, customer information, or any other information that could be damaging to the company and its reputation. It was reported that information security management is currently the top technology initiative among organizations and has been since 2002. As discussed earlier, security threats can be internal or external, human or non-human, accidental or intentional operationalized security into five aspects: Security Policy, Host Security, Network Security, Organizational Security and Legal Security.

2.2.2 Hole, Moen, and Tjostheim[51] suggested the management of banks in Norway typically has little understating of real security and tends to assume a system is secure if all information about it is kept secure. They reported all banks employees have to sign nondisclosure agreements, which preventing them discussing any security problems with anyone outside their systems. The authors made this claim based on the banks' reaction when the authors tried to inform the selected banks about their findings. The authors believed that the banks' security-by-obscurity policy led to a false feeling of security instead of real security, making the systems vulnerable to 7 / 14 rather trivial attacks during 2003 and 2004. The authors claimed this policy is actually against real security.

2.2.3 Koskosas I[52] focused on the communication of security risk messages among organizations and particularly on communication between IT employees and managers within a bank in Greece. An important aspect of any information systems

[51] Hole, Moen, and Tjostheim, "An Analysis of the Online Banking Security Issues," *Department of Computer Science, University of Auckland, Australia*

[52] Ioannis Koskosas, "E-banking security: A communication Perspective," *Palgrave journal* 13, no.2 (2011): 81–99.

(IS) security activity is about ensuring the security of its infrastructure, and in doing so, communication is a key necessity for present e-banking security managers.

2.2.4 Malam, Zainol and Nelson[53] basically represented on the relation between weak internal control system and security threats of computerized branch. Internal control system is an important pillar in an organization. Considering the evidence from major accounting fraud cases that occurred consequence to weak internal control, such as Enron, it could also occur in a financial institution. Hence, the objective of this study is to investigate the bank managers' opinion on the likelihood of security threats in the computerized banking systems (CBS) in Malaysia. Since most major financial institutions operate in the capital city of Kuala Lumpur, questionnaires were sent to selected bank branches in Kuala Lumpur. The findings are expected to provide a platform for bank managers to share their threats' experience. Secondly, to assist them in designing and formulating a sound and effective internal control system that will provide reasonable assurance for achieving the bank's mission. Findings are also expected to provide general insights of internal control system, as most information is very remote and confidential, thus generate a platform for promoting an efficient and effective internal control practice in financial institutions.

2.2.5 Hertzum M., et al.[54] suggested electronic banking must be secure and easy to use. An evaluation of six Danish web-based electronic banking systems indicates that the systems have serious weaknesses with respect to ease of use.

[53] Abu Bakar Malam, Zaini Zainol and Sherliza Puat Nelson, "Security threats of compterized banking systems (CBS): The managers' perception in Malaysia," *International Journal of Economics and Finance Studies* 4, no. 1 (2012): 21.

[54] Morten Hertzum, et al. "Usable security and e-Banking: Ease of use vis-a-vis security," *Australasian Journal of Information Systems* 11, no. 2 (2004): 52-65.

Analysis of the weaknesses suggests that security requirements are among their causes and that the weaknesses may in turn cause decreased security. Conceptually viewing the conflict between ease of use and security in the context of usable security, intended to match security principles and demands against user knowledge and motivation. Automation, instruction, and understanding can be identified as different approaches to usable security. Instruction is the main approach of the systems evaluated; automation relieves the user from involvement in security, as far as possible; and understanding goes beyond step-by-step instructions, to enable users to act competently and safely in situations that transcend preconceived instructions. The article discussed the pros and cons of automation and understanding as alternative approaches to the design of web based e-banking systems.

2.2.6 Kasemsan and Hunhgam[55] purposed the internet banking security guideline model for banking business in Thailand. At the present, the uses of the Internet have grown rapidly, but there are not many customers who use the Internet banking services because they do not trust the bank security systems. As a result, the study of the Internet banking security guideline model and tools development as well as information technology were conducted to ensure the security of the Internet banking services by using the concept of reliability, innovation adoption theory, the quality of the Internet connection and e-commerce law. The collected data were taken to form the Internet banking services security model by using innovation adoption theory, trust of the system, the quality of the Internet connection, e-commerce legal support, authentication theory, key locker security, and one time password (OTP).

[55] M. L. Kulthon Kasemsan and Nantana Hunhgam, "Internet Banking Security Guideline Model for Banking in Thailand," *IBIMA Publishing* 2011, no. 2010 (2011):13.

2.2.7 Sheikh and Rajmohan[56] basically focused on weakness of internet banking is based on analysis of current security models. Internet banking services must be more responsive towards security requirements. There is no doubt that Internet banking transaction have protection against security threats, the providers of internet banking should approach security considerations as part of their service offerings. Internet banking fraud is an issue being faced globally and is continuing to prove costly to both banks and customers. Frauds in Internet banking occur as a result of compromises in security ranging from weak authentication systems to insufficient internal controls.

2.3 E- Banking and Risk Management

2.3.1 Sarma and Singh[57] focused on risks associated by bank and applicability of biometric technology for authentication. Internet banking creates new risk control challenges for national banks of India. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital. Effective management of a banking regular activity requires that bank authority have understood and control the bank's risk culture. Therefore, in this paper firstly writer is going to analyze the various types of risks faced by Internet Banking. The following are the various types of risks associated with Internet Banking. These are credit risk, foreign exchange risk, compliance risk, strategic risks, reputation risk, transaction risk etc.

[56] Bilal Ahmad Sheikh and P. Rajmohan, "Interne Banking, Security Models and Weakness." *International Journal of Research in Management & Business studies* 2, Issue 4 (October-December 2015):17.

[57] Gunajit Sarma and Pranav Kumar Singh, "Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication," *International Journal of Pure and Applied Sciences and Technology* 1, no. 2 (2010): 69-70.

2.3.2 Ndlovu and Sigola[58] revealed that the adoption of e-banking requires the incorporation of sound risk management principles for it to be effective. Each financial institution should apply guidelines based on its scope and level of sophistication. Typically, electronic banking amplifies the scale of exposure of banks to traditional risks, such as transaction, strategic, reputational, and compliance risks, among others. Therefore, banks should ensure that there are adequate policies and procedures relating to risk management which involve an element of a segregation of duties; an effective security program has been implemented with appropriate communication on policy, procedures, and practices, with the necessary support from the bank's directorate.

2.3.3 Solanki[59] concentrated on e-banking risks such as operational risks, money laundering, cross borders, firewalls, customer education, auditing etc. The author mentioned that the risks involves in e-banking are operational risk security risk, system architecture & design risk, market risk, business risk, reputational risk, legal risks, money laundering risk, strategic risk and other risk. Having made an assessment of risks and its risk tolerance, bank management should take steps to manage and control risks. This phase of a risk management process includes activities such as implementing security policies and measures, co-coordinating internal communication, evaluating and upgrading products and services, implementing measures to ensure that outsourcing risks are controlled and managed, providing disclosures and customer education, and developing contingency plans. Senior management should ensure that staffs responsible for

[58] Ian Ndlovu and Mlungisi Sigola "Benefits and Risks of E-Banking: Case of Commercial Banking In Zimbabwe," *The International Journal Of Engineering And Science* 2, Issue. 4 (2013): 34-40.

[59] Virender Sing Solanki, "Risk in e-banking and their management," *International Journal of Marketing, Financial Services & Management Research* 1, no. 9 (September 2012): 164.

enforcing risk limits have authority independent from the business unit undertaking the electronic banking or electronic money activity. Banks increase their ability to control and manage the various risks inherent in any activity when policies.

2.3.4 Abdou, English and Adewunmi[60] focused on investigating of risk management practices in e-banking of major UK banks, using the framework of principles introduced by the Basel Committee on Banking Supervision (BCBS). Research results also confirm that UK banks are complying with the 14 BCBS risk principles and are well managed in terms of their security controls for e-banking.

2.3.5 Akbari P[61] illustrated on operational e-banking risks. Technological innovation by e-banking systems has brought about many benefits to customers while it has been accompanied by a number of risks including the operational ones. This risks need to be identified and managed by the Banks. This particular research identified, compared, and ranked factors affecting operational e-banking risks in viewpoints of customers and employees of Kermanshah Melli bank in Iran.

2.3.6 Koskosas I[62] this research article focused on the communication of security risk messages among organizations and particularly on communication between IT employees and managers within a bank in Greece. An important aspect of any information systems security activity is about ensuring the security of its infrastructure, and in doing so, communication is a key necessity for present e-

[60] Hussein A. Abdou, John English and Paul O. Adewunmi, "An investigation of risk management practices in electronic banking: the case of the UK banks," *Banks and Bank Systems* 9, Issue 3 (2014).

[61] P. Akbari, "A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry: Case Study: Kermanshah Melli Bank*," International Journal of Management and Business Research* 2, no. 2 (2012): 123-135.

[62] Ioannis Koskosas, "E-banking security: A communication perspective," *Risk Management 13. no.1 (2011):81–99.*

banking security managers. A new communication practices is able to reduce hole between IT professionals and non-IT managers. The issues of communication found to play an important role in e-banking security included: organizational flexibility, availability of resources, e-banking project alignment, support from top management, information transparency and security knowledge and awareness.

2.4 E-banking and Customer Satisfaction

2.4.1 Haque, et al.[63] described that only protected transaction, have significant impact on consumers' perception about e-banking security, followed by service quality and regulatory frame work issues. The research result showed that the consumers' attention towards the trust and confidence on the e-banking security system is the significant element.

2.4.2 Ibok, Nkanikpo and Ikoh[64] basically proposed a model of customer satisfaction and its determinants on internet banking. Major determinants are access of account, account control, use of account, costs time effectiveness, ease of use and privacy and security. This study basically attempted to identify factors that determine customers' satisfaction with internet banking within the Nigerian banking context.

2.4.3 Sakhaei, Afshari and Esmaili[65] presented a study to investigate service quality indexes in Internet banking. Six service quality dimensions namely reliability, efficiency, responsiveness, fulfillment, security/privacy and website

[63] Ahasanul Haque and et al. "Electronic transaction of internet banking and its perception of Malaysian online customers," *African Journal of Business Management* 3, no. 6 (June 2009): 248-259.

[64] Ibok, Nkanikpo Ibok and Itoro Moses Ikoh, "Determinants of Customers Satisfaction with Internet Banking Services," *British Journal of Arts and Social Sciences* 14, no. 2 (July 2013):178.

[65] S. Fatemeh Sakhaei, Ahmad J. Afshari and Ezzatollah Esmaili, "The Impact of Service Quality on Customer Satisfaction in Internet Banking," *Journal of mathematics and computer science* 9, no.4 (2014): 33-40.

design have been established. This paper evaluated influence of service quality on customer satisfaction in Internet banking. The study showed that the six service quality dimensions have meaningful relationship with customer satisfaction in Internet Banking. The purpose of this research paper is to understand the impact of service quality factors of Internet banking on customer satisfaction in Iran.

2.4.4 Kaur and Kaur[66] the main objectives of this empirical study have been to determine the bank-wise comparison among the customers usage of internet banking services by using one-way ANOVA and to evaluate consequent impact of the Internet banking service quality on the customer satisfaction through multiple-regression statistical techniques. ANOVA results have depicted that there is no significant difference in facilities determining the customers' usage of internet banking services of Public-sector, Private-sector and Foreign Banks in India. The regression measures have indicated that responsiveness, security/privacy and site-aesthetic are influential factors, whereas, reliability and efficiency have insignificant impact on satisfaction of the online customers.

2.4.5 Nupur[67] tried to explore the relationship between service quality and the customer satisfaction. The study showed that these factors are the core service quality dimensions for customer satisfaction in e-banking. The study also explored that reliability, responsiveness and assurance have more contribution to satisfy the customers of e-banking in Bangladesh.

[66] Jasveen Kaur and Baljit Kaur, "Determining Internet Banking Service Quality & Customer Satisfaction in India," Bangalore. India, AIMS International Conference on Management, Jan. 2013. Web. 15 Jan. 2016.

[67] Jannatul Mawa Nupur, "E-Banking and customers' satisfaction in Bangladesh: An analysis," *International Review of Business Research Papers* 6, no. 4 (September 2010):145 – 156.

2.4.6 John and Rotimi[68] the study found that there is a significant relationship between electronic banking and customers' satisfaction. Also that e-banking has become popular because of its convenience and flexibility, and transaction related benefits like speed, efficiency and accessibility. Although these are fraught with insecurity and most importantly power challenges. The paper suggested that critical infrastructure like power; security and telecommunication should be strengthened to ensure the application of electronic banking in Nigeria and optimum satisfaction on the part of customers.

2.5 E-banking and Banks' Commercial Success

2.5.1 Wu, Hsia and Heng[69] focused on the impact of e-banking on the incumbent banks. However, to successfully cope with the challenge of the e-banking innovation, the incumbent banks must understand the nature of the change and capability barriers that it presents [Southard and Siau 2004]. Without this understanding, attempts to migrate to e-banking may be doomed to failure.

2.5.2 Manzoor, Umra and Abbas[70] highlighted substantial influence of e-banking on bank's performance. The aim of this paper is to examine the impact of e-banking on the profitability of Pakistani banks, in particular. The results showed that e-banking has increased the profitability of banks; it has enabled the banks to meet their costs and earn profits even in the short span of time.

[68] Ogunlowore Akindele John and Oladele Rotimi, "Analysis of electronic banking and customer satisfaction in Nigeria," *European Journal of Business and Social Sciences* 3, no.3 (June 2014):14-27.

[69] Jen-Her Wu, Tzyh-Li Hsia and Michael S H Heng, "Core Capabilities for Exploiting Electronic Banking," *Journal of Electronic Commerce Research*, 7, no.2 (2006):111.

[70] Mohammad Khurram Manzoor, Hassan H. Sumra and Momina Abbas, "The Impact of E-Banking on the Profitability of Banks: A Study of Pakistani Banks," *Journal of Public Administration and Governance* 1, No. 1 (2011): 32-38.

2.5.3 Kujur and Shah[71] presented impact of e-banking on banks' return. The introduction of e-banking in banking sector is to bring customer satisfaction, there by enhance the banks' profitability. E-banking is flapping with banking services. It provides enormous benefits to consumers in terms of the ease, simplicity and cost of transactions. It can improve banks' efficiency and competitiveness, so existing and potential customers can benefit from a greater degree of convenience in effecting transactions. But it also poses new challenges to banking entities and authorities in regulating and supervising the financial system and in designing and implementing macroeconomic policy. The online banking is a demand of today's customers, but the adaption of e-banking by CBs increases security and different types of risks. The increasing popularity of e-banking has attracted the attention of both lawful/legitimate and unlawful/legitimate banking practices, thereby, exposing customers to fraud, thefts and various other threats of similar nature. The impact of e-banking on the banking performance, to know the various risks and security challenges in e-banking that help bankers to understand the risk and security aspect of various e-banking services where customers have high level of concern.

2.5.4 Oyewole, et al.[72] consequently focused on the impact of electronic banking on banks' performance in Nigeria. The study comprised annual audited financial statements of eight banks that have adopted e-banking and retained their brand name banking between 2000 and 2010 as well as macroeconomic

[71] Teju Kujur and Mushtaq Ahmad Shah, "Electronic banking: Impact, Risk and security Issues," International Journal of Engineering and Management Research 5, Issue 5 (October 2015): 207-212.

[72] Oginni Simon Oyewole et al. "E-banking and Bank Performance: Evidence from Nigeria," *International Journal of Scientific Engineering and Technology* 2, Issue.8 (Aug. 2013): 766-771.

control variables were employed to investigate the impact of e-banking on return on asset (ROA), return on equity (ROE) and net interest margin (NIM). Result from pooled OLS estimations indicated that e-banking begins to contribute positively to bank performance in terms of ROA and NIM with a time lag of two years while a negative impact was observed in the first year of adoption. It was recommended that investment decision on electronic banking should be rational so as to justify cost and revenue implications on bank performance.

2.5.5 Ngango, et al.[73] Electronic banking system like ATM, Pay direct, electronic check conversion, mobile telephone banking and e-transact has a great impact on bank performance because they increase profitability, reduce bank cost of operations, and increase bank asset and bank efficiency.

Conclusion

The chapter basically represents different sorts of vulnerabilities and securities faced by e-banker in different countries around the world as well as the effective techniques or models for information security risk management are developed by scholars, which has also been fulfilling this research purpose.

[73] Asia Ngango, et al. "E-banking and performance of commercial banks in Rwanda: A case of bank of Kigali," *European Journal of Accounting Auditing and Finance Research*. 3, no.4 (April 2015): 25-57.

Chapter III
Research Approach

Introduction

This chapter talks over in detail the research methodology that has been espoused in this study on E-banking in Bangladesh: Vulnerabilities and Securities. The method that has been embraced in this study was so prudently planned as to go well with the area of inquiry. The area of study is CBs of Bangladesh where banker's and customer's cooperation and information were important to the researcher.

The respondent's valuable participation has been very much useful to the study to arrive at the findings that have exposed existing e-banking security vulnerabilities. Hence, basic statistical and advanced analytical tools have been employed to evaluate e-security flaws of CBs here in Bangladesh. The literature reviews have supported the researcher to emphasis on the type of research method that is most suitable for this area of study.

3.1 Methodology

Research methodology is an approach to conduct the study into research destination. Natures of research, data collection techniques, data analyze techniques, interpretation are designed in this section. In this study, both qualitative and quantitative data have been used to make it comprehensive. It is an evaluation research under applied social science research using survey method techniques. Because, the study evaluated the present existing information security vulnerabilities status maintained by e-bankers. Information

was generated through the techniques of personal interview, structured questionnaire, participant observation, in-depth or group interview. The study has been verified with the help of descriptive and inferential statistics.

For the most part, these methods consist of the following elements; perform more or less, in the following order.

i) assess the vulnerability of critical assets to specific threats;
ii) determine the risks (i.e. the expected likelihood and consequences of specific types of attacks on specific assets);
iii) identify ways to reduce those risks; and
iv) prioritize risk reduction measures based on a strategy.

Collecting data sources for this study are classified in the following ways:

(a) Primary data source

(b) Secondary data source

3.1.1 Data Collection Techniques

(A) Primary Sources of Data:

There are several methods of collecting primary data particularly in surveys. Important ones are: (i) observation method, (ii) interview method, (iii) through questionnaires. Data were collected from primary source using the following methods:

Methods used by the study to collect the required primary data:

In-depth Interview or Group Interview	119
Participants Observation	05
Free story interview	02
Grand Total	**126**

Figure-3.1

(i) Observation Method:

The observation method is the most commonly used method. Under the observation method, the information is sought by way of investigator's own direct observation without asking from the respondent. The study observed all sorts of vulnerabilities and the security related activities of the bank and collected required information from the sample banks.

(ii) Interview Method:

The interview is a face to face interpersonal situation in which one person, the interviewer, asks a person being interviewed, the respondent, question designed to obtain answer pertinent to research problems. In order to have the required information the researcher met the respondents. IT professionals, experts, faculties, related officials and branch customers were interviewed to collect required data.

(Area wise In-depth or Group Interview)

Stratum	Institute and Organ.	No. of Respondents (Purposive sampling)	Total
Sonali bank Ltd. (Strata -01)	Head office (IT Division and Risk Management Division) Controlling office (Dhaka, Rajshahi and Chittagong) Branch level (Dhaka, Rajshahi and Chittagong) Sonali Bank Staff College & Training Institute (Dhaka and Rajshahi)	Top executives & IT professionals of head office (2×3)=6 3 Controlling office from 3 division, 3 from each (3×3) = 9 Branch level officers, 3 branches from each division (9×2)=18 Branch level customers (9×5)=45 (Out of 5 customers depositor 2 and borrower 3) Principal, Chief Instructor (2×1)=2 Senior Faculties (2×2)=4	84
Dutch-Bangla Bank Ltd. (Strata -02)	Head office (IT Division and IC & CD or Vigilance division) Branch level (Dhaka, Rajshahi, and Chittagong)	Top executives & IT professionals of head office level (2×3)=6 Branch level officers (3×2)=6 Branch level customers (3×5)=15 (Out of 5 customers depositor 2 and borrower 3)	27
Bangladesh Bank (Strata -03)	Head office, Dhaka (Research & IT Dept.)	Top executives & IT Officers (2×2)	04
Ministry of ICT (Strata -04)	Secretariat, Dhaka	High official & IT professionals (2×2)	04
Total			**119**

Figure-3.2

(iii) Questionnaire Method:

This method of data collection is quite popular, particularly in case of big enquiries. A questionnaire consists of a number of questions printed or typed in a definite order on a form or set of forms. The study made different sets of questionnaire for different categories of respondents. Both free response or open end and closed end questions with short replies were developed after in depth study of literature and other materials of the research for applicable respondents.

Questionnaires were sent by post to the concerned persons with a request to answer the questions and return the questionnaire.

Three different questionnaire sets were prepared for different sections of respondents.

Questionnaire set

Sonali bank Ltd. (Strata -01)	01
Dutch-Bangla Bank Ltd. (Strata -02)	01
Bangladesh Bank (Strata -03)	01
Total	**03**

Figure- 3.3

(B) Secondary Sources of Data:

Secondary data means data that are already available i.e., they refer to the data which have already been collected and analyzed by someone else. Secondary data may either be published data or unpublished data. The study collected required secondary data from the following sources:

(i) various publications of the governments;

(ii) various publications of foreign governments or of international bodies and their subsidiary organizations;

(iii) technical and trade journals;

(iv) books, magazines and newspapers;

(v) reports and publications of various associations connected with business and industry, banks, stock exchanges, etc.;

(vi) reports prepared by research scholars, universities, economists, etc. in different fields; and

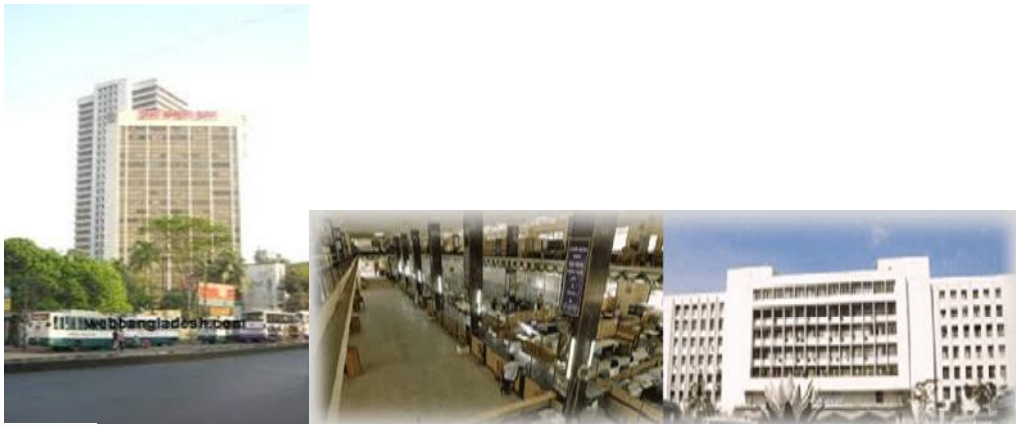
(vii) public records and statistics, historical documents, and other sources of published information.

3.1.2 Study Area

Every research has to be limited in its theoretical and geographical area. A limited area is helpful in intensive study of the research problem. The theoretical area of the study is limited to vulnerabilities of e-banking securities of commercial banks in Bangladesh and its impact on bank's core risk, commercial success and customer satisfaction. The geographical area of the study was three big divisions i.e., Dhaka, Chittagong and Rajshahi. Judgment and convenience guided the choice of geographic scope.

3.1.3 Study Population

The term 'population' refers to the total of items about which information is desired for the study. Population of this study was all the CBs operating in Bangladesh which have been introduced e-banking services. For study purpose, the study comprised of IT professionals, experts, faculties, related officials and branch customers of selected public and private sector banks.



Dutch-Bangla Bank Ltd.
(Head office)
195, Sena kalyan bhaban
(4th Floor),
Motijheel C/A, Dhaka,
Bangladesh.

Sonali Bank Ltd.
(Head office)
35-42, 44 Motijheel C/A, Dhaka ,
Bangladesh.

Figure- 3.4

To make the study more informative additional two related institutions or organs have been included here. Professionals of central bank and the Ministry of Information & Communication Technology of Bangladesh were also included to interview. To making the study effective and more useful, the entire research population was divided into different stratum or strata.

3.1.4 Sample size and Sampling method

Sampling it is the process of obtaining information about an entire population by examining only a part of it. The researcher selected only a few items from the universe for his study purposes. All this is done on the assumption that the sample data will enable him to estimate the population parameters. According to Bangladesh bank, there are 52 commercial banks currently operating their activities in Bangladesh. This is a huge sector. However, due to limited access to data and resources, the study followed purposive sampling technique. It is worth noting that purposive sampling, also known as judgmental**,** selective or expert

opinion sampling is a type of non-probability sampling technique**.** Non-probability sampling focuses on sampling techniques where the units that are investigated are based on the judgment of the researcher. A core characteristic of non-probability sampling techniques is that samples are selected based on the subjective judgment of the researcher, rather than random selection (i.e. probabilistic methods).[74]

By nature the major e-banking vulnerabilities and security of Commercial Banks are almost similar. But because of the accessibility, availability and reliability of data two banks, one each from public and private sector in three divisions were selected. Therefore, the study purposively selected IT professionals, experts, faculties, related officials and branch customers of Sonali Bank Limited and Dutch-Bangla Bank Ltd.

The Sonali Bank Limited is a state owned largest public sector commercial bank operating with 1207 local and foreign branches. The Dutch-Bangla Bank Ltd., on the other hand, is a private sector joint venture commercial bank and a pioneer e-banker in Bangladesh operating with 155 branches with full automation took place in 2003 and e-banking division was established in 2002[75].

Two other related institutions and organs were also purposively selected (i.e. central bank and the Ministry of Information & Communication Technology of Bangladesh) by the researcher. Hope, the selected sample presented whole e-banking vulnerabilities and security scenario of CBs. Though Sonali Bank Limited has different sort of e-products and services such as ABB, SMS banking,

[74] http://dissertation.laerd.com/purposive-sampling.php (Accessed on: January 14, 2015).
[75] http://www.dutchbanglabank.com/DBBLWeb/branchlocation.jsp (Accessed on: May 24, 2016).

electronic clearing, ATM, CBS etc. The bank transacts daily total amount of Tk. 7213.5 million (Tk. 721crore and 35 lac) equivalent to US dollar 92.480 million by using bank-office electronic banking tools.[76] On the other hand, DBBL a fully automated bank has different sorts of e-products and services such as ATM, MFS, EFT through truncation and internet banking, PC banking etc. DBBL introduced FT network in 265 more vital locations across the country which is a new fashion of e-banking in Bangladesh. The daily average transaction of DBBL is approximately Tk. 1050 million (Tk. 105 crore) equivalents to US dollar 11.66 million through EFT, MFS and ATM.[77] In Bangladesh e-banking trends have been positively increasing day by day. Number of A/C holders has also been increasing according to Bangladesh Bank report.

3.1.5 Questionnaire Design

To collect the data from bank respondents, a structured questionnaire was prepared. The questionnaire was prepared in consultation with banking experts especially in the field of e-banking. Researcher also took into account the inputs of e-banking users to include important aspects of e-banking security in the questionnaire. The first part of the questionnaire dealt with the demographic profile of the respondents. The second part of the questionnaire was designed to collect information about major e-banking vulnerabilities and securities, bank's commercial success, bank's core risks and customer satisfaction. The next section was planned to collect information of e-security system adoption by e-bankers and its impact on bank business. And the final section of the

[76] Sonali bank limited, Head office, IT division (Dhaka: May 18, 2014)
[77] DBBL, *annual report* , 2013.

questionnaire was intended to collect information on existing e-banking transactions related vulnerabilities and security of e-banker (commercial banks).

3.1.6 Reliability and Validity of the Questionnaire

Questionnaires were checked for reliability and validity before produced those to the respondents. The content validity of all construct was checked by three experts (Two academicians and one banking expert).

3.1.7 Pre-testing of the Questionnaire

In order to screen out problems in the instructions or design of a questionnaire, a trial run with a group of 20 respondents were conducted. The questionnaire was found to have easy understanding and unambiguous statements.

3.1.8 Period of Survey

The survey of bank employees and customers were carried out during the period of June 2015–November 2015.

3.1.9 Data Attainability

To collect the data from e-banking providers, survey method based on the use of self-administered questionnaire was used. Initially, a sample of 119 respondents (84 from Sonali Bank and 27 from Dutch-Bangla Bank) was planned. In addition, 8 Questionnaires were also made to professionals of the central bank and of the Ministry of Information & Communication Technology of Bangladesh. However, the researcher could obtain all 119 valid questionnaires. Thus, the findings of this study are based on opinion of 119 respondents.

3.1.10 Data Processing and Analyzing

Collected data were processed and analyzed in accordance with the research plan. Processing implies editing, coding, classification and tabulation of collected data so that they are amenable to analysis. The term analysis refers to the computation of certain measures along with searching for patterns of relationship that exist among data-groups.

3.1.11 Techniques of Data Analysis

Data analysis method was applied in the present research. Correlation coefficient and Chi-squire test were used for estimating the relationships among selected variables. It is notable that Chi-square test is a statistical test commonly used to determine whether there is a significance difference or association between the expected and observed frequencies in one or more categories depending on specific hypothesis. Similarly Pearson's correlation is used to find a linear relationship between two variables. Data were furnished in charts, graphs and tabular presentation.

3.1.12 Variables

Dependent (response)

In this particular study, V*ulnerabilities* of e-banking are considered as dependable variable which depends upon diverse factors and indicators of e-banking security. Securities ensure secured e-banking where risks reduce and banks gain commercial success.

Independent (explanatory)

Here, *Securities* of e-banking have significant influence on e-banking vulnerabilities. So, e-banking securities have considered as the major independent variable for e-banking vulnerabilities. However other related factors and indicators had also been considered into account.

Other Intervening variables

This study includes *Core risks, Customer satisfaction and Commercial success* of bank as intervening variables. These are the results or core goal of secured e-banking system. Indicators of all type of variables discussed below in details.

The host study discussed elaborately below about the indicators of above stated variables to test the drawn hypothesis.

For the first and second hypothesis, the indicators of e-security systems are system secure from all possible vulnerabilities or threats, such as system authorization, authentication, configured network with updated firewall, cryptography and VPN mechanism, sound and vigilant application software, system with anti-malicious software, quality internet connections in branch level, access control, CCTV facilities in branch office, error free and timely response system, no communication failure, routine IT audit, internal control and compliance, computer enclave, routine backup & restore and DRS, verify transaction vouchers, insurance on intelligent device, tech-savvy employees routine meeting or discussion on security culture, IT policy & regulations, checklist on IT security, central oversight security team and so on.

On the other hand indicators of e-banking security vulnerabilities or flaws are anything that offers a potential avenue of attack against a system. Things are like systems without authentication, incorrectly configured systems/network, flawed application software, pirated/outdated operating system, system without anti-malicious software, faulty internet connection in branch/office, weak access control, slow response system, communication failure, chance of customers' data

loss, system ready for malicious attack, non tech-savvy employees, bank has no security checklist, policy or regulations on ICT , bank has no central oversight security team for audit, lack of legal support for bank and customer and so on.

For the third hypothesis, the indicators of bank's commercial success are the all positive achievement in business. Things are like minimize transaction costs, increase profit and profitability, image or reputation of bank business, accountability of bank business, competitiveness and so on. The indicators of e-security systems are mentioned above.

For the fourth hypothesis, the selected variables of e-security system are as same as above and the indicators of bank core risks are seven major risks addressed by central bank in its risk management guideline. These are ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk. Risks like reputational risk, operational risk and other related risks to be considered here.

For the fifth hypothesis, the indicators of customer's satisfaction are error free system, customer friendly and timely response system, quality internet connection (availability and reliability of internet) in branch level and so on. On the other hand the indicators of e-security system adoption are as same as mentioned above.

Conclusion

Methodologies discussed are considered appropriate to progress this study achieve its goal. Researcher turn to apply them to the data gathered attain the possible outcomes of the study.

Chapter IV
Theoretical and Conceptual Framework

Introduction

This chapter contains an in depth discussion on the concept, theoretical basis and different sorts of models of major e-banking vulnerabilities and securities that are important in conducting the research. It also represents the information security risk management process and the role of regulatory authority or forum in reducing risk.

The most dangerous attack in a versatile networking world is electronic attack. Electronic attack is merely possible when a system is vulnerable and ready for the threats. In a versatile networking world internet can be seen as a truly global phenomenon that has made time and distance irrelevant to many transactions. One industry that is using this new communication channel to reach its customers is the banking industry.[78]

Today truly e-banking is not possible without networking (internet). E-banking transaction between bank and customer or one branch to the other requires a new advanced communication channel through internet. In an internet world, system with improper security is more vulnerable and easy to be infected. So, as an e-banker, automated commercial banks need to identify and understand present complex nature of vulnerabilities or threats they have been facing now. Technology is being upgraded day by day and attack took new shape

[78] Tejinder Pal Singh Brar, Dr. Dhiraj Sharma and Dr. Sawtantar Singh Khurmi," Vulnerabilities in e-banking: A study of various security aspects in e-banking," *International Journal of Computing & Business Research* ISSN (2012): 2229-6166.

accordingly. That's why any traditional security measure cannot ensure safety bank's security. So, banks need to adopt standard and time demanding security mechanism or model to protect their system from any harm which is defined by the security experts, professionals or organizations. Security adoption can be implemented properly by proper management and proper management will ultimately reduce operational and technological risks for e-banker. Moreover, Security risk management issue is very much concern to make e-bankers safe and sustainable.

E-banking services can be safe and secured by using the concept of reliability, innovation adoption theory, the quality of the Internet connection, trust of the system, authentication theory, key locker security, one time password (OTP), biometrics, secured networking devices (switch, router, firewall, etc.) and required e-commerce law. Yet Three-Tier Security Model for e-business familiarized as a security model for e-banking services. It is constituted by authentication, encryption, and certification. Authentication, encryption, and certification authority (SSL/IPSce) are well known security mechanisms for processing Internet-based services for a very long time, and it is currently in use by the existing Internet banking models. Implementing the three-tier security model for Internet Banking will offer safe Internet banking transactions that protect both the customers and banks.[79] However, many models were developed excluding above mentioned security initiatives to keep online banking services harmless.

[79] Yu Lasheng, and Mukwende Placide, "Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services." *International Computer Science and Computational Technology* Huangshan, P. R. China, 26-28 December 2009.

4.1 Inherent security threats and countermeasures by banks

4.1.1 Identifying major vulnerabilities and threats

Banks and service providers need to guard against various types of online attacks. The object of an attack may vary. Attackers may try to exploit know vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a web site during a short time frame thus denying service to other customers. To simplify matters we can categorize the attacks into three main groups: local, remote and hybrid attacks. Local attacks happen on the victim's machine, remote attacks don't modify the machine but try to intercept or redirect the traffic of a session and hybrid attacks combine local and remote attacks and are the most powerful.[80]

Scholars found some flaws in the security of online banking. These are-

i) Flaws in banking websites

ii) Flaws in banking Policies

iii) Flaws in users usability and customer awareness

According to Gordon and Loeb, Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solutions and managerial actions. Banks are not only dealing with intangible money transactions, but also with protection of highly sensitive information such are credit cards' PINs, personal information about the customers, history of transactions regarding their bank accounts and all other kinds of information that could enable to third party conducting the criminal

[80] Ibid, 33.

activities and making damage for both, customer and bank.[81] All commercial operating systems have vulnerabilities, also known as weaknesses in the computer system said Landwehr. According to Loch, et al. and Whitman these vulnerabilities create opportunities for possible threats to the information housed on these systems. Security threats can be classified into several categories from internal to external, human or non-human, and intentional or non-intentional.[82]

Researcher reviewed different literatures and found some special and advanced type of vulnerabilities in European and Scandinavian countries like spyware, phishing, spoofing, skimming, denial of service, man in the middle attack and so on. Most of the vulnerabilities are online banking related. Even in Asia especially countries like India and Bangladesh it is found that sorts of vulnerabilities which is merely similar to above stated threats. Researcher visited some public and private CBs and identified vulnerabilities like identity theft, malware virus contagion, faulty ICT infrastructure and networking (internet) connection, delay of transaction, lack of technological knowledge and intentional or accidental occurrence by bank people are the common reasons of e-banking fraud and forgeries here in Bangladesh.

Attack can be taken place through hardware, software or hybrid form of technologies. In a local circumstance, attack is occurred through infection by hardware devices with malware or physical presence of intruders where access is not controlled properly. On the other hand, in a cyber context attack takes place

[81] Nedim Makarevic, "Comparative analysis of perceptions towards IT security in online banking; Students of Monternegro vs Aabanian students," *European Scientific Journal* edition 11, no.28 (October 2015): 1857 – 7881

[82] Bilal Ahmad Sheikh and P. Rajmohan, "Internet Banking, Security Models and Weakness," International Journal of Research in Management & Business Studies 2, Issue 4 (December 2015):17-22.

through remote access by intruders using advance technology (spyware, phishing, denial of service attack, man in the middle attack, credentials theft by mail, etc.) or through faulty configured network system. Both local and cyber vulnerabilities are simultaneously responsible for operational and technological threats. A survey result was conducted to find out the kind of flaws carry by e-bankers where adverse representations of vulnerabilities are brought out. It is found that in Bangladesh a large portion of the banks carry 'very high' risks of online fraud and security threats, found in a study conducted by BIBM a national training, research, consultancy and education institute on banking and finance in Bangladesh. Below pie chart is presented the vulnerabilities consequence stated above.

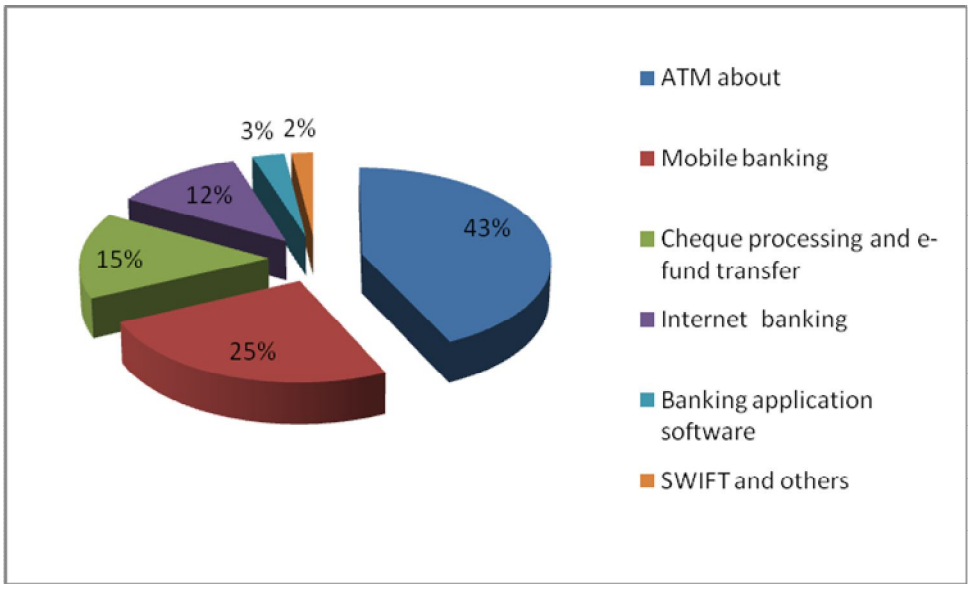


Chart- 4.1

Despite of numerous security risk management guide lines provided by the regulatory authority and international forum, CBs have continuously been facing massive internal and external attacks in recent time here in Bangladesh. Some

[84] Zachary B. Omariba, Nelson B. Masese and Dr. G. Wanyembi, "Security and Privacy of Electronic Banking," International Journal of Computer Science Issues 9, Issue 4, no 3 (July 2012):432-446.

public and private sector banks already confronted skimming, theft of credentials, malware contagion, internal human error, intentional cyber robbery and so on mostly in the year of 2016. Even system (SWIFT platform) of regulatory authority in our country is not almost safe from cybernetic intruders. Hence, the financial service industry became the target of clever hackers and proved merely vulnerable. There are serious technological, operational and compliance related vulnerabilities are found in this particular sector.

4.1.2 Security adopted by the banks

In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved.[84] The key areas are security, privacy, authentication and divisibility. Similarly operational and law related matter is unavoidable part. However, despite of numerous threats various defenses can be applied to e-banking such as awareness or education of bank people and customer, personal firewalls, SSL mechanism, password policies, vulnerability assessment tool like switching software or Intrusion detection tool, audits of security logs and so on.

Taking security measures like factor authentication, point solution encryption, network security by VPN, configuration of and anti-malicious scanning software tools ensured e-banking security in many countries. Similarly, in order to maintain secured e-banking service internal control and compliance is very important considerable part to the banks.

According to Indian Central bank report, Security issues include questions of adopting internationally accepted state-of-the art minimum technology standards

for access control, encryption and decryption, firewalls, verification of digital signature, Public Key Infrastructure (PKI) etc. Beside, the information systems security could be achieved by implementing a suitable set of controls which consists of policies, practices, procedures, organizational structures, hardware and software functions. Ensuring internet banking security controls and measures bank requires considering three important things described below.

i) Information Security Policy (Information security policy should, inter alia, relate to policies such as firewall, email, network security, and password which should also address issues relating to prevention of cyber attacks by deploying appropriate technologies such as two-factor authentication. Structured well defined documented security policies, standards and guidelines);

ii) Security Systems (Hardware and Software); and

iii) Committees for security (Fraud Monitoring Committee, Information Technology Strategy Committee, Information Security Governance).[85]

In Bangladesh some private sector bank is pragmatic regarding technology issue such as factor authentication, security certificate, secured network, anti-skimming device in ATM and so on but operational measures of e-banking seem to be imperfect. On the contrary, public sector bank is far behind compare to private sector bank from technology viewpoint as well as operational issues. Regulatory instructions relating to e-banking is also ignored by CBs. Even they didn't installed proper security mechanisms or model to e-banking services. Operational

[85] Rajpreet Kaur Jassal and Ravinder Kumar Sehgal, "Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example," *IOSR Journal of Computer Engineering* 13, Issue. 1 (Jul. - Aug. 2013):114-121.

issue like surveillance of branch is found poor in different branches at the population banks.

Bank	Branch	Security Status
Sonali Bank Ltd.	Six branches at Rajshahi City	i) Customers have access in computer enclave ii) Two of six have CCTV facilities (Corporate and Court Building branch) iii) Core banking process is recently started. Online PC banking exists. iv) Faulty network connection (ISP). Not error free v) Delay fund transfer
Dutch Bangla Bank Ltd.	One branch at Rajshahi City	i) Customers do not have access in computer enclave ii) Having full CCTV facilities (Rajshahi branch) iii) Bank has centralized core banking solution iv) Good network connection (ISP). Low error v) Sometime delay fund transfer

Figure- 4.1

The largest state own financial intermediary Sonali Bank Ltd. has rendering same services with different banking software (e.g. “Baxi bank” , “Easy banking”, “SBS” an in-house banking software). It might be called “one function through different software” system. It is obviously very unfortunate security strategy from technological and operational point of view. Different software has its own mechanisms which can conflict with each other (if it is not configured as per requirement) during online data transformation. Although recently the bank started to install integrated centralized banking software “CBS” which will give the bank core banking status. But it takes huge time to complete installation in almost all of the branches. Access control, physical layout of digital device, electric layout, present networking connectivity and other necessary inside security is

over looked which doesn't comply particular model discussed above. Beside, DBBL is more conscious to adopt technological security mechanisms but flaws are found in operational issue.

4.2 Security Pillar

4.2.1 Security experts' definition and models

Generally, protection of e-banking services from any adverse situation can be termed e-banking security. Security can be implemented in a variety of ways. There is a ton of information that none of us want anyone else having access to the system (i.e. passwords, social security numbers, bank accounts, etc.). Information can easily be stolen. "Identity theft" is the illegal use of someone else's personal information in order to obtain money or credit. This could easily be obtained from organizations' computer network if the network is not properly secure.[86] Information security refers protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-[87]

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure including means for protecting personal privacy and proprietary information; and

[86] http://www.infosecwriters.com/text_resources/pdf/KRodriguez_OSI_Model.pdf (Accessed on January 6, 2015).

[87] http://www.expertglossary.com/definition/information-security (Accessed on: December 2, 2014).

- Availability, which means ensuring timely and reliable access to and use of information.

So, Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security[88]

Information security is prime objective when an organization deals with internet or extranet. Today's banking industry is one of the most important sectors using internet as a business communication channel. Internet is a communication tool for online banking. There is continuously growing number of customers who use Internet banking because of its convenience. But the security and privacy of Information may be one of the biggest concerns to the online banking users[89] as well as bankers. Internet banking or online banking is not possible without ICT infrastructure. So, technological (IT) security is the pre-condition for e-banking operation. Different security experts and security organizations emphasized on it. According to Rick Lehtinen, G.T. Gangemi computer and network security are built on three pillars, commonly referred to by the C- I - A acronym:[90] These are-

- confidentiality;
- integrity; and
- availability.

[88] http://www.thefreedictionary.com/Information+security (Accessed on: December 1, 2014).

[89] Syeda Farha Shazmeen and Shyam Prasad, "A Practical Approach for Secure Internet Banking based on Cryptography," *International Journal of Scientific and Research Publications* 2, no.12 (December 2012).

[90] Rick Lehtinen, G.T. Gangemi Sr., *Computer Security Basics* (Gravenstein Hwy N Sebastopol, CA O'Reilly Media, 2nd ed., 2006), 9.

But the persistence of the classic triad of CIA is inadequate to describe what security practitioners include and implement when doing their jobs. So now there needs a new information security framework that is complete, correct, and consistent to express, in practical language, the means for information owners to protect their information from any adversaries and vulnerabilities.[91] The general meaning of the new information security has taken all possible security measures what is completely needed to protect organizational data (information). That means all possible way to protect any kind of vulnerabilities and threats.

Security experts Parker suggests a new model of Information security which consists of six essential foundation elements: availability, utility, integrity, authenticity, confidentiality and possession. Parker claims that his model addresses the limitation of Information security by the CIA-triad.[92]

According to Boukhonine et al., the main priority of every bank is to provide a safe and secure environment for their clients to perform online banking transactions. Based on the security policy of each bank the main considerations of framing a security policy are accountable, confidentiality, availability, integrity and non-repudiation are the primary concerns.[93]

There are several models approached by the scholars and researchers. Technology Adoption Model (TAM) is one of them. TAM is considered as a relevant model when it comes to the acceptance of technology to understand the

[91] Donn B. Parker, *Fighting Computer Crime, A new Framework for Information Security* (New York: John Wiley & Sons, 1998), 229-255.
[92] D. Parker, Fighting Computer Crime (NY: J. Wiley and Sons, 1998).
[93] Dhurgham T. Ahmad & Mohammad Hariri, "User Acceptance of Biometrics in E-banking to improve Security," *Business Management Dynamics* 2, no.1 (July 2012): 01-04.

attitude of human behavior and intention to accept the technology which is biometrics in the context of this study.

Technology Adoption Model (TAM)

TAM was the basic model being used in most of the research work related to the acceptance of technology where the core constructs of the study being perceived ease of use (PEU), Perceive usefulness related to the intention of sue of technology. One such study were used this model to consider adoption of biometrics in banks. “Internet banking security guideline model for banking in Thailand” were conducted by M.L.Kulthon Kasemsan and Nantana Hunngam to examine customer’s trustworthiness on technological security by using TAM.[94] The study of the Internet banking security guideline model and tools development as well as information technology were conducted to ensure the security of the Internet banking services by using the concept of reliability, innovation adoption theory, trust of the system, ease of use, the quality of the Internet connection and e-commerce law.

Perceptions of Biometrics banking Security

User perception to adopt biometrics in banking is closely related to the security being offered in this form of banking and how it influences the user’s perception to accept this technology. This construct is related to the perceptions of the users to adopt the technology of biometrics in the banking activities which suggests that adopting biometrics would make online banking more secured and offer the best

[94] M. L. Kulthon Kasemsan and Nantana Hunhgam, “Internet Banking Security Guideline Model for Banking in Thailand,” *IBIMA Publishing* 2011 (2010):13.

of services at the comfort of his own which again is in turn influenced with the construct self efficacy.[95] Security biometric is the science of using physical characteristics (fingerprints, eyes, hands) to identify a person and some of the products used in this system include fingerprint readers *and* retinal scanners. When you are considering security biometric, you want to have physical characteristics that are constant and do not change over time and are also difficult to fake or change on purpose.[96]

STRIDE model

Another security analysis model is STRIDE threats model. This model derives from an acronym for the following six threat categories:

- *Spoofing Identity*: The illegal use of another user authentication information;
- *Tampering with Data*: A maliciously modified data;
- *Repudiation*: Users refuse to engage in activities, and there is no way to prove he was repudiation;
- *Information Disclosure*: Information is exposed to the access to it is not allowed;
- *Denial of Service*: Refuses to the legitimate user service;
- *Elevation of Privilege*: No privileged user access privileges, so as to have enough ability to damage or destroy the entire system.

[95] Ibid.,1.
[96] http://findbiometrics.com/applications/biometrics-security/ (Accessed on: January 15, 2015).

By considering threats of these various categories for each single element in the data flow diagram (DFD), STRIDE greatly supports the identification of threats within the application. The study is based on online banking system data flow analysis as the foundation, analysis of whether each data flow and its associated asset information is vulnerable to any type of S, T, R, I, D and E threat, threat model to construct the entire online banking system.[97]

Three-Tier Security Model

A new model for processing Internet banking transactions is presented by Chinese scholars Yu Lasheng and Mukwende Placide is Three-Tier Security Model that increases trust and security over the existing model, by allowing customers and banks to authenticate each other, and sign processed transactions online, It enhances security through use of a three-tier, trusted, layered, and secure channel. The model ensures that only qualified people can access Internet banking accounts, that the information viewed remains private and can't be modified by third parties, and that any transactions made are traceable and verifiable. For customers to use Internet banking services comfortably, they must have confidence that their online services are trustworthy and secure. Similarly, for banks to provide Internet banking services they need confidence in the security of online transactions.[98]

Hidden Markov Model

Authentication, Encryption, and Certification Authority are well known security mechanisms for processing Internet-based services for quite a long time, and these are currently in use by the existing Internet banking models. This is

[97] Tong Xin and Ban Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model," *International Journal of Security and Its Applications* 8, no.2 (2014): 271-282.

[98] Yu Lasheng and Mukwende Placide. Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services. *2009*. Web. 12 December. 2015.

basically site to site VPN communication with different tunnel based security protocols (PPTP/ALS/L2TP/SSL/IPSec). Hidden Markov Model (HMM) is the statistical tools for engineer and scientists to solve various problems regarding internet banking fraud detection. The methodology is aimed at detecting fraud incase of internet banking. In internet banking a fraud detection system will run at the banks server and its function to detect fraud in online transaction. This is a state and transition probabilities prediction system. Fraud detection is carried out using HMM which uses baum-welch algorithm.

An HMM is initially trained with the normal behavior of an account holder. If an incoming online banking transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, ensuring that genuine transactions are not rejected. Experimental results show the performance and effectiveness of the system and demonstrate the usefulness of Hidden Markov Model.[99]

Open system interconnection (OSI) security model

One more popular security mechanism is open system interconnection (OSI) security model for information communication through seven layers such as physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer. It is a holistic networking security stack and ensures internet security properly. E-bankers can rely on this security mechanism because it is simplest and easy to understand compare to other model.

[99] Sunil S Mhamane and L.M.R.J Lobo, "Use of Hidden Markov Model as Internet Banking Fraud Detection," *International Journal of Computer Applications* 45, no. 21 (2012).

In 1983, the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) merged documents and developed the OSI model which is based on a specific hierarchy where each layer builds on the output of each adjacent layer.[100] The OSI model is a protocol stack where the lower layers deal primarily with hardware, and the upper layers deal primarily with software. The OSI model's seven layers are designed so that control is passed down from layer to layer. The OSI security architecture reference model is also designed around seven layers, reflecting a high level view of the different requirements within network security.[101] It is perceived level of security stack in OSI layer which can be used as a truly time demanding security model for e-banking networking infrastructure. The OSI model defines the basic building blocks of computer networking, and is very essential part of a complete understanding of modern TCP/IP networks.[102]

OSI security stack architecture

Layers	Security Model
Application	Authentication
Presentation	Access Control
Session	Non-Repudiation
Transport	Data Integrity
Network	Confidentiality
Data Link	Assurance/Availability
Physical	Notarization / Signature

Figure- 4.2

[100] http://www.studymode.com/essays/Network-Security-At-Osi-Layer-49384293.html (Accessed on: January 10, 2015)

[101] http://searchnetworking.techtarget.com/answer/Security-of-each-level-of-the-OSI-model (Accessed on : December 1, 2014).

[102] http://computerguru.net/Network (Accessed on: May 2, 2015).

The above stack is taken each layer of the OSI model and described a relevant vulnerability with a solution to that problem area as users became more aware of the vulnerabilities that exist in the IT environment. More importantly, the user could be able to use the OSI model as a guide to simplify the security process.

Any attempt to establish electronic security needs to be built on at least the following eight important pillars: (i) an adequate legal and enforcement framework—which is not present today in many emerging markets; (ii) adequate arrangements to ensure electronic security of payment systems; (iii) an adequate supervision and prevention regime that creates better incentives to implement appropriate layered risk-management systems, including electronic security for financial services providers; (iv) encourage and promote a framework within which private insurance companies can insure against and monitor e-risk, thereby helping to improve standards in this area via the underwriting covenants they require; (v) develop certification standards and processes established with respect to digital signatures and, more broadly, to vendors operating in the electronic security industry; (vi) actions to improve the accuracy of information available about e-security incidents and the roles of the public and private sectors in this process; (vii) educate citizens, employees, and management on security issues as a means of preventing e-security incidents; and (viii) implement a twelve-layer security structure.[103]

[103] The World Bank, *Electronic Security: Risk Mitigation In Financial Transactions* (June, 2002), 7-8.

4.2.2 Standard policy and mechanisms

According to Charles P. Pfleeger and Shari Lawrence P.fleeger, to meet the challenges, any organization should adopt proper policy and policy can be implemented by mechanism. Once a security policy has been laid down, it becomes possible to concentrate on the security mechanisms by which a policy can be enforced.[104]

Important security mechanisms are:

i) encryption (Encryption transforms data into something an attacker cannot understand);

ii) authentication (The service must learn the client's identity. Users are authenticated by means of passwords);

iii) authorization (Seeking proper permission);

iv) auditing (Auditing tools are used to trace which clients accessed what, and which way).

So, e-security system means system secure from all possible vulnerabilities or threats, such as system authorization, authentication, access control, configured network or firewall, encryption, quality internet connections in branch level, error free and timely response system, legal support and so on. Standard mechanisms represent such a security condition where system is safe from all possible attacks. Preamble of information security guideline of Bangladesh (draft) mentioned that this document (draft) is a guideline to help government agencies

[104] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing* (New Jersey: Pearson Education Inc., 2003), 415.

to formulate their own Information Security Policy to protect their information in the cyber space.[105] Central banks of different countries and international forum like Bessel Committee on banking supervision have different online banking policy guideline for commercial banks. In Bangladesh, Bangladesh Bank is a regulatory authority directs CBs regarding online transactions.

4.3 Security risk management

4.3.1 Role of the local and international regulatory authorities or forums

Security risk management is completely different and unique in nature. In this particular study, security risk management represents informational and technological, operational and laws related security risk management of e-banking system. In the world of virtual banking, it is obviously more important to manage. E-banking is merely impossible without proper technological and operational security risk management and this particular risks management has very close relation to banks strategic risk, transaction risk, compliance risk, reputation risk, information security risk, credit risk, interest rate risk, price risk and foreign exchange risk.

Managing the risks and implementing controls for Internet banking initiatives follows the same principles as other risk management processes. The most dangerous thing is to treat this as a technical problem and leave it to IT management to manage. So, Information and communication security risk management is one of major risk management agenda out of seven core risk management process according to Bangladesh bank.[106] Basel Committee

[105] BCC and Ministry of ICT, *Information Security Policy Guideline, Bangladesh, Draft*, 6.
[106] Ganesh Ramakrishnan, "Risk Management for Internet Banking," *ISACA* 6 (2001):12.

recommends this is a general management issue which needs attention from senior management. A general framework of risk management is set forth below:

Board and Management Oversight

The board and senior management should establish effective management control over the risks associated with e-banking activities, including specific accountability, policies and controls to manage these risks. Further, management should clearly understand the role of Internet banking in meeting the institution's overall strategic objectives. The business should set specific objectives for Internet banking, such as revenues, profits, transaction costs and service levels. An unambiguous objective sets the tone for a robust risk posture.

Security Controls

Authentication— This means ensuring customers are verified and their identities established before conducting business over the Internet. Passwords, biometric methods, challenge-response systems, PKI are some of the ways of strengthening authentication. There is a growing trend towards single-sign-on applications, where the customer needs only a single ID to access his entire relationship. These increase the risk of compromise.

Non repudiation— Banks should make certain that customers who transact on the Internet cannot later deny having originated the transactions. Using techniques like PKI (digital certificates), strong non repudiation can be achieved. However, legal enforceability in many countries is still suspect. Segregation of duties— as in any traditional process, segregation of duties is vital to prevent perpetration of fraud by any one individual.

Legal and Reputational Risk Management

Legal and reputational risk management can be broken down into the following:

Privacy— Banks should articulate a privacy policy and should communicate this to customers. Customers must be allowed opt-out options, and great care must be exercised before sharing customer information with outside entities. If customers are from a different jurisdiction, then the strongest privacy law may be applied.

Availability— Banks should have business continuity and contingency planning processes to help ensure continuous availability of Internet banking services. This is challenging because of the potential for high transaction volume and the demand for 24-hour, seven-day-a-week availability.

Incident response— Banks should formulate appropriate incident response plans to detect, manage, contain and minimize problems arising from internal and external attacks. There should be clear escalation paths, a communication strategy for customers and the press and a documented chain of command. Finally, there should be a process for collecting and preserving forensic evidence after an adverse event.[107] H. Van De Vyver an expert on risk management in e-banking told that there are two types of risks associated with e-banking operation. Type one risks are:

- Technology and infrastructure;
- Security;

[107] Ibid., 43.

- Data integrity;
- System reliability;
- Internal controls-audits; and
- Outsourcing

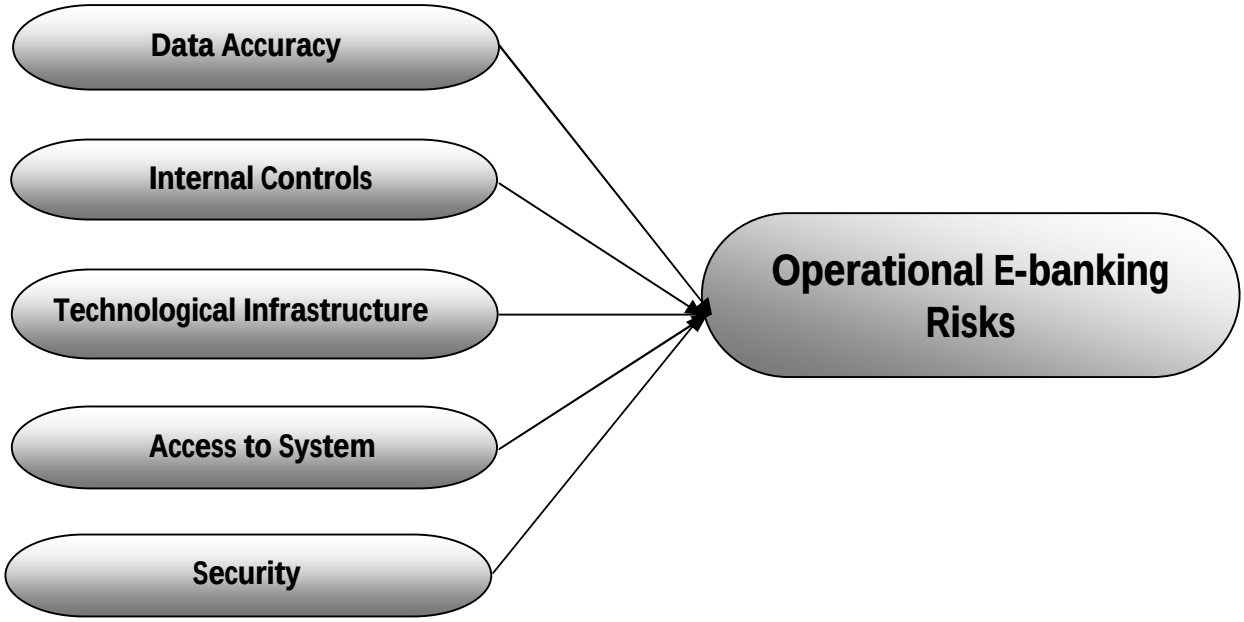


Figure- 4.3

Type two risks are:

- Reputational risk;
- Legal risk
- Other traditional risks are such as credit, liquidity, market and foreign exchange risks.

Ganesh Ramakrishnan and Vyver both basically emphasized on Bessel committee's conceptual model or principles on information security risks management for e-banking.

Vyver recommended possible risks and risks management measures in retail electronic banking and electronic money[108]

Examples of possible risks	Possible manifestation	Potential effect on the banking organization	Possible risk management measure
Operational risks			
Unauthorized system access	Hacker gains entry to internal systems. Confidential customer in formations is intercepted by unauthorized third party. Virus injected into bank systems. Bank's system and data deliberately corrupted and crashed.	Loss of data. Theft of, or tempering with, customer information. Disabling of a significant portion of bank's internal computer system. Costs associated with repairing system. Perceived insecurity of bank's systems and potential adverse publicity.	Penetration testing for vulnerabilities. Surveillance to detect anomalies in usage. Deployment of communication security measures such as firewall, password management, encryption techniques, and proper authorization of end users. Deploy virus checking and on-going monitoring of security measures in internal systems.
Employee fraud	Employee alteration of data in order to draw funds from general bank accounts and to obtain information from record.	Costs associated with reimbursing customer losses and with reconstructing accurate data on customers. Possible losses from redeeming electronic money for which no corresponding repaid funds were retrieved. Customer may perceive the bank as being unreliable. A bank faces legal and regulatory sanctions, and negative publicity.	Develop policies for adequately screening new employees, institute internal controls, including segregation of duties. External auditing of employee performance. Proper control over storage, manufactures, etc. of smart cards.

Figure- 4.4

[108] http://www.slideshare.net/hubvv/risk-management-and-regulation-in-electronic-banking (Accessed on: November 29, 2015).

According to security risk management experts Andre N. Klingsheim et. al. risk management implies that exposure to risks should be a conscious decision. The starting point for a risk management process is to decide the risk acceptance criteria, reflecting how much risk one is willing to take. Figure 3.6 shows a high-level view of a qualitative risk management process containing two phases, assessment and treatment of risks. As computer systems and their threats tend to change over time, the process must be carried out periodically. The first activity of the risk assessment stage aims to establish a good overview of the system. Second, threats and vulnerabilities are identified. The combination of a threat and vulnerability constitute a risk to the system. Finally, the risks are evaluated by determining the likelihood and impact of each threat-vulnerability pair. A thorough assessment is of great importance to the success of the overall risk management process. In the second phase, the determined risks are subject to risk treatment in light of the risk acceptance criteria. For each risk there are four approaches:

Accept - The risk is acceptable, no action taken.

Control - The risk is too high, measures are taken to reduce the likelihood and/or impact of the risk, thus making it acceptable.

Reject - The risk is too high, the risk is avoided by e.g. dropping risky functionality or working around the risk.

Transfer - The risk is transferred to another party, e.g. through insurance.

Bellow figure- 3.6 illustrates a risk management process by risk assessment, risk identification and its treatment.

Risk Management Process

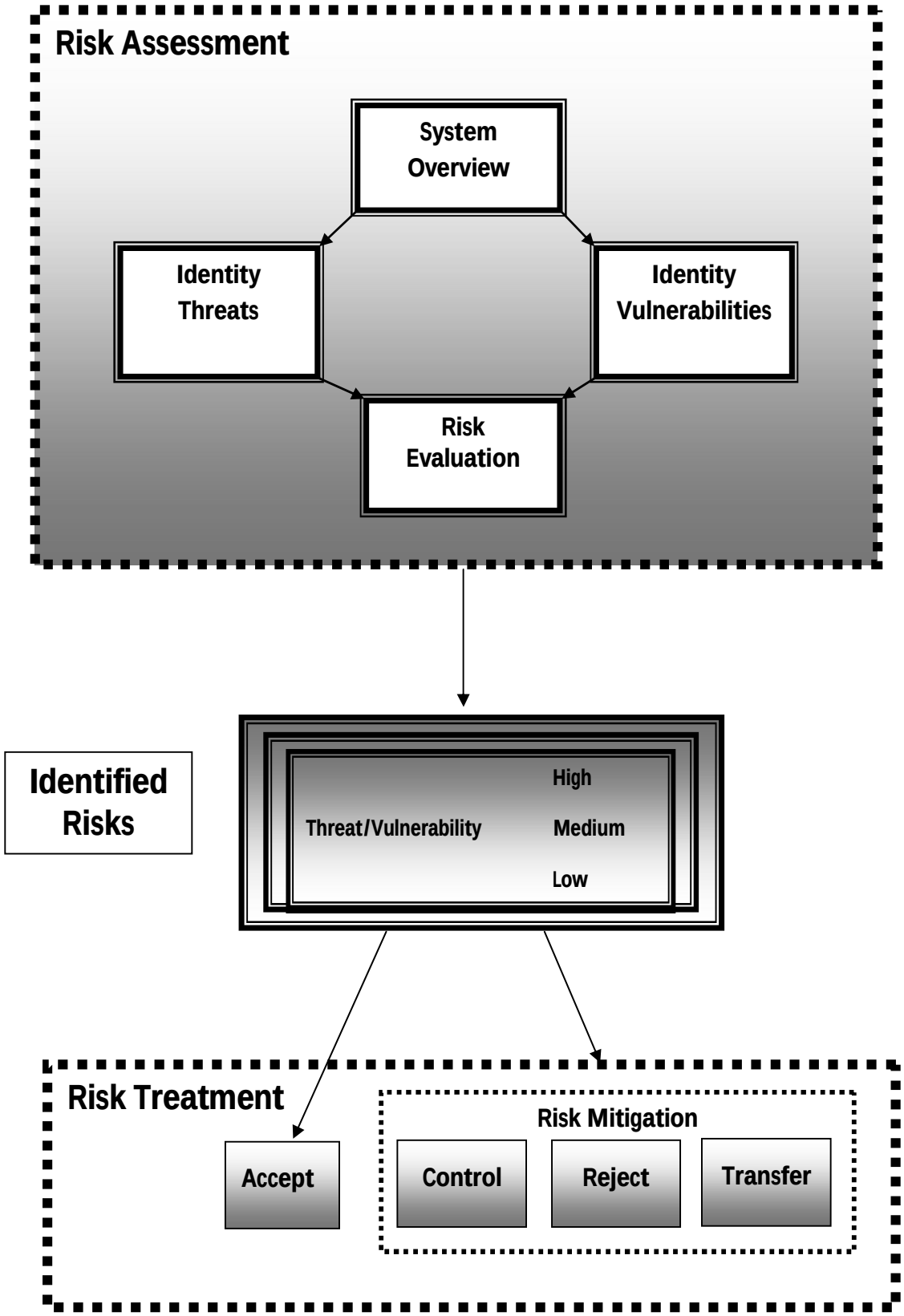


Figure- 4.5

After the risk treatment phase there are remaining risks, referred to as residual risks that satisfy the risk acceptance criteria.[109]

According to Thomas Glaessner, Tom Kellermann and Valerie McNevin[110] today the gap between the risk management of physical assets and the risk management of informational assets is large. Moreover, the gap between a bank's operational risk management and information technology risk management requirements places many of the bank's key information assets at risk. Management of e-security risks can be thought of as a twofold process. The first part is risk analysis, which has three major components: identify and inventory assets for a baseline, analyze and assign values to the assets, and establish how critical each asset is, in priority order. The second part of security is development of an approach to risk management. The major elements of risk management are to develop and implement policies and procedures, educate users (employees and customers), and audit and monitor for quality assurance. A prudent approach might reflect the following thesis: "Expect to be hit – Prepare to survive." The three general axioms to remember in building a security program are as follows:

- Attacks and losses are inevitable.
- Security buys time.
- The network is only as secure as its weakest link.

[109] Andre N. Klingsheim, et. al., "Risks in Networked Computer Systems" (Diss., University of Bergen, 2008), 7-8.

[110] The World Bank, *Electronic Security: Risk Mitigation In Financial Transactions* (June 2002), 52.

12 core layers of proper security are essential for maintaining the integrity of data and mitigating the risks associated with open architecture environments, and in many instances, actual implementation of a specific layer need not entail large capital investments or outlays. Twelve stated core layers are as follows:

i) Information Security Officer: The creation of the position of Chief Security Officer who overseas that the other 11 layers are carried out and implemented in accordance with the best practices.

ii) Risk Management: A broad based framework based upon CERT's OCTAVE paradigm for managing assets and relevant risks to those assets.

iii) Access Controls/Authentication: Establish the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication). The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI).

iv) Firewalls: Create a system or combination of systems that enforces a boundary between two or more networks.

v) Active content filtering: At the browser level, it is prudent to filter all material that is not appropriate for the workplace or that is contrary to established workplace policies.

vi) Intrusion detection system (IDS): This is a system dedicated to the detection of break-ins or break-in attempts, either manually or via software expert systems that operate on logs or other information available on the network. Approaches to monitoring vary widely, depending on the types of attacks that the system is expected to defend against, the origins of the attacks, the types of assets, and the level of concern for various types of threats.

vii) Virus scanners: Worms, Trojans, and viruses are methods for deploying an attack. A virus is a program that can replicate itself by infecting other programs on the same system with copies of itself. Trojans do not replicate or attach themselves to other files. Virus scanners hunt malicious codes. Annex I details proper maintenance and configuration of these scanners.

viii) Encryption: Encryption algorithms are used to protect information while it is in transit or whenever it is exposed to theft of the storage device (e.g. removable backup media or notebook computer).

ix) Vulnerability testing: Vulnerability testing entails obtaining knowledge of vulnerabilities that exist on a computer system or network and using that knowledge to gain access to resources on the computer or network while bypassing normal authentication barriers.

x) Proper systems administration: This should be complete with a list of administrative failures that typically exist within financial institutions and corporations and a list of best practices.

xi) Policy Management Software: A software program should control Bank policy and procedural guidelines vis-à-vis employee computer usage.

xii) Business Continuity/Incident response plan (IRP): This is the primary document used by a corporation to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically.

Many banks have assumed that Internet banking primarily increases information security risks and have not sufficiently focused on the effect on other banking-specific risks. Risk management disciplines have not evolved at the same speed and many institutions, especially the smaller ones, have not been able to incorporate Internet banking risk controls within their existing risk management

structures. Information security risk management is a holistic approach to managing these risks.

By considering the findings of the research in other countries, the researchers have found five kinds of risks: Security, financial, social, time and performance risks in e-commerce area. Moreover, through the research carried out in Iran, two more kinds of risks were discovered which are: legal and hardware risks based on the fact that e-commerce is a kind of newly established business in Iran from the customers' point of view.[111] Above mentioned literatures proved that how many risks are associated with security risk management. It is worth notable that security risk management is connected with banks all other risks.

Many national and international regulatory authority or forum designed e-banking policy and mechanism to protect banks' information and systems. Bessel Committee on banking supervision and Central Banks of different countries are important of them. In Bangladesh, as a local regulatory authority Bangladesh Bank designed guideline on ICT security for scheduled Banks and financial institutions[112] and separate guidelines on MFS for the banks that directed e-bankers how to make a policy or guideline to protect their own information (asset) from any harm. In India, Reserve Bank of India constituted a Working Group to examine different issues relating to internet banking and recommend technology, security, legal and operational standards keeping in view the international best

[111] Reza Shafei and Vala Mirani, "Designing a model for analyzing the effect of risks on e-banking adoption by customers: A focus on developing countries," *African Journal of Business Management* 5 (2011): 6684-6697.

[112] Bangladesh Bank, *Guideline on ICT Security For Scheduled Banks and Financial Institutions (*2010)

practices.[113] On the other hand, as an international forum for supervising authority Bessel Committee on banking supervision expects the rapid development of e-banking capabilities carries risks as well as benefits of bank. Such risks to be recognized addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services.[114] The committee has designed full fledge risk management principles for electronic banking both national and cross border transactions.

Nevertheless, some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. Basel Committee on Banking Supervision introduced in January 2013 a comprehensive 14 BCBS principles of e-banking risk management through Principles for effective risk data aggregation and risk reporting. These are Governance, Data architecture and IT infrastructure, Accuracy and Integrity, Completeness, Timeliness, Accuracy, Comprehensiveness, Clarity and usefulness, Frequency, Distribution and Review.

4.3.2 Self strategy of commercial banks

In Bangladesh, e-banking is nothing more than traditional banking and banks just use a new communication channel (networks or internet) for e-banking services. But it adds new kinds of e-risk to banking. Risks like distance banking through communication channel, strategic risk of losses and new form of competition, electronic infrastructure are really challenging for today's banking. Equally

[113] Virender Singh Solanki, "Internet banking: A study of regulatory, supervisory & management issues," *ZENITH International Journal of Business Economics & Management Research* 2, no. 5 (2012):119.

[114] Bank for international settlement, Bessel Committee on banking supervision, *Risk Management Principles for Electronic Banking (*2003)

technological investment is huge by amount. But it is worth noting that investment for risk management or e-security is very insufficient compare to investment of IT infrastructure by banks. Hence, CBs tried to minimize the risk to ensure quality service by increasing investment of e-security. In our country, CBs have own written policy and online banking guideline to conduct e-banking operation. But that is in the form of black and white. It is practically not maintained properly as regulatory authority directed to the bank. Other than policy guideline they have additional ICT checklist to audit e-banking operational activities. But it has some flaws according to analysts. However, banks in Bangladesh have been trying to introduce standard ICT policy and mechanisms of their own. Still it is merely a transitional period for bankers here in Bangladesh. Banks have developed ICT security guideline but not able to implement properly because of non-availability of tech-savvy people, budget and support but they have positive attitude to implement those regulations designed by their own. Recently some banks hired outsourcing to manage their whole electronic infrastructure and try to overcome the deficiencies mentioned above.

4.3.3 Security practices by the banks

In banking industry, security is a core issue in banking operation. But in a virtual world, electronic system experienced different sorts of vulnerabilities and threats. Internet banking security is well known and many security models and protocols have been developed for it.[115] Banks of many countries around the world follow different security techniques and models. These are first factor authentication or (OTP), second factor authentication (biometrics), cryptography, technology

[115] Ibid., 6.

acceptance model (TAM), STRIDE threats model, three-tire-security model etc. The word “security” is in-built idea both for manual banking and electronic banking. Banks here in Bangladesh do not precisely follow such particular mechanism for their online transactions which are mentioned above. In this regard lapses are found. It is a hybrid type of security system introduced by the banks as it is observed. The practice of the electronic security is not a unique rather it is a continuous process. The regulatory authority directs CBs and financial institutions regarding type of physical security, infrastructure of systems, system security, and security of online transaction, internal information system audit, training and awareness but didn’t forced to install any particular security mechanism or model followed by banks abroad. So, it is banks’ freedom which type of model bank will be installed in its side.

4.3.4 Ethics of bank HR

“*Ethics are moral standards that help guide behavior, actions, and choices*. Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions). According to Laudon, et al. in most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable.” Business ethics comprises the principles, values, and standards that guide behavior in the world of business.[116]

[116] O.C. Ferrell, John Fraedrich and Linda Ferrel, “*Business Ethics: Ethical Decision Making and Cases,*” (Boston: Houghton Mifflin, 3rd ed., 1997), 7.

Similarly ICT ethics are not exceptional from the above-mentioned view of ethics. In a world where information and communication technology has come to define how people live and work, and has critically affected culture and values, it is important for us to review ethical issues, as well as social responsibility, in the Asia-Pacific region. This is a difficult task because of the diversity in creed, class, caste, dialect, language, culture and race throughout the region. Moreover, the issue of ICT ethics takes on added significance as the region struggles with the dynamics of globalization and the current political environment after the September 11 incident.[117]

So, in spite of taking all possible technological security measures fraudulent transaction or sabotage might be occurred by the employees because of unethical standard or lack of moral principles of banks' executives. Ethics of bank HR is very much concern in this particular field. Conversely, it is said that internal control and compliance is another effective step to control unethical issues in banking sector. Bank cannot stop intentional incident in ICT without ethics. As an integral part of ICT e-banking operation demands today ethical and moral values of banks' HR.

4.4 Conceptual framework

The study encompasses three core issues in broad array i.e. Vulnerabilities, Securities and Secured e-banking. Considering some applicable research techniques and models on e-banking security vulnerabilities, researcher has formulated an innovative conceptual framework for presenting secured e-banking

[117] Tengku Mohd T. Sembok, "Ethics of information communication technology (ICT)," *Regional Unit for Social & Human Sciences in Asia and the Pacific*, UNESCO (November 2003), 5-7.

system of CBs in Bangladesh which is able to reduce simultaneously technological, operational, other related vulnerabilities and attain customer satisfaction and commercial success.

Finally, over this process of model this study attempted to mitigate all possible threats and gain commercial success which is ultimate goal of bank. Researcher mentioned some important variables and indicators relating to the research discussed in detail in methodology section and the relationship or influence among the indicators has been verified in data analysis and interpretation chapter. It is said that related literatures have been reviewed to physique particular variables. This model is presented as a summary of proposed secured e-banking system as e-bankers can follow the model to mitigate core risks for their valued system.

The conceptual framework of secured e-banking is designed for mitigating all sorts of flaws and gain commercial success.

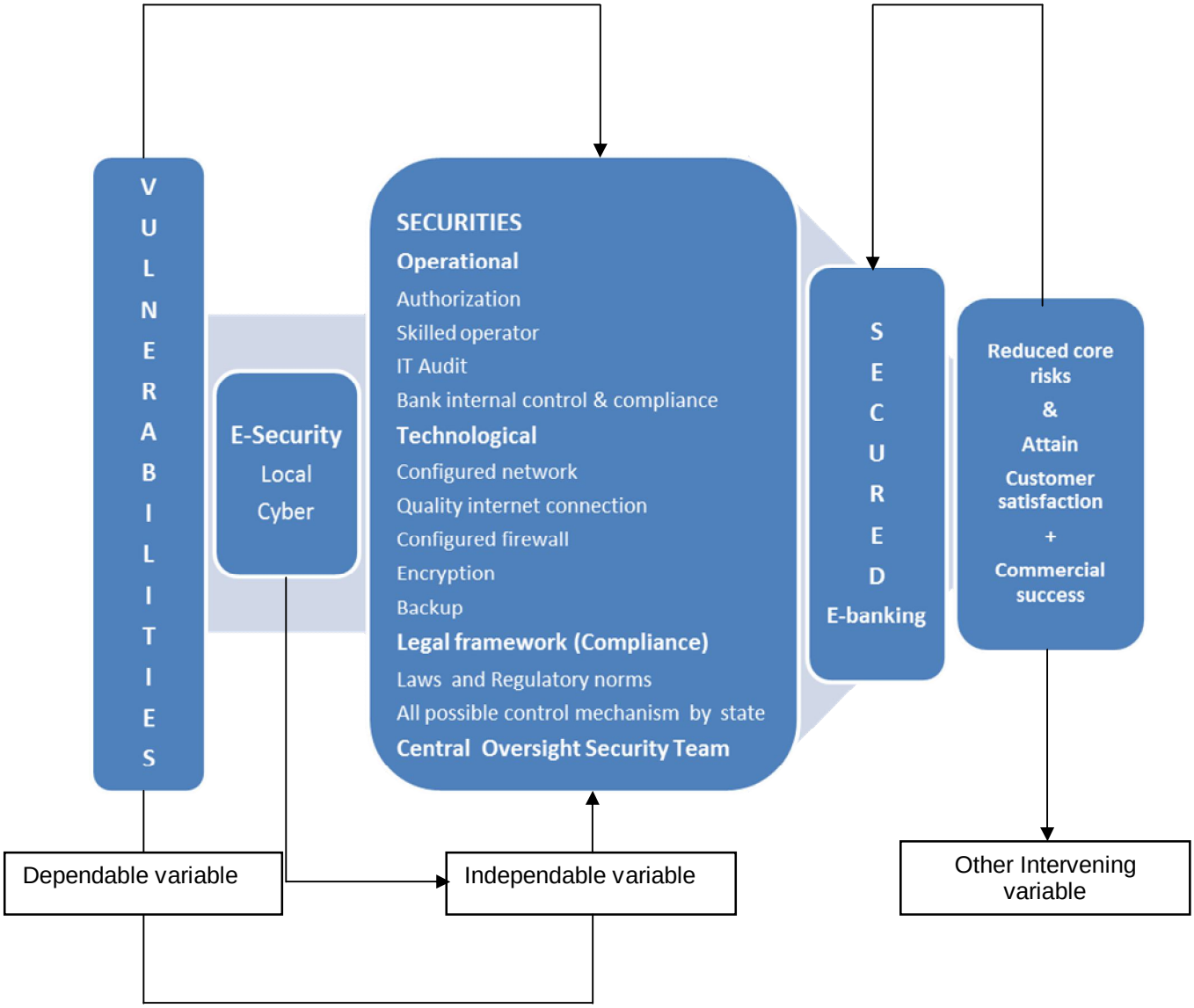


Figure - 4.6

The host study explained that independent variables technological security connotes securities related to hardware and software or services, operational security implies securities related to those resources (i.e. people, process, systems and external events) that are responsible to switch the technology, last of all legal frameworks and compliance signifies major control mechanisms by existing laws and regulations relating to e-banking service security. All those securities cover local and cyber security, through these process bankers obtain secured e-banking which reduce risks and gain commercial success.

Beside dependable variables vulnerabilities imply technological, operational and compliance related weakness. Other intervening variables core risks, customer satisfaction and commercial success depict ultimate e-banking goal through secured e-banking operation.

Securities of e-banking improve core risks, attain customer satisfaction and finally gain commercial success. Yet core risks, customer satisfaction and profitability depend on security vulnerabilities of e-banking. So in this study securities are independent variable and vulnerabilities are dependent variable. Increases of securities improve core risks, customer satisfaction and profitability while decreases of vulnerabilities weakening core risks, fading customer satisfaction and drop profitability.

Conclusion

Conceptual issues are a holistic overview which focuses a complete security package for CBs from their own risk management point of view. This chapter has discussed different sort of vulnerabilities and threats which invite risks for e-banking service, existing security status of banks, security models followed by banks' in different countries across the world and the role of the national - international forum or regulatory authority to e-security. This chapter attempts to make a best quality of security road map (model or mechanism) for e-banking here in Bangladesh which can ultimate make CBs safe and credible in terms of risk management and business success viewpoint.

Chapter V
Laws and Regulations relating to E-banking Security

Introduction

Almost 2500 years ago, the Greek Philosopher, Heraclitus quoted that, there is nothing permanent but change. These words quoted by Heraclitus are ever true today. People are living in a constantly changing world. Advance technology has almost done it. With increasing dependency on advance technology, diverse new threats to the computer network and information (data) security has clearly appeared. People find growing vulnerabilities to cybercrime (electronic crime) in a versatile world. This is also true for the country like Bangladesh where every day the number of advanced technology users are increasing and ICT is inevitable part for the whole economy particularly for the financial institutions like bank, stock market and many others business organizations.

Electronic crime is fast and increasing due to the evolution of technology fast, but the evolution of ICT is fast and the evolution of law is slow.[118] So the adequacy of related laws and regulations against electronic crime is important and mandatory. Similarly it requires a coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery.[119] In banking sector e-banking is an alternative banking channels all over the world. But adequate legal framework and proper security policy are the two essential factors for e-banking (online banking). So, this chapter basically discusses the existing polices, laws and

[118] M. Imran Siddique and Sana Rehman, "Impact of Electronic crime in Indian Banking Sector – An Overview," *Int. J Busi. Inf. Tech* 1, no. 2 (2011):163.
[119] Ibid.,163.

regulations regarding e-banking available in Bangladesh and try to present frequently the needs to enactment new rules of law or amendment of existing laws if necessary.

Before discussing the laws and regulations relating to e-banking, it is necessary to find the different pros and cons and issues relating to e-banking process. In this study researcher focused basically operational, technological and compliance related vulnerabilities (risks) faced by the e-players and how banks mitigate those vulnerabilities by utilizing laws and regulations enacted by the different states or national and international organizations or forums.

This section of study basically focused on the laws and regulations available here in Bangladesh in conducting secured e-banking operation. Simultaneously it was checked the soundness of these laws to protect secure e-transaction among the banks.

5.1 Criminal conducts in cyber space

To make an effective legal framework against cyber crime, business people need to be aware about cyber crime (frauds), its critical nature and how crimes are committed in a virtual world. Today, it is a transnational issue which requires a true strategy to mitigate casualties.

The main factor promoting e-banking frauds are:-

- Global dimensions;
- In adequate or nonexistent laws on national or international level;
- In adequate international co-operation;

- In adequate governmental or public defense system (prevention);
- In adequate staff; and
- In adequate technical support[120]

5.1.1 Cyber-crime (Electronic crime)

Cyber-crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.[121]

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[122] It is a technological crime and a misnomer term. It is also known as computer crime, electronic crime, hi-tech crime and e-crime. Actually it involves a broad range of potentially illegal activities conducted by the misuse of computers and different types of communication networks.[123]

Cyber crime is happened by cyber attacks which generally refer to criminal activities performed via the network or internet. The natures of these particular crimes are a criminal offense regarding the internet, violation of law on the internet, stealing organization's intellectual property or critical information, confiscating online bank accounts, computer and network related fraud and forgeries, creating and distributing viruses on other computers, disrupting

[120] Pooja Pasricha and Sanjeev Mehrotra, "Electronic crime in Indian banking," *Sai Om Journal of Commerce & Management* 1, Issue 11, (November, 2014): 8.

[121] http://study.com/academy/lesson/what-is-cyber-crime-definition-types examples.html (Accessed on: May 17, 2015).

[122] Understanding cybercrime: a guide for developing countries, *ICT Applications and Cyber security Division Policies and Strategies Department, ITU,* draft (April, 2009),17.

[123] Ashiquddin Mohammad Marufd, Rabiul Islam and Bulbul Ahamed*, "*Emerging cyber threats in Bangladesh: In quest of effective legal remedies," *The Northern University Journal of Law* 1, (2010):113.

operation, identity theft, denial of service, stalking victims use of internet, hacking, terrorist use of internet for personal gain or any electronic attack which may cause harm for user as well as the organizational function.

5.1.2 Natures and phenomena

Computer and computer network can be interrupted or suspended through intentional, unintentional or accidental activities. But in the host study intentional crimes or attacks are taken into account. Study found that two common medium of crimes available in virtual world. These are local and cyber crimes by computer and network. Local crimes are internal which mostly took place by insiders and cyber crimes are external conducted from distance location. Malicious, denial of service, web-based attacks, malicious code, phishing and social engineering, stolen devices, viruses, worms, Trojans, malware, botnets and so on are the medium of cyber intruder.

The term “cybercrime” is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences:

i) Offences against the confidentiality, integrity and availability of computer data and systems;

ii) Computer-related offences;

iii) Content-related offences; and

iv) Copyright-related offences.

This above typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: “offences against the confidentiality, integrity and availability of computer data and systems”; content-related offences; and copyright related offences. The fourth category of “computer-related offences” does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as “cyber terrorism” or “phishing”) cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.[124]

Cyber-attacks statistics (April 2015)[125]

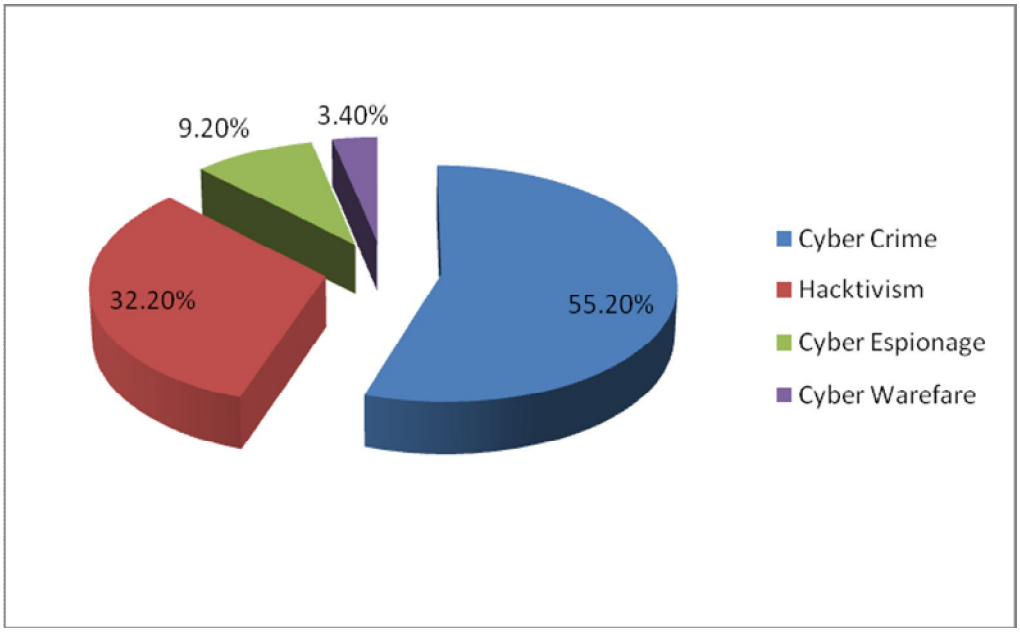


Chart- 5.1

[124] Dr. Marco Gercke,” Understanding cybercrime: Phenomena, challenges and legal response,” *International Telecommunication Union Telecommunication Development Bureau*, Geneva, Switzerland (September, 2012):12.

[125] http://hackmageddon.com/2015/05/12/april-2015-cyber-attacks-statistics/ (Accessed on: January 15, 2016).

On the other hand, “International Survey of Cybercrime Laws: Consensus Crimes”—looks at eight categories of cybercrime:

i) Entering without authority: unauthorized access, hacking, trespass;

ii) Unauthorized destruction, modification, copying or other manipulation of data files;

iii) Computer sabotage;

iv) Unlawful use of information systems: theft of computer time and use of computer systems to commit traditional crimes such as forgery, terrorism, etc.;

v) Computer fraud;

vi) Espionage (industrial, national, security, others);

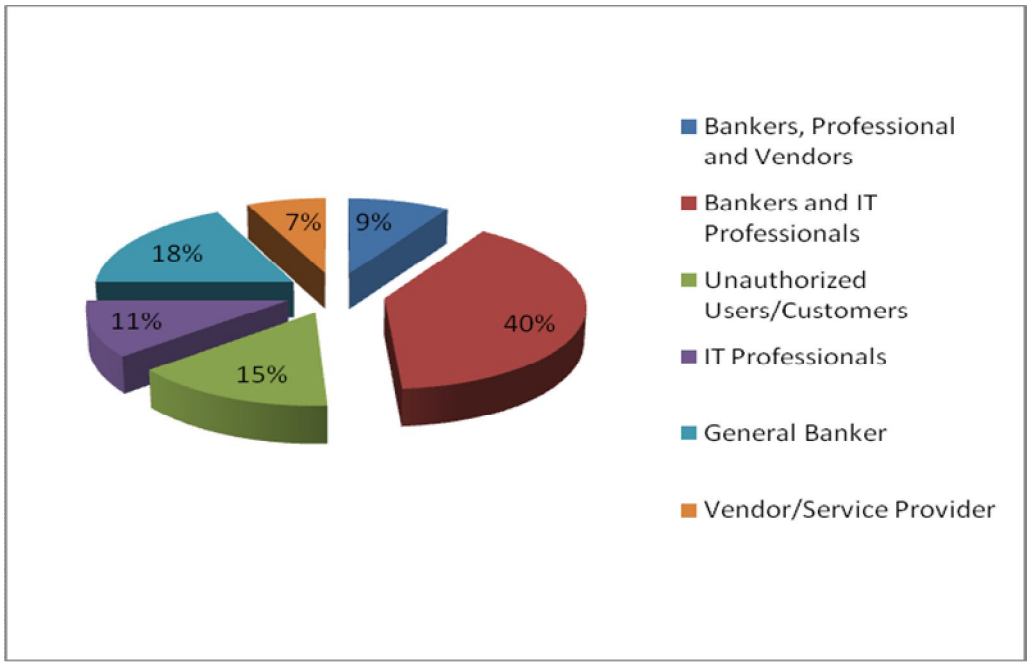
vii) Breach of privacy;

viii) Damage and/or theft of hardware or software.[126]

Category of fraudsters committed financial frauds in banking sector of Bangladesh. BIBM conducted a survey and revealed the picture as shown (Figure-4.2) bellow. In that study, it is also seen that bank employees, either general bankers or IT professionals or both, are involved in 78% cases. A good number of unauthorized external users (15%) are also responsible for online frauds.[127] According to below pie chat fraudulent involvement by bank professionals are seen rigorously very high. This statistics are alarming bank’s senior management as well as board in recent time.

[126] Marc D. Goodman and Susan W. Brenner, “The emerging consensus on criminal conduct in cyberspace,” *Journal of Law and Technology* 6 (2002).

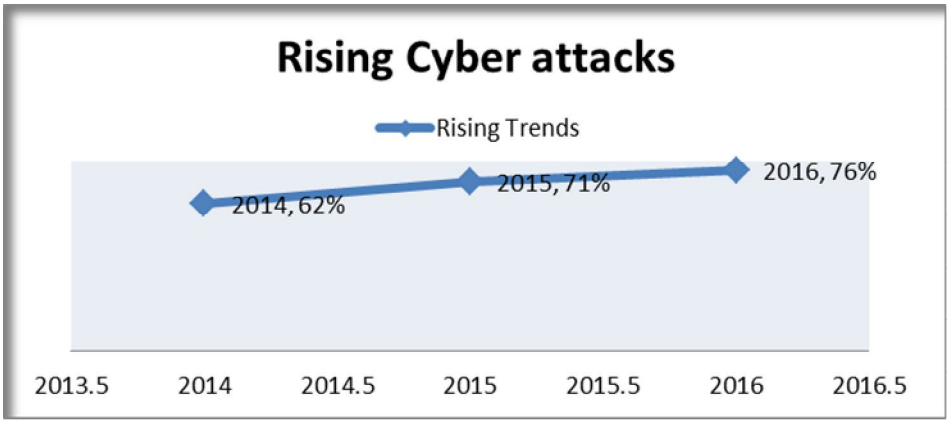
[127] Md. Mahbubur Rahman Alam ,“Online Frauds and Security Issues in Banks,” *BIBM Bulletin* 17, no. 1 & 2, (March and June, 2014).



Source: BIBM survey 2013

Chart- 5.2

There are many true and destructive consequences associated with electronic crime. These are waste of time, loss of reputation, loss of customer's trustworthiness, loss of return and finally it affects more than the financial integrity of a business. Electronic attack results in intangible losses (costs). Now, let us see the rising trend of cyber heist given below:

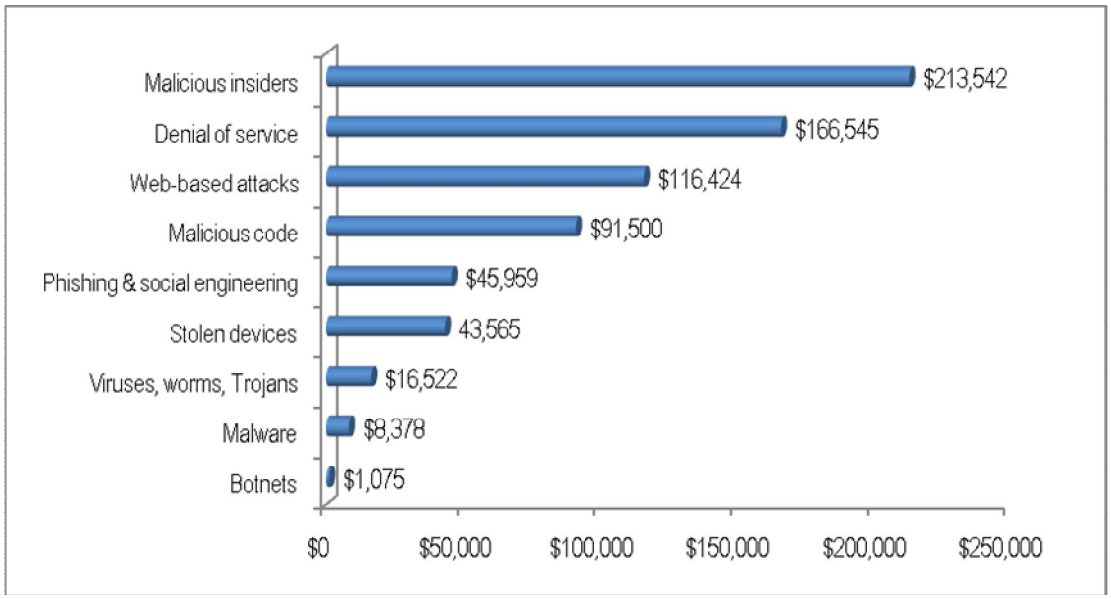


Source: Cyber Edge Group 2016

Chart-5.3

The rising cyber attacks are increasing year by year which costs have raised intensely. A hack and its consequences globally cost hugely. Recently the main target of attackers is financial intermediaries to gain financial advantages. Average annualized cybercrime cost weighted by attack frequency is given below by bar chart.

Cost expressed in US dollars
Consolidated view, n=257 separate companies



Source: Ponemon Institute 2015

Chart- 5.4

The cost of Cyber Crime 2014 is shown above (Figure-4.3). The annual Ponemon research study is out now and unsurprisingly cybercrime continues to be on the rise. The study finds that organizations are seeing more attacks and the cost of these attacks continues to increase. In 2013 there were 1.4 successful attacks per company each week. In 2014 this has risen to 1.7. The most costly cybercrimes are those caused by malicious insiders, denial of services and web-based attacks. These account for more than 55 percent of all

cybercrime costs per organization on an annual basis. The cost is mainly derived from business disruption, information loss and loss of revenue.[128]

5.2 Cybercrime laws and regulations around the World

Laws and regulations are available in different countries to control and punish offender for ICT related crime or attack. E-banking is a process in banking sector rendering services to the customers with the help of ICT technologies. So, any cyber-attack infringes e-banking security.

But readers have a right to know the actual distinction between law and regulation. Laws are the products of written statutes, passed by either the state legislatures. The legislatures create bills that, when passed by a vote, become statutory law. Regulations, on the other hand, are standards and rules adopted by administrative agencies that govern how laws will be enforced.[129] Like laws, regulations are codified and published so that parties are on notice regarding what is and isn't legal. And regulations often have the same force as laws, since, without them, regulatory agencies wouldn't be able to enforce laws.

5.2.1 Laws

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.[130] Nations around the world are very concerned about cybercrime, a

[128] http://jscconsultant.co.uk/cost-cyber-crime-can/ (Accessed on: June 10, 2015).

[129] http://blogs.findlaw.com/law and life/2015/10/ whats the difference between laws and regulations.html (Accessed on: February 5, 2016).

[130]Cyber Crime and Punishment, Archaic Laws Threaten Global Information, MCCONNELL INTERNATIONAL (December 2000)

concern shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe. A number of reasons to be concerned, perhaps the most important being the problems law enforcement officials and prosecutors encounter in trying to apply existing law cyberspace crime.[131] Unlike traditional crime, cybercrime is global crime. As a European Commission report explains, "computer-related crimes are committed across cyber space and do not stop at the conventional state-borders. They can be perpetrated from anywhere and against any computer user in the world.

Since the 1970s, there has been a growing consensus that existing criminal laws covering the variety of crimes that can be committed with a computer either do not cover some computer abuses or are not strong and clear enough to discourage computer crimes and allow expeditious prosecution.[132] Nowadays the scenario has been improving and laws against electronic crime enacted in different countries around the world. But it is noted that somewhere these endorsed laws are still insufficient or inadequate to punish cyber criminal perpetrate in cyber space and it is not much stronger or clear.

It is stated that the first wave of law reform started in most western legal system regarding the protection of privacy, data storing from 1970s to 1997s. Administrative, penal and civil legislation was endorsed to protect data and citizens' right to privacy. After invention of www site cyber-attack is changing its nature and new avenue of attack for intruders were revealed. Computer and network faced difficulties by much unknown attacks. In this circumstance some

[131] Marc D. Goodman and Susan W. Brenner, "The emerging consensus on criminal conduct in cyberspace," *Journal of Law and Technology* 6 (2002): 4.
[132] Ibid., 31.

international and supranational states and organizations have recognized the laws and regulations to provide for offences relating to the misuse of digital devices and experienced the limitations of unilateral approach compare to international harmonization of legal, technical, and other solutions. Now, the study has a look bellow the different laws endorsed by the nation states to protect its data and systems from trespassers.

United States of America

Cybercrime legislation has been adopted at both the state and federal levels. The survey below concentrates on federal legislation, both because of its more general applicability and because the idiosyncrasies of the legislation adopted by the fifty states is quite outside the ambitions of this endeavor.

Denmark

Section 263(2) of the Danish Criminal Code makes it an offense to, “in an unlawful manner,” obtain “access to another person’s information or programs which are meant to be used in a data processing system”. The basic sanction is imprisonment “for a term not exceeding 6 months”, but if the offense is committed with the intent to “procure or make oneself acquainted with information concerning trade secrets of a company or under other extraordinary aggravating circumstances,” the penalty is increased to “imprisonment for a term not exceeding 2 years.”

Section 279 of the Danish Penal Code outlaws using a computer to commit fraud. Specifically, it declares that anyone who, “for the purpose of obtaining for himself or for others an unlawful gain” unlawfully alters, adds or erases “information or

programs for the use of electronic data processing, or who in any other manner attempts to affect the results of such data processing" is guilty of computer fraud.

Sweden

Sweden has made "data trespass" a crime. Any person who unlawfully procures access to a recording for automatic data processing or who unlawfully alters or deletes or inserts such a recording in a file shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years, unless the offence is punishable under the Penal Code. Equivalent to a recording in a file is, in this respect, information being transmitted by electronic or similar means to be used in automatic data processing.

Australia

Australia's Crimes Act 1914 establishes four cyber-offenses: unlawful access to data in Commonwealth and other computers, damaging data in Commonwealth and other computers, unlawful access to data in Commonwealth and other computers by means of Commonwealth facility, and damaging data in Commonwealth and other computers by means of Commonwealth facility.

Iran

A study published in December of 2000 found that Iran had no cybercrime specific laws in place. It noted that "for the past six years Iran has examined various aspects of cyber law including computer offenses, but so far no laws have been adopted. In June of 2001, the Iran Telecommunications Company issued regulations "to filter all materials presumed immoral or contrary to state security, including the Web sites of opposition groups," and to bar Internet access for those under eighteen.

Russia

Russia has developed an extensive legal framework to detect, punish, and prevent computer crime, but implementation remains problematic. Other countries of Central and Eastern Europe have also started addressing cybercrime as part of the larger on-going legal reforms in the region. Romania and Poland have draft laws underway that include computer-related provisions.

Estonia

Estonia recently adopted legislation outlawing computer fraud, sabotage and related offenses. The computer fraud provision makes it a crime to receive "proprietary benefits through entry, replacement, deletion or blocking of computer programs or data" which "influences the result of the data processing operation. The computer sabotage provision makes the "unlawful replacement, deletion, damaging or blocking of data or programs in a computer" and/or the "unlawful entry of data or programs in a computer" a crime if "significant damage is thereby caused". Another provision makes it illegal to disseminate computer viruses; the basic punishment is a fine or up to one year's imprisonment, but if the offense is repeated or is committed "in a manner which causes significant damage" the allowable period of imprisonment rises to three years. Another provision makes it unlawful to damage or block computer network connections. It is also illegal to distribute "the protection codes of a computer, computer system or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences.

South Korea

South Korea has two methods of implementing computer crime laws. They have established numerous articles within their criminal code, which went into effect on July 1, 1996, and they have implemented the Promotion of Utilization of Information and Communications Network Act, which went into effect on July 1, 1999.

Malaysia

Malaysia's cybercrime legislation is contained in the "Computer Crimes Act 1997." The Act creates four offenses: unauthorized access, unauthorized access with intent to commit or facilitate commission of further offense, unauthorized modification of the contents of a computer, and wrongful communication. It also criminalizes aiding and abetting and attempting to commit any of these offenses.

China

The bulk of China's cybercrime provisions are contained in its "Computer Information Network and Internet Security, Protection and Management Regulations", which were promulgated to "strengthen the security and the protection of computer information networks and of the Internet, and to preserve the social order and social stability.

Japan

Japan's cybercrime legislation is contained in two enactments, the "Unauthorized Computer Access Law," and the "Computer Crime Act." The Unauthorized Computer Access Law creates two offenses: unauthorized computer access and facilitating unauthorized computer access. The Computer Crime Act creates five: computer forgery; disrupting the operations of a business computer; computer theft; computer fraud; and destroying computer records. In April of 2002,

Japanese officials announced that they intended to put forward legislation which would criminalize the online transmission of child pornography; while the sale and distribution of child pornography is already illegal in Japan, the law does not outlaw "showing pornographic images of children on websites.

India

India's cybercrime legislation is set out in "The Information Technology Act, 2000". The offenses are set out in Chapter XI of the Act. They include: tampering with computer source documents, unauthorized access, damaging or destroying computer data; publishing obscenity; disclosing confidential information without authorization, publishing a false digital signature certificate, and creating or publishing a digital signature certificate for fraudulent purposes.

Pakistan

Pakistan enacted the PAK Ordinance, which specifically addresses hacking, and virus related offenses. The PAK fails to address obscenity, cyber fraud, intellectual property rights, content filtering, censorship and spamming. Instead, it leaves these offenses to be covered under existing common law. Section 32 of the Pak makes international offenders liable.

Bangladesh

Bangladesh's responses to a United Nations survey on cybercrime law indicate that it has not adopted cybercrime-specific penal legislation. But the country enacted ICT act in 2006 (amended 2013) and going to endorse a cyber-crime law shortly.[133]

[133] Ibid., 90-152.

5.2.2 Regulations & Regulators

Generally, regulation means the guidelines and legal instruction prescribed by the related organizations, regulatory authorities, forums or government. But regulation stands for a rule, principle, or condition that governs procedure, behavior or executive order which is prepared under act.

E-banking is a new distribution channel for banking sector but it also poses new challenges for regulatory authorities in regulating and supervising the financial system within the territory and multinational space. E-banking operation needs clear executive order & regulatory norms from international and national forums or regulatory authorities. Bank for International Settlements, Basel Committee on Banking Supervision, International Telecommunication Union, United Nations and central banks of respected country are the major regulatory forums or organizations for e-banking operation. All those regulatory partners or forums have designed and developed guidelines for e-players in financial service industry around the world. The major regulators in the world are as follows:

Bank for International Settlements

Established on 17 May 1930, the Bank for International Settlements (BIS) is the world's oldest international financial organization. The BIS has 60 member central banks, representing countries from around the world. The head office is in Basel, Switzerland and there are two representative offices: in the Hong Kong Special Administrative Region of the People's Republic of China and in Mexico City.

The mission of the BIS is to serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks. In broad outline, the BIS pursues its mission by:

i) fostering discussion and facilitating collaboration among central banks;
ii) supporting dialogue with other authorities that are responsible for promoting financial stability;
iii) carrying out research and policy analysis on issues of relevance for monetary and financial stability;
iv) acting as a prime counterparty for central banks in their financial transactions; and
v) serving as an agent or trustee in connection with international financial operations.[134]

Basel Committee on Banking Supervision

The Basel Committee is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability.

Each year the Basel Committee sets out its work programme for the next two years. The work programme, which is endorsed by the Governors and Heads of Supervision, serves as a guide for the Committee's policy, supervision and implementation activities.[135] The above two forums have electronic banking guideline for CBs of different countries.

[134] https://www.bis.org/ (Accessed on: May 19, 2015).
[135] http://www.bis.org/bcbs/ (Accessed on: May 19, 2015).

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is the United Nations specialized agency for telecommunications. It was established in 1865 as an impartial, international organization within which governments and the private sectors could coordinate the operation of telecommunication networks and services, and advance the development of information and communication technology (ICT). Today, ITU is also devoting considerable effort to bridging the digital divide and bringing the benefits of ICT to all. ITU Global Cyber security Agenda (GCA) is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is built upon the following five strategic pillars, also known as work areas:

- Legal measures
- Technical and procedural measures
- Organizational structures
- Capacity building
- International cooperation

United Nations

The General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law which is closely related to e-trade or e-finance even with e-banking. The said resolution recommends *inter alia* that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity

of the law applicable to alternatives to paper-based methods of communication and storage of information.

Central banks

Central bank is the monetary authority and major regulatory of bank in a country. Its functions include issuing and managing the country's currency, controlling monetary policy and supervising money market operations, managing exchange and gold reserves, acting as lender of last resort to commercial banks, and providing banking services to the government. Central banks are state-controlled but are increasingly being given an independent status.[136] These central authorities also supervise and monitor e-player's activities in banking industry of their respected country by their own framed regulations.

As an influential forum European central bank recommended for the security of internet banking and the bank has conducted a survey received upon 59 respondents in 17 European Union countries and included both European and national associations and authorities.[137]

Like many others, issues were also raised with respect to data protection legislation. The European central bank believes that the processing and exchange of data on suspicious transactions, IP addresses and accounts is necessary in order to detect, analyze, prevent and stop malicious attacks on internet payment infrastructures. It also facilitates the reversal of fraudulently initiated payments. Any processing and exchange of such information must, of

[136] http://lexicon.ft.com/Term?term=central-bank (Accessed on: May 19, 2015).

[137] European central bank, *recommendation of the security of internet payments: outcome of the public consultation* (January, 2013)

course, take place in a secure environment and between trusted and duly identified parties.[138]

Except above mentioned international and national regulators, some important summit sets to sign executive order to mitigate cybercrime like regulatory bodies. The summit on Cyber security at Stanford University in California held at the second month of this year. The President of USA Barack Obama discussed cyber security with world famous tech-bosses namely Apple's Tim Cook and many others.[139] On the other hand, Commonwealth telecom body's meeting held in Dhaka last September 2014. Bangladesh was hosted the 54th council meeting and annual forum of Commonwealth Telecommunications Organization (CTO) for the first time. The CTO council meeting and forum would promote, facilitate and guide members in using ICT to deliver effective development intervention, Brig Gen Golam Mowla Bhuiyan, BTRC director general, said at a briefing. The present strategies emphasized six main areas where cyber security and cybercrime is the important one.[140]

5.3 Computer forensics and organizational audit

Generally computer forensics is the application of investigation and analysis techniques to collect and preserve evidence from a particular digital device.

Computer forensics is used to bring to justice, those responsible for conducting attacks on computer systems throughout the world. Because of this the law must be follow precisely when conducting a forensics investigation. It is not enough to

[138] Ibid., 3.
[139] *bd24live.com*, February 14, 2015, 1.
[140] "Commonwealth telecom body's meeting in Dhaka in sept," *The Daily Star*, 13 June 2014, Sec. B, 1.

simple know an attacker is responsible for the crime, the forensics investigation must be carried out in a precise manner that will produce evidence that is amicable in a court room. For computer intrusion forensics many methodologies have been designed to be used when conducting an investigation. A computer forensics investigator also needs certain skills to conduct the investigation. Along with this, the computer forensics investigator must be equipped with an array of software tools.[141]

Computer Forensics can further be defined as the application of computer investigation and analysis techniques in the interest of determining potential evidence, which might be sought in a wide range of computer crime, or misuse, including but not limited to theft of trade secrets, theft or destruction of intellectual property, and fraud.[142] Robbins, a computer crimes specialist and investigator said that "Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence."

New Technologies Inc. expands on Robbins' definition. "Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information (data).[143]

According to Robbins the key here is "potential legal evidence." The data obtained by a related investigator must be able to hold up under the scrutiny of a court of law to be useful. An investigator must keep in mind and assume that any

[141] Nathan Balon, Ronald Stovall and Thomas Scaria, "Computer Intrusion Forensics," 1.
[142] Robbins, Judd. "An Explanation of Computer Forensics,"
[143] http://www.giac.org/paper/gsec/559/computer-forensics-overview/101340 (Accessed on: May 25, 2015).

and all evidence discovered which accuses an individual as guilty of a crime, will end up in court and be subject to intense analysis and scrutiny by the defense counsel. So, forensics is not a subject for investigation or analysis technique only, but the result of investigation should be preserved and documented in a good condition as it is useful in the court room for punishment the guilty.

On the contrary, generally audit means systematic examination and verification of a firm's books of account, transaction records, other relevant documents, and physical inspection of inventory and qualified accountants or auditors. The motto of audit is an organization's risk management, governance and internal control processes as it is operating effectively. But IT audit can be defined as any audit that encompasses review and evaluation of automated information processing systems, related non-automated processes and the interfaces among them.144 So, organizational audit relating to the ICT is simply stand for examination and verification of automated information processing systems and infrastructures according to the legal instruction prescribed by organization. Organizational legal issues are involved here.

5.4 Adequacy of laws and regulations in Bangladesh

The purpose of this branch of study is to focus mainly on the availability of laws and regulations for the smooth operation of e-banking in Bangladesh. The Bangladeshi banking system has been facing difficulties from electronic fraudulent and crime by the insiders and outsiders which invite legal or compliance risks for banks as well as customers. In Bangladesh, the central bank

[144] http://resources.infosecinstitute.com/itac-planning/ (Accessed on: July 29, 2015).

recognized some acts as a banking operation acts for banks. Beside some regulations and guidelines are designed to control and regulate country's financial system. It is said that after adoption of e-banking as a new delivery channel central bank developed and prescribed some of these regulations and guidelines or regulative tools for e-players in banking industry. But some existing laws and regulations still facilitate paper based transactions which apparently are not applicable today to technological changes. It should be acquainted as per requirement of e-banking nature and culture. So it demands amendment or new act endorsement in a changing virtual environment. Update technology, reliable human resources and devices are merely not the solution here, because security fears exist for both banks and in the mind of customers. So, effective laws and regulations in this regard are very much important. Time has come to enact new laws or revise existing laws and regulations to regulate properly the e-players in Bangladesh.

The two important legal issues are subject to discuss here regarding e-banking operation. One is *"laws n acts"* and another is *"regulations n guidelines"* of central bank designed by their own. A set of acts, laws, regulations, and guidelines have been enacted and promulgated time to time since Bangladesh Bank's establishment which helped it to perform its role as a central bank particularly to control and regulate country's monetary and financial system. Among others, important laws and acts include[145] Bank Company Act 1991, The Negotiable Instruments Act, 1881, The Bankers' Book Evidence Act, 1891, Foreign Exchange Regulations Act, 1947, Financial Institutions Act, 1993, Money

[145] http://www.bangladesh-bank.org/aboutus/regulationguideline/lawsnacts.php (Accessed on: May 13, 2015).

Laundering Prevention Act, 2012, Anti-terrorism Act, 2009. In all above mentioned laws there is no single provision that carter for the use of electronic banking operation in Bangladesh despite the fact that there were enacted during the era of electronic banking. Actually ICT act, 2006 is legitimate for e-banking operational security. Very few section of this act discussed punishment against cyber crimes or heist. But it is merely not possible to cover all the things by executing just only one act. In order to control cyber crime at an affordable mark country needs to enact one specific cyber law to punish cyber offences. National Cyber security Strategy prioritized on legal measures to mitigate security threats which will be a comprehensive set of national cybercrime legislation that is regionally and globally applicable and harmonized.[146]

Except above mentioned laws or acts some more important regulations and guidelines are Guideline on ICT security for banks and financial institutions, 2010, Risk Management Guidelines for Banks, 2012, Regulations on Electronic Fund Transfer 2014, Bangladesh Payment and Settlement Systems Regulations 2014, BEFTN operating rules and so on. It is said that President's order no.127 of 1972 (Bangladesh Bank Order, 1972) are also considered as important regulation focusing basically on central bank's nature, functions, scope, responsibilities etc.

Further it is argued that operation of banking through electronic medium should be accompanied by adequate and effective legal framework.[147] In banking industry difficulties is every day story for e-players. Some major laws or acts are still not

[146] Information and Communication Technology Division, *The National Cyber security Strategy of Bangladesh* (March 03, 2014)

[147] Mayonga Nguhecha and Shepo M. John, "Law relating to e-banking in Tanzania: an analytical overview of data protection in e-banking," (University of IRING, Tanzania, 2014), 35-37.

adequate (with changing nature of e-banking) to mitigate e-banking security. Divergently some specific lawful regulations or guidelines appear to be frail.

Laws like The Negotiable Instruments Act, 1881, The Bankers' Book Evidence Act, 1891, and ICT act, 2006 seem to be inefficient or insufficient here in Bangladesh. Simultaneously existing regulations or guidelines can be updated in accordance to new difficulties (vulnerabilities).

5.5 Comparative discussion on existing laws and regulations

With this changing environment many countries around the world amended or enacted the laws and upgraded their regulations relating to e-banking. In India related laws have already been amended and given very clear explanations for particular clauses to lawful solutions. India amended The Negotiable Instruments Act, 1881, The Bankers' Book Evidence Act, 1891, and IT act, 2000 to recognize electronic transactions significantly. Amendments of above mentioned laws in India are discussed below:

The Negotiable Instruments Act, 1881

In chapter II of N I Act, 1881 defined "cheque"- A "cheque" is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on demand. (Section-6)

Substitution of new section for section 6 (passed by Lok Sabha the lower house of parliament of India on 21 November 2002)

"A "cheque" is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on and it includes the electronic image of a truncated cheque and a cheque in the electronic form."

The Bankers' Book Evidence Act, 1891

Section 2 of (3) defined "Bankers' books"- "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank.

Substitution of new section for section 2 of (3)

"Bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device.

IT acts, 2000

Section.2 Definitions

Section 2(1) *(f) "asymmetric crypto system"* means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(r) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(x) *"key pair"* in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(z) *(zc) "private key"* means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorized access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(ze) "secure system" means computer hardware, software, and procedure that—
(a) are reasonably secure from unauthorized access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Section.3 Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be affected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.— For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known' as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Section.4 Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

Later the act amended in 2008 and inserted the term *"communication device"* means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.- section 2(h) (ha) of IT (amendment) act, 2008

"cyber security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.- Section 2(nb) of IT (amendment) act, 2008.

So, specific regulatory and legal challenges include laws and regulations governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and Reserve Bank of India (RBI) continues to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships. Some of the legal requirements and regulatory guidance that frequently apply to e-banking products and services have been issued by RBI in its notification on 14th June,

2001, which were the findings of a working group on internet banking[148] (then on information security in 2011) like India many countries in the world have been enacted and timely revised specific laws and regulations for e-banking in a changing electronic era.

On the other hand in Bangladesh, the Negotiable Instruments Act, 1881, The Bankers' Book Evidence Act, 1891, ICT act 2006 amended frequently but it didn't knock those particular sections which are associated directly with e-banking operation and its security. Still the Negotiable Instruments Act, 1881, The Bankers' Book Evidence Act, 1891, facilitate paper based transactions which apparently are not applicable to technological changes or electronic transactions that are currently taking place in Bangladesh.

Rather, Bangladesh doesn't have any cyber law. The Bangladesh Computer Security Incident Response (BD-CSIRT) is entrusted with protecting websites of government and other organizations from cyber-attacks but its capacity is limited. The Bangladesh Telecommunication Regulatory Commission (BTRC) and ICT division of Ministry of ICT has combinely planned to prepare a long-term cyber security strategy to protect computers, networks, programmes and data from unintended access and destruction. Mustafa Jabbar, former president of Bangladesh Computer Samity (BCS) said that existing cyber security is very vulnerable and fragile, which might lead to disaster anytime in future. Country's financial institutions including banks are vulnerable to possible cyber-attack. The IT analyst suggested that presently the government is following ICT act to deal

[148] Virender Sing Solanki, "Risks in e-banking and their management," *International Journal of Marketing, Financial Services & Management Research* 1, Issue 9 (2012):169-170.

with the cybercrime, which is not desirable. So that government should enact a cyber-security law immediately, taking the opinion of all parties including experts into account.[149]

ICT act of Bangladesh does not define what the cyber law by any section is. But cyber laws are contained in the ICT act 2006. Therefore this act present the legal infrastructure for e-commerce and others legal solution relating with cybercrime in Bangladesh. Rather sections and clauses of ICT act, 2006 is not so obvious or distinct from technical viewpoint. The country further amended ICT act 2006 last 9 October 2013 where it amended section 54 (2), which increased punishment (imprisonment) from 10 years to 14 years for cyber offences and according to section 76 (2) ka (K) & kha (L) offences mentioned in section 54, 56, 57 & 61 would be considered as cognizable and non-eligible for bail. But sections or clauses regarding security mechanism like the term “asymmetric crypto system”, “public and private key”, “secure system”, “security procedure” , “communication device”, “cyber security” and so on didn’t mention and explain clearly as section 2(1) *(f),* 2(4) z *(zc), (zd), (ze) & (zf)* of IT act, 2000 and 2(h) (ha) and (nb) of IT (amendment) act 2008 of India or other country’s act mentioned clearly in their respective ICT act. Study found that in Bangladesh many laws and regulations have evolved to regulate and control e-banking operation but it seems to be insufficient, inadequate and unsupportive in term of security viewpoint for both bank and customer. So, legal requirement on e-banking is today’s demand to fulfillment of consumer legal expectations.

[149] “Plan to craft strategy as cybercrimes crank up,” *The Financial Express*, 14 May, 2015, Sec. Trade & Market, 17.

Above comparative discussion between India and Bangladesh on adequacy of laws and regulations relating to e-banking transactions or securities demonstrated that it looks upon as inadequate in Bangladesh and it is a high time to think about it. In our country most of the customers inadequately inform their rights and obligations about electronic transactions. So to protect customer data special act like data protection act or any such law can be endorsed which could ensure secure data integrity, store, disclosure and privacy. A data protection authority will be replaced through this type of acts. So the law must keep alongside each other of technological changes as they affect the way of doing business here in Bangladesh.

In Bangladesh central bank has introduced Bangladesh payment and settlement system regulations 2009 (revised on 2014) for all electronic transactions including cross border transactional activities and prepared an ICT security guideline for CBs and FIs (while India passed a bill on 20th December 2007 in their parliament "the Payment and Settlement Systems Act, 2007" as an act). Through this payment and settlement systems regulations the central bank of Bangladesh has clearly defined electronic transactions and instrument's electronic nature. In this regulation it mentioned "*Cheque Image*" means a digital representation of the front and back of a cheque. [Section 3(5)], *"Electronic Fund Transfer"* means any transfer of funds which is initiated by a person by way of instruction, authorization or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfer initiated by telephone, internet and card payment [Section 3(8)] and "*Cheque Truncation and*

Electronic Cheque Image Presentment" Bangladesh Bank shall issue rules, procedures, guidelines and operating directives under these regulations that will govern paper-based payment items and other instruments that are eligible for truncation and electronic cheque image presentment. The purpose of imaging, image exchange and the transmission of electronic information between and among banking companies is to improve the efficiency of cheque clearing in Bangladesh (Section-7).[150] To do so Bangladesh Bank shall have jurisdiction to grant payment systems, Payment System Operator (PSO) and Payment Service Provider (PSP) licenses for the operation of payment systems and payment services in Bangladesh. The central bank shall have jurisdiction to authorize certain cross-border payment system activities whose operations affect payment systems in Bangladesh (Section-4) and for violation of conditions of a license, the bank may direct a licensed Payment System Operator or Payment Service Provider to compensate an aggrieved party or may impose financial penalty [Section-5 (a)]. The regulation is given indication of ATM business. In its section 3(1) mentioned "Automated Teller machine" is an electromechanical device that permits authorized users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services, such as balance enquires, transfer of funds or acceptance of deposits, etc. In order to ensure the access of unbanked people by taking advantage of countrywide mobile network coverage, Bangladesh Bank has brought out Guideli ne on Mobile Financial Services (MFS) for the Banks as an operating guideline for adoption by the CBs doing mobile (Cell phone) banking business. From legal and regulatory perspective, only the bank-led model will be allowed to operate.

[150] Bangladesh Bank, Bangladesh Payment and Settlement Systems Regulations, 2009

Here bank-led model shall offer and alternative to conventional branch-based banking to unbanked population through appointed agents facilitated by the Mobile Network Operator's/Solution Providers[151] In this regard, things are very risky to operate "Mobile Account" without account and each customer seeking to avail mobile financial services with all the required documents (KYC, TP etc.). All these electronic procedures have been performing via The Bangladesh Electronic Funds Transfer Network (BEFTN) introduced for participating banks in the EFT Network and the EFT Operator (BEFTN) will be inter-connected via communication links.

The host study found that regulations and guidelines of e-banking securities are not much explained and relevant compare to present acts here in Bangladesh. The country didn't amend Section 2 of (3) of The Bankers' Book Evidence Act, 1891 or section 6 of The Negotiable Instruments Act, 1881 but imposed similar regulations for e-banking operation and security by the regulatory authorities.

But it must be said that initiative from government side over national security on ICT infrastructure (technological and legislative) is a today's demand. Study found that legislative initiatives have already started. Information Security Policy Guideline, Bangladesh has recognized by the government and In its preamble point it out that the government sector has faced number of cyber-attack incident (e.g. web defacement, information damage, information theft, Distributed Denial of Service, etc.). In most of the case the reasons are lack of information protection procedure, weak and unmanaged security controls and under skilled personnel and lack of expertise. Currently, there are no preventive, reactive,

[151] Bangladesh Bank, Guideline on Mobile Financial Services (MFS) for the Banks

detective and administrative security measures to protect digitized government resources. To protect digitized government resources from unauthorized access, this is fundamental requirement to have proper security policy and implementation mechanism in place.[152] According to the national security guideline each and every public sector organizations those are in electronic process shall have their own IT policy to ensure security and privacy of data and systems.

Conclusion

In developing countries, like Bangladesh, nowadays, e-crime or attack is a truly problem for banking industry. Lack of professional knowledge to investigate the crime and unsupportive legal framework is another distress for bank and customers. Hence it requires a genial cooperation and coordination measures on the part of the bank, customers and country's law enforcement machinery (government) to incorporate it properly. It is a due diligence to the government as financial intermediaries of the country can take steps on the basis of genuine acts.

[152] Ministry of ICT, Government of the People's Republic of Bangladesh, *Information Security Policy Guideline, Bangladesh.*

Chapter VI
Data Analysis, Interpretation and Findings

Introduction

This chapter basically comprised the results of data analysis, interpretation and findings of the study. Each hypothesis is being empirically tested applying Pearson's Chi-square (X^2) test and Pearson's Correlation Coefficient (r) test to find the relationship among the variables through SPSS software. It can be a positive or negative relationship, as long as it is significant. Testing results of five drawn hypotheses and to meet core objectives of the study data is carried out in two phases. The first phase, which is based on the questionnaire, the results of frequency distribution tables collected first hand data from respondents. The second, which is also based on the questionnaire, deals with a quantitative manner were tested by Chi-square and Correlation Coefficient. The purpose of this study was to identify whether the system 'e-banking process' is vulnerable or not and which factors are affecting security vulnerabilities of e-banking services.

6.1 Frequency Table

A frequency table (distribution) is most simple way to present the number of occurrences of a particular value or characteristic. After completion of data collection it is to organize in a meaningful form so that data can be presented easily and in a meaningful way.

These tables discussed the important e-banking securities flaws and other related issues using percentage distribution of the respondents from different directions which are very simplest way to understand the obtainable result.

Phase: I

6.2 Frequency tables of SBL

Table: 6.2.1 Percentage distribution of the respondents of major security used as banking software.

What are the major securities that used in your banking software?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	First Factor Authentication	38	76.0	77.6	77.6
	Second Factor Authentication	10	20.0	20.4	98.0
	Third Factor Authentication	1	2.0	2.0	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
Total		50	100.0		

From the above table, 76% respondents used one factor authentication as the major security of their banking software and about 20% respondents used second factor authentication as the major security of their banking software. Considering this factor, system seems to be vulnerable.

Table: 6.2.2 Percentage distribution of the respondents of second factor authentication guarantee 100% protection against theft of user credentials.

Do you think second factor authentication guarantee 100% protection against theft of user credentials?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not sure	23	46.0	50.0	50.0
	No	5	10.0	10.9	60.9
	Yes	18	36.0	39.1	100.0
	Total	46	92.0	100.0	
Missing	System	4	8.0		
Total		50	100.0		

Table result implies that about 46% respondents who were not sure about two factor authentication guarantee 100% protection against theft of user credentials and about 10% respondents told that second factor authentication didn't ensure 100% guarantee against theft of user credentials and about 36% respondents opined that two factor authentication guarantee 100% protection against theft of user credentials. Result found that some bank people has on sufficient technological knowledge regarding this matter. Hence, lack of technological knowledge demonstrated the existing system is not safe and secured.

Table: 6.2.3 Percentage distribution of the respondents type of authentication that bank use.

What types of authentication do you use?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Service (Software)	24	48.0	52.2	52.2
	Hybrid (Combination of hardware and software)	22	44.0	47.8	100.0
	Total	46	92.0	100.0	
Missing	System	4	8.0		
	Total	50	100.0		

The result shows that about 48% respondents were used as authentication tool and the rest 44% respondents used combination of hardware and software as authentication tool. Comparatively the system is secured.

Table: 6.2.4 Percentage distribution of using antivirus software in every single PC.

Did you install antivirus software in every single PC?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Just installed after purchased from vendor	14	28.0	28.0	28.0
	Configured correctly after purchased from vendor	36	72.0	72.0	100.0
	Total	50	100.0	100.0	

Result indicates that about 72% respondents configured correctly after purchased from vendor and the rest 28% respondents inform the just installed antivirus in every single computer after purchased from vendor without configuration. From this particular point of view, the system is comparatively secured.

Table: 6.2.5 Percentage distribution about type of network use in delivering services to the bank customer.

What type of network you use for delivering your services to the customer?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Internet	5	10.0	10.0	10.0
	VPN	39	78.0	78.0	88.0
	PN with encryption	6	12.0	12.0	100.0
	Total	50	100.0	100.0	

Above table represents that about 78% respondents told that they used VPN for delivering their services to the customer where 12% used private network with encryption and the rest 10% respondents used internet. VPN is more secured than open internet.

Table: 6.2.6 Percentage distribution about Performance of internet connection.

What about the performance of your internet connection?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Slow response	5	10.0	10.2	10.2
	Have a little bit problems	44	88.0	89.8	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
	Total	50	100.0		

Above distribution table illustrates that about 88% informed internet connection had little bit problem and the rest 10% respondents opined that internet connection was slow. So, the system appears to be vulnerable.

Table: 6.2.7 Percentage distribution about to use of network protocol security suit like IPSec or SSL or any digital certificate by bank

Do you use network protocol security suit like IPSec or SSL or any digital certificate?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	25	50.0	51.0	51.0
	Yes	24	48.0	49.0	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
	Total	50	100.0		

The result implies that about 50% respondents told they did not use digital certificate or network protocol security suit like IP Sec or SSL. Hence, opinion of majority proved that their web site or communication system has technological weaknesses to gain unauthorized access.

Table: 6.2.8 Percentage distribution about the solutions to the security issues for securing end-to-end transaction.

What are the solutions to the security issues for securing end-to-end transaction?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Software-based solutions involve the use of encryption	22	44.0	48.9	48.9
	Hybrid (Combination of hardware and software)	23	46.0	51.1	100.0
	Total	45	90.0	100.0	
Missing	System	5	10.0		
	Total	50	100.0		

Above table represents that about 46% used hybrid system to secure end-to-end transaction and the rest 44% respondents opined that bank use software-based solutions.

Table: 6.2.9 Percentage distribution about installation of recovery tools (e.g. Acornis) in bank PC.

Have you installed any recovery tools (e.g. Acornis) in bank PC?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	31	62.0	62.0	62.0
	Yes	19	38.0	38.0	100.0
	Total	50	100.0	100.0	

Total 62% respondents spoke that bank didn't use any recovery tools to retrieve data and the rest 38% told that they used recovery tools. So, damaging operating system may cause harmful for the system and the system looks to be vulnerable.

Table: 6.2.10 Percentage distribution about checking and cleaning branch computer and other digital devices (physical security)

Do you clean and check branch computer and other digital devices regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	When problem occurred	22	44.0	44.0	44.0
	After 6 months	12	24.0	24.0	68.0
	Regularly	16	32.0	32.0	100.0
	Total	50	100.0	100.0	

About 44% respondents stated that bank checked physical security of hardware when problem occurred, other 32% opined that it was checked on regular basis and the rest 24% informed that it was checked six months basis. Regular basis trouble shooting is more secured in this regard.

Table: 6.2.11 Percentage distribution about data transmition from one location to another.

In which form your data transmit from one location to another?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Plain text	26	52.0	52.0	52.0
	Cipher text (encryption)	24	48.0	48.0	100.0
	Total	50	100.0	100.0	

The result interpreted that about 52% respondents addressed that data transmit from one location to another as plain text. On the other hand, 48% opined that it transmits in the form of cipher text (in the form of encryption). Hence, it is very risky to transmit valued data without encryption.

Table: 6.2.12 Percentage distribution about data backup

In which device do you use to take data backup regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	In the server only	5	10.0	10.0	10.0
	In the secondary device (DVD/Pen drive/Any other device)	6	12.0	12.0	22.0
	Combination of two	39	78.0	78.0	100.0
	Total	50	100.0	100.0	

According to the above table, about 10% respondents stored their data backup into the server only. Other 12% stored in the secondary device. However, the rest 78% kept their data backup in both the server as well as in the secondary device.

Table: 6.2.13 Percentage distribution about devices used to preserve data backup.

In which site you preserve your data backup?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Inside of branch	2	4.0	4.0	4.0
	Outside of branch	12	24.0	24.0	28.0
	Combination of both	36	72.0	72.0	100.0
	Total	50	100.0	100.0	

From the above table, it is found that about 72% respondents specified they preserve backup data both inside and outside of branch of the bank for data security. The table also represented that only 4% kept their data in his own bank office. On the other hand, 24% preserved their data outside bank. Here, system seems to be secured.

Table: 6.2.14 Percentage distribution about retrieve of data backup process.

How do you retrieve backup data?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Never	16	32.0	32.7	32.7
	After three months	14	28.0	28.6	61.2
	In every month	19	38.0	38.8	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
	Total	50	100.0		

From the above table it is shown that 32% bankers never retrieve or check their backup data. 28% do their job after three months and 38% in a month. It appears serious mistake from operational point of views. So, the system can be faced critical problem.

Table: 6.2.15 Percentage distribution about disaster recovery site.

Where is your disaster recovery site?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	At HO premise	11	22.0	22.0	22.0
	Outside of bank premise	39	78.0	78.0	100.0
	Total	50	100.0	100.0	

The results of the above table represent that 78% bankers are interested to preserve their data for security outside of bank premise or building considering disaster period. On the other hand, 22% do the same in the head office building. It is good practice for bank people.

Table: 6.2.16 Percentage distribution about customer access in computer enclave.

Can customer get access easily in your computer enclave?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	13	26.0	26.0	26.0
	Depend	19	38.0	38.0	64.0
	No	18	36.0	36.0	100.0
	Total	50	100.0	100.0	

The table represents that 26% customer can get easily access in the computer enclave or room, 38% customer can go computer room depending on situation and 36% cannot get access in the computer room of the bank. So, it appears little bit vulnerable.

Table: 6.2.17 Percentage distribution about installation of CCTV in branch to detect fraud and forgeries.

Did you install CCTV in all important branches to detect fraud and forgeries?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, it is available at few branches	33	66.0	66.0	66.0
	Yes, it is available at all branches	17	34.0	34.0	100.0
	Total	50	100.0	100.0	

From the above table the opinion of the 66% respondents are very few branches installed CCTV. The remaining 34% respondents informed that the CCTV is available in every branch. It's a bad practice which cannot track fraud and forgeries in branch location.

Table: 6.2.18 Percentage distribution about communication failure.

Does branch face any communication failure during distance transactions?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, most of time	5	10.0	10.0	10.0
	Yes, sometime	45	90.0	90.0	100.0
	Total	50	100.0	100.0	

The result of frequency distribution table depicts that about 90% respondents opined they faced communication failure sometime during distance transactions and the rest 10% stated branch faced communication failure most of time during distance transactions. It's a vital error which can be lost bank reputation.

Table: 6.2.19 Percentage distribution about short and test audit on branch IT infrastructure.

Do you conduct short and test audit on branch IT infrastructure in branch level regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	10	20.0	20.8	20.8
	Yes	38	76.0	79.2	100.0
	Total	48	96.0	100.0	
Missing	System	2	4.0		
	Total	50	100.0		

From the above table the researcher found that 76% cases occur short and test audit. The event does not occur at the 20% branches.

Table: 6.2.20 Percentage distribution about IT audit conducted by whom.

Who conducts IT audit?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	General executives	12	24.0	24.5	24.5
	IT executives	9	18.0	18.4	42.9
	Combination of two	28	56.0	57.1	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
Total		50	100.0		

It is shown from the table that 24% audit are conducted by the general officer, 18% are conducted by the IT officer and 56% audit are conducted by combining the general and the IT officer.

Table: 6.2.21 Percentage distribution about ICT security check list.

Do you have any ICT security check list to maintain security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	5	10.0	10.0	10.0
	Yes	45	90.0	90.0	100.0
	Total	50	100.0	100.0	

The result indicates that 90% use ICT security check list to maintain security and 10% do not use ICT security check list to maintain security. System seems to be secured.

Table: 6.2.22 Percentage distribution about checking of specific software security system by audit team.

Do you check IT banking specific software security system (e.g. Officers' User name and password nomination, cancelation, password change timely, database security, network security etc.) by audit team?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	10	20.0	22.2	22.2
	Yes	35	70.0	77.8	100.0
	Total	45	90.0	100.0	
Missing	System	5	10.0		
Total		50	100.0		

The result of the above table represents that 70% are inquired by audit team and 20% are not.

Table: 6.2.23 Percentage distribution about checking of branch daily transaction list.

Do you check daily transaction list of branch after transaction?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, we don't check	1	2.0	2.0	2.0
	Yes, we check by IT operation officer	16	32.0	32.0	34.0
	Yes, we check by other officers	33	66.0	66.0	100.0
	Total	50	100.0	100.0	

The result interprets that 2% didn't check daily transaction list, 32% checked daily transaction by the IT officer and 66% checked daily transaction other than IT officer. It's, a good practice for bank people thus the transaction can be comparatively safe.

Table: 6.2.24 Percentage distribution about sending IT experts to monitor ATM booth

Do you send IT experts to monitor ATM booth during servicing by the vendor?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	21	42.0	48.8	48.8
	Sometime	19	38.0	44.2	93.0
	Regularly	3	6.0	7.0	100.0
	Total	43	86.0	100.0	
Missing	System	7	14.0		
Total		50	100.0		

According to the table, 42% bankers didn't send IT experts to monitor booth during servicing by the suppliers. 38% sent sometimes and only 6% did it regular basis. That means the trend is not good for security of booth. It appears the system bearing risks to skimming or any other frauds by ATM.

Table: 6.2.25 Percentage distribution about system vulnerabilities.

You think your system has no vulnerabilities at all?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	A little bit vulnerabilities	45	90.0	90.0	90.0
	Yes, no vulnerabilities	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

Respondent's perception about system vulnerabilities found that 90% were faced little bit vulnerabilities and the rest 10% is not. It is proved that system has been facing problems and it is almost not secured.

Table: 6.1.26 Percentage distribution about security measures taken by bank

Do you have sufficient security measures to render services?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, not sufficiently, it is necessary	38	76.0	76.0	76.0
	Yes, absolutely	12	24.0	24.0	100.0
	Total	50	100.0	100.0	

Result shown that about 76% stated it is not sufficient and according to the rest 24% it has absolute security initiatives. Statement shown that system sensibly seems to be vulnerable.

Table: 6.2.27 Percentage distribution about impact of vulnerabilities on business profitability

Do you think that security vulnerabilities have impact on your business profitability?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	5	10.0	10.0	10.0
	Yes, moderately	28	56.0	56.0	66.0
	Yes, strongly	17	34.0	34.0	100.0
	Total	50	100.0	100.0	

According to frequency distribution, 10% bankers thought that security vulnerabilities have impact on business profitability. But opinion of 56% appear it has impact moderately and the rest 34% said strongly. Statement proves the association between security vulnerabilities and profitability are exist.

Table: 6.2.28 Percentage distribution about IT security has an impact on business image.

Do you think that IT security has an impact on business image?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, moderately	17	34.0	34.0	34.0
	Yes, strongly	33	66.0	66.0	100.0
	Total	50	100.0	100.0	

About 66% respondents indicate IT security has an influence on business image strongly and the rest 34% stated moderately. So, bankers need to bring attention about security as their system should be running safe and secured.

Table: 6.2.29 Percentage distribution about ability of secured e-banking to minimize cost and increase profit, reputation and accountability

Do you think that secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Little bit	2	4.0	4.0	4.0
	Yes, of course it is	48	96.0	96.0	100.0
	Total	50	100.0	100.0	

About 96% respondents stated that secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank and the rest 4% spoke little bit. Hence, secured system can only ensure above stated matters.

Table: 6.2.30 Percentage distribution about e-banking security and minimizing core risks.

Do you think that e-security can minimize the core risks of bank (e.g. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Little bit	3	6.0	6.0	6.0
	Yes, strongly	47	94.0	94.0	100.0
	Total	50	100.0	100.0	

According to the result 94% bank people perceived that e-security can minimize core risks strongly and the rest 6% informed little bit. So, the influence of e-security on core risks appears very positive.

Table: 6.2.31 Percentage distribution about system error during customer service.

Can you render your services timely (no delay) and error freely?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes but sometime we faced technical problems	47	94.0	94.0	94.0
	No delay or error at all	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

About 94% respondents stated that officers faced technical problem sometime which makes service delay and the rest 6% told no error at all. That means system has error that can be generated problems. So it seems to be vulnerable.

Table: 6.2.32 Percentage distribution about reliability of internet connection.

Do you think that Customers are fully satisfied about availability and reliability of branch internet connection?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	8	16.0	16.0	16.0
	Partially	42	84.0	84.0	100.0
	Total	50	100.0	100.0	

Opinion proven that according to 84% respondents customer are partially satisfied about reliability of branch internet connection and the rest 16% told not. Hence, it ultimately goes to disfavor of bank business which is not safe and appears to be vulnerable.

Table: 6.2.33 Percentage distribution about existing laws and regulation relating to e-banking security.

Do you think that existing laws and regulations in Bangladesh relating to e-banking are sufficient for banking operation and maintain security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, it can be amended or added	37	74.0	74.0	74.0
	Yes, it is sufficient	13	26.0	26.0	100.0
	Total	50	1r00.0	100.0	

Table result showed that 74% bankers desired laws can be amended or added and other 26% categorically told it is sufficient. According to the statistics, laws are merely not appropriate to ensure e-banking security in Bangladesh. So, systems are running with vulnerabilities.

6.3 Frequency tables of DBBL

Table: 6.3.1 Percentage distribution of the respondents of major security used in banking software.

What are the major securities that used in your banking software?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	First Factor Authentication	10	20.0	20.0	20.0
	Second Factor Authentication	40	80.0	80.0	100.0
	Total	50	100.0	100.0	

From the above table, 80% respondents used second factor authentication as the major security of their banking software and about 20% respondents used one factor authentication as the major security of their banking software. It's a good practice and the system is proven safe and secured.

Table: 6.3.2 Percentage distribution of the respondents of second (two) factor authentication guarantee 100% protection theft of user credentials

Do you think second (two) factor authentication guarantee 100% protection theft of user credentials?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	25	50.0	50.0	50.0
	Yes	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

According to above table 50% respondents did not sure two factor authentication guarantee 100% protection theft of user credentials and the rest 50% respondents informed two factor authentication ensure 100% guarantee to theft of user credentials. Banker's lake of knowledge regarding theft of credentials is found. So, system seems to be vulnerable.

Table: 6.3.3 Percentage distribution of the respondents of type of authentication bank use.

What types of authentication do you use?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Service (Software)	6	12.0	12.0	12.0
	Token (Hardware)	5	10.0	10.0	22.0
	Hybrid (Combination of both)	39	78.0	78.0	100.0
	Total	50	100.0	100.0	

The result is signifying that 78% bank employees were used hybrid system as authentication tool, other 12% used software to authentication system and the rest 10% used token to authentication system. Comparatively it is sound from the security point of views.

Table: 6.3.4 Percentage distribution of using antivirus software in every single PC.

Do you install antivirus software in every single PC?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Just installed after purchased from vendor	10	20.0	20.0	20.0
	Configured correctly after purchased from vendor	40	80.0	80.0	100.0
	Total	50	100.0	100.0	

Result found that 80% bankers configured correctly after purchased from vendor and the rest 20% just install antivirus in their computer after purchased from vendor. So, system found comparatively sound.

Table: 6.4.5 Percentage distribution about type of network use in delivering services to the bank customer.

What type of network you use in delivering your services to the customer?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Internet	20	40.0	40.0	40.0
	VPN	25	50.0	50.0	90.0
	PN with encryption	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

50% respondents used VPN, other 40% used internet and the rest 10% used private network to delivering their services to the customer. So system found reasonably safe.

Table: 6.3.6 Percentage distribution about Performance of your internet connection.

Performance of your internet connection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Have a little bit problems (Sometime)	45	90.0	90.0	90.0
	Completely error free (No delay)	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

Above distribution table illustrates that about 90% informed that internet connection had little bit problem and the rest 10% respondents opined that internet connection was error free. So, the system seems to be vulnerable.

Table: 6.3.7 Percentage distribution about use of network protocol security suit like IPSec or SSL or any digital certificate by bank.

Do you use network protocol security suit like IPSec or SSL or any security certificate?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	8	16.0	16.0	16.0
	Yes	42	84.0	84.0	100.0
	Total	50	100.0	100.0	

The result implies that about 84% respondents told they used digital certificate or network protocol security suit like IP Sec or SSL and the remaining 16% didn't use digital certificate or network protocol security suit like IP Sec or SSL. Hence, opinion of majority proves that their web site or communication system has technologically strong and sound.

Table: 6.3.8 Percentage distribution about the solutions to the security issues for securing end-to-end transaction.

What are the solutions to the security issues for securing end-to-end transaction?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Hardware-based solutions	5	10.0	10.0	10.0
	Software-based solutions involve the use of encryption	5	10.0	10.0	20.0
	Hybrid (Combination of the two)	40	80.0	80.0	100.0
	Total	50	100.0	100.0	

Above table represents that about 80% used hybrid system to secure end-to-end transaction and the rest 20% used both the hardware and software-based solutions. Hence the system is sensibly safe.

Table: 6.3.9 Percentage distribution about installation of recovery tools (e.g. Acornis) in bank PC.

Do you install any recovery tools (e.g. Acornis) in bank PC?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	18	36.0	36.0	36.0
	Yes	32	64.0	64.0	100.0
	Total	50	100.0	100.0	

Total 64% respondents spoke that bank used recovery tools to retrieve data and the rest 36% didn't use recovery tools. So, the system looks secured because majority used acornis in their PC.

Table: 6.3.10 Percentage distribution about clean and check (physical security) branch computer and other digital devices regularly.

Do you clean and check (physical security) branch computer and other digital devices regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	When problem occurred	25	50.0	50.0	50.0
	Regularly	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

About 50% respondents stated that bank checked physical security of hardware when problem occurred, other 50% opined that it was checked on regular basis.

Table: 6.3.11 Percentage distribution about data transmition from one location to another.

In which form your data transmit from one location to another?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Plain text	19	38.0	38.0	38.0
	Cipher text (encryption)	31	62.0	62.0	100.0
	Total	50	100.0	100.0	

According to result it is found that 62% transmitting their data in the form of cipher text. On the other hand, 38% opined data transmit from one location to another as plain text. So, the system appears to be secured.

Table: 6.3.12 Percentage distribution about data backup is taken regular basis.

In which device do you use to take data backup regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	In the secondary device (DVD/Pen drive/Any other device)	5	10.0	10.0	10.0
	In local and central server	6	12.0	12.0	22.0
	Combination of two	39	78.0	78.0	100.0
	Total	50	100.0	100.0	

Respondents opinion regarding data backup represents that 12% stated it is in local or central server and the other 10% kept data backup in the secondary device and 78% was taken data backup through combination of both devices.

Table: 6.3.13 Percentage distribution about process used to preserve data backup

In which site do you preserve your data backup?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Inside of branch	5	10.0	10.0	10.0
	Outside of branch	25	50.0	50.0	60.0
	Combination of both	20	40.0	40.0	100.0
	Total	50	100.0	100.0	

Result showed that 50% preserved data outside of the branch, 10% preserved data inside of the branch and 40% did the job by combination of both process.

Table: 6.3.14 Percentage distribution about retrieve of data backup process.

Do you retrieve data backup (test basis)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	After six months	30	60.0	60.0	60.0
	Regularly	20	40.0	40.0	100.0
	Total	50	100.0	100.0	

About 60% retrieved backup after six months basis and the rest 40% retrieved their backup data regulary.

Table: 6.3.15 Percentage distribution about disaster recovery site.

Do you have a disaster recovery site?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	At Head office premise	5	10.0	10.0	10.0
	Outside of bank premise	45	90.0	90.0	100.0
	Total	50	100.0	100.0	

90% opined it is outside of bank premise, where 10% respondents told it is situated at head office premise.

From the above table, it is found that 90% respondents specify they preserved backup data outside of bank premise for data security. The table also represent that 10% kept their data in his own bank office. Here, system also seems to be secured.

Table: 6.3.16 Percentage distribution about customer access in computer enclave.

Can customer get access easily in your computer enclave?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Depend	7	14.0	14.0	14.0
	No	43	86.0	86.0	100.0
	Total	50	100.0	100.0	

The table represents that 86% customer cannot get easy access in the computer enclave or room, 14% customer can go computer room depending on situation. So, it appears safe.

Table: 6.3.17 Percentage distribution about installation of CCTV in branch to detect fraud and forgeries.

Do you install CCTV in all important branches to detect fraud and forgeries?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, it is available at few branches	7	14.0	14.0	14.0
	Yes, it is available at all branches	43	86.0	86.0	100.0
	Total	50	100.0	100.0	

86% respondents informed that the CCTV is available in every branches. Remaining 14% informed it is available in very few branches. It's a good practice which can track fraud and forgeries in branch location.

Table: 6.3.18 Percentage distribution about communication failure.

Doesn't branch face any communication failure during distance transactions?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, sometime	45	90.0	90.0	90.0
	No, never	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

The result of frequency distribution table depicts that about 90% respondents opined they faced communication failure sometime during distance transactions and the rest 10% stated branch faced communication failure most of time during distance transactions. It's a vital error which can be lost bank reputation.

Table: 6.3.19 Percentage distribution about short and test audit on branch IT infrastructure

Do you conduct short and test audit on branch IT infrastructure in branch level regularly?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	100.0	100.0	100.0

Total 100% respondents informed short and test audit is conducted in branch level on regular basis.

Table: 6.3.20 Percentage distribution about IT audit conducted by whom.

Who conducts IT audit in branch?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT executives	25	50.0	50.0	50.0
	Combination of two	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

The result implies that 50% audit conducted by IT executives and remaining 50% opined it is conducted by both IT executives and general executives.

Table: 6.3.21 Percentage distribution about ICT security check list.

Do you have any ICT security check list to maintain security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	100.0	100.0	100.0

The result indicating that total 100% bankers maintain IT security check list for their operational security. It is good trend for security.

Table: 6.3.22 Percentage distribution about checking of specific software security system

Do you think that IT audit team checks banking specific software security system (e.g. Officers' User name and password nomination, cancelation, password change timely, database security, network security etc.)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	100.0	100.0	100.0

The result illustrates that 100% respondents specified IT audit team checked banking specific software security system. So, the system seems to be secured.

Table: 6.3.23 Percentage distribution about checking of branch daily transaction list

Do you check daily transaction list of branch after transaction?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, check by the officer of IT section	5	10.0	10.0	10.0
	Yes, check by the other officers	45	90.0	90.0	100.0
	Total	50	100.0	100.0	

The result depicted that 90% employees checked daily transaction list by other officers and the rest 10% checked by IT officers.

Table: 6.3.24 Percentage distribution about checking of branch daily transaction list

Would you sent IT experts to monitor ATM booth/Fast Track during servicing by the vendor?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sometime	25	50.0	50.0	50.0
	Regularly	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

50% bank sending experts to monitor ATM booth/Fast Track during servicing by the vendor, other 50% did it on regular basis.

Table: 6.3.25 Percentage distribution about system vulnerabilities.

Do you think your system has no vulnerabilities at all?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	A little bit vulnerabilities	25	50.0	50.0	50.0
	Yes, no vulnerabilities	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

According to result, 50% respondents seem to be little bit vulnerabilities, other 50% respondents observed no vulnerabilities.

Table: 6.3.26 Percentage distribution about security measures taken by bank

Do you have sufficient security measures to render services?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Partially	50	100.0	100.0	100.0

Distribution table result is indicating that 100% banker thought it is not sufficient but partially secured.

Table: 6.3.27 Percentage distribution about ability of secured e-banking to minimize cost and increase profit, reputation and accountability.

Do you think that secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Little bit	9	18.0	18.0	18.0
	Yes, of course it is	41	82.0	82.0	100.0
	Total	50	100.0	100.0	

82% respondents made their comment secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank. Other 18% told little bit.

Table: 6.3.28 Percentage distribution about e-banking security and core risks.

Do you think that e-security can minimize the core risks of bank (e.g. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	A Little bit	10	20.0	20.0	20.0
	Yes, strongly	40	80.0	80.0	100.0
	Total	50	100.0	100.0	

Result implies that 80% found e-security can minimize core risks strongly and the rest 20% informed little bit.

Table: 6.3.29 Percentage distribution about system error during customer service.

Can You render your services timely (no delay) and error freely?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes but sometime we faced technical problems	45	90.0	90.0	90.0
	No delay at all	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

90% respondents told officers faced technical problem sometime which make service delay and the rest 10% respondents opined no error at all.

Table: 6.3.30 Percentage distribution about reliability of internet connection.

Do you think that customers are fully satisfied about availability and reliability of branch internet connection?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Partially	40	80.0	80.0	80.0
	Fully	10	20.0	20.0	100.0
	Total	50	100.0	100.0	

Above table result shown that 80% customers are partially satisfied regarding availability and reliability of branch internet connection and the rest 20% customers are fully satisfied about reliability of branch internet connection.

Table: 6.3.31 Percentage distribution about existing laws and regulation relating to e-banking security.

Do you think that existing laws and regulations in Bangladesh relating to e-banking are sufficient for banking operation and maintain security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, it can be amended or added	45	90.0	90.0	90.0
	Yes	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

According to 90% respondents seem it should be amended or added. So respondents are emphasized on amendment of laws relating to e-banking.

Table: 6.3.32 Percentage distribution about e-security system adoption has positive impact on e-banking vulnerabilities.

Do you thing that proper e-security system adoption has positive impact on e-banking vulnerabilities?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	9	18.0	18.0	18.0
	Yes	41	82.0	82.0	100.0
	Total	50	100.0	100.0	

From the above table, 82% seems e-security has positive impact on e-banking vulnerabilities and other 18% seems there is no positive influence of e-security on e-banking vulnerabilities.

Table: 6.3.33 Percentage distribution about customer satisfaction depends on e-security.

Is customer satisfaction profoundly depending on e-security system adoption issue, do you think that?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	29	58.0	58.0	58.0
	Partially	21	42.0	42.0	100.0
	Total	50	100.0	100.0	

Result found that 58% observed customer satisfaction is profoundly depending on e-security and other 42% assumed it is partially depends.

Table: 6.3.34 Percentage distribution about control culture.

Is branch meeting held on regular basis to develop the all over control culture (e.g. IT, ICC and other related matters)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not regularly	45	90.0	90.0	90.0
	Yes, regularly	5	10.0	10.0	100.0
	Total	50	100.0	100.0	

From the above table result, in 90% cases it is found that branch meeting did not hold on regular basis to develop the control culture and the rest 10% informed it is done on regularly.

Phase: II

6.4 Testing of Hypotheses

To test of drawn hypotheses researcher was used same sets of variables for sample banks. Statistical analysis is conducted applying Pearson Chi-square and correlation test.

First Hypothesis: E-security system has significant impact on e-banking vulnerabilities.

Null hypothesis (H0): There is no association between e-security (second factor authentication guarantee 100% protection theft of user credentials) and system vulnerabilities.

Alternative hypothesis (H1): There is association between e-security (second factor authentication guarantee 100% protection theft of user credentials) and system vulnerabilities.

Table: Cross-tabulation of e-security (second factor authentication guarantee 100% protection theft of user credentials) and system vulnerabilities.

		You think your system has no vulnerabilities at all		Total
		A little bit vulnerabilities	Yes, no vulnerabilities	
Do you think second factor authentication guarantee 100% protection theft of user credentials	Not sure	23	0	23
	No	4	1	5
	Yes	14	4	18
Total		41	5	46

Chi-Square Tests for SBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.630[a]	2	.053
Likelihood Ratio	7.554	2	.023
N of Valid Cases	46		

Interpretation: The Chi-square tests represent the Pearson Chi-Square statistics is 5.630 with degrees of freedom (df) 2 [degrees of freedom= (r-1)(c-1)=(2-1)(2-1)=1] and level of significance is 5%, thus the null hypothesis that the table variables are independent can be rejected. Thus, we can conclude that there is a significance association between e-security (second factor authentication guarantee 100% protection theft of user credentials) and system vulnerabilities. That is, e-security system has significant impact on e-banking vulnerabilities.

		You think your system has no vulnerabilities at all		Total
		A little bit vulnerabilities	Yes, no vulnerabilities	
Do you think second factor authentication guarantee 100% protection theft of user credentials	Not sure	7	5	12
	No	8	10	18
	Yes	10	10	20
Total		25	25	50

Chi-Square Tests for DBBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	0.556[a]	2	0.757
Likelihood Ratio	0.558	2	0.757
N of Valid Cases	50		

Comment: The Chi-square tests represent the Pearson Chi-Square statistics is 0.556 with degree of freedom 2 and level of significance is 10%, thus the null hypothesis that the table variables are not independent can be accepted. Hence, association between e-security (second factor authentication guarantee 100% protection theft of user credentials) and system vulnerabilities is adversarial. That is, e-security system has no significant impact on e-banking vulnerabilities.

Second Hypothesis: There is a positive correlation between e-security system and vulnerabilities

Null hypothesis (H0): There is no relationship between e-security (installed CCTV in all important branches to detect fraud and forgeries) and system vulnerabilities.

Alternative hypothesis (H1): There is relationship between e-security (installed CCTV in all important branches to detect fraud and forgeries) and system vulnerabilities.

Table: Cross-tabulation of e-security (installed CCTV in all important branches to detect fraud and forgeries) and system vulnerabilities.

		You think your system has no vulnerabilities at all		Total
		A little bit vulnerabilities	Yes, no vulnerabilities	
You installed CCTV in all important branches to detect fraud and forgeries	No, it is available at few branches	28	5	33
	Yes, it is available at all branches	17	0	17
Total		45	5	50

Chi-Square Tests for SBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.862[a]	1	.091
Likelihood Ratio	4.437	1	.035
N of Valid Cases	50		

Interpretation: The Chi-square tests represent the Pearson Chi-Square statistics is 2.862 with degrees of freedom 1 and level of significance is 10%, thus the null hypothesis that the table variables are independent can be rejected. Thus, results show that there is a significance relationship between e-security (installed CCTV in all important branches to detect fraud and forgeries) and system vulnerabilities.

		You think your system has no vulnerabilities at all		Total
		A little bit vulnerabilities	Yes, no vulnerabilities	
You installed CCTV in all important branches to detect fraud and forgeries	No, it is available at few branches	3	4	7
	Yes, it is available at all branches	22	21	43
Total		25	25	25

Chi-Square Tests for DBBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	0.166	1	0.684
Likelihood Ratio	0.167	1	0.683
N of Valid Cases	50		

Comment: The Chi-square tests represent the Pearson Chi-Square statistics is 0.166 with degree of freedom 1 and level of significance is 10%, thus the null hypothesis that the table variables are not independent can be accepted. Hence, result found that there is no significant association between e-security and system vulnerabilities.

Third Hypothesis: Bankers' commercial success significantly depends on e-security system.

Null hypothesis (H_0): There is no association between e-security (data is transmitted from one location to another) and commercial success (secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank).

Alternative hypothesis (H_1): There is association between e-security (data is transmitted from one location to another) and commercial success (secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank.

Table: Cross-tabulation of data is transmitted from one location to another and secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank.

		Do you think secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank		Total
		Little bit	Yes, of course it is	
Your data is transmit from one location to another as	Plain text	0	26	26
	Cipher text (encryption)	2	22	24
Total		2	48	50

Chi-Square Tests for SBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.457[a]	1	.103
Likelihood Ratio	3.026	1	.082
N of Valid Cases	50		

Interpretation: The Chi-square tests represent the Pearson Chi-Square statistics is 2.457 with degrees of freedom 1 and level of significance is 10%, thus the null hypothesis that the table variables are independent can be rejected. Thus, results show that there is a significance association between e-security (data is transmitted from one location to another) and commercial success of bank (secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank).

		Do you think secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank		Total
		Little bit	Yes, of course it is	
Your data is transmit from one location to another as	Plain text	3	16	19
	Cipher text (encryption)	6	25	31
Total		9	41	50

Chi-Square Tests for DBBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	0.101[a]	1	0.750
Likelihood Ratio	0.103	1	0.478
N of Valid Cases	50		

Comment: Comment: The Chi-square tests represent the Pearson Chi-Square statistics is 0.101 with degree of freedom 1 and level of significance is 10%, thus the null hypothesis that the table variables are not independent can be accepted. Hence, as a result there is no significant association between e-security and bank commercial success.

Forth Hypothesis: Relationship between e-security system and bank core risks is significant.

Null hypothesis (H_0): There is no association between e-security (clean and check branch computer and other digital devices regularly) and each and every mentioned core risks.

Alternative hypothesis (H_1): There is association between clean and check (physical security) branch computer and other digital devices regularly and each and every mentioned core risks.

Table: Cross-tabulation of e-security (Clean and check branch computer and other digital devices regularly) and each and every mentioned core risks of bank.

		ICT (e-banking) security system has relationship with each and every mentioned core risks (i.e. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk		Total
		Little bit	Yes, strongly	
Do you clean and check (physical security) branch computer and other digital devices regularly	When problem occurred	6	16	22
	After 6 months	1	11	12
	Regularly	0	16	16
Total		7	43	50

Chi-Square Tests for SBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.144[a]	2	.046
Likelihood Ratio	7.830	2	.020
N of Valid Cases	50		

Interpretation: The Chi-square tests represent the Pearson Chi-Square statistics is 6.144 with degrees of freedom 2 and level of significance is 5%, thus the null hypothesis that the table variables are independent can be rejected. Thus, we can conclude that there is a significance association between e-security (physical security of branch computer and other digital devices and with each and every mentioned core risks mentioned above.

		ICT (e-banking) security system has relationship with each and every mentioned core risks (i.e. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk		Total
		Little bit	Yes, strongly	
Do you clean and check (physical security) branch computer and other digital devices regularly	When problem occurred	4	17	21
	After 6 months	1	3	4
	Regularly	5	20	25
Total		10	40	50

Chi-Square Tests for DBBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	0.104[a]	2	0.850
Likelihood Ratio	0.106	2	0.823
N of Valid Cases	50		

Comment: The Chi-square tests represent the Pearson Chi-Square statistics is 0.104 with df 2 and level of significance is 10%, thus the null hypothesis that the table variables are not independent can be accepted. Hence, result found that e-security has no significant influence on each and every mentioned core risks of bank.

Fifth Hypothesis: There is a positive correlation between e-security system and customer satisfaction.

Null hypothesis (H_0): There is no association between e-security (network protocol security suit like IPSec or SSL or any digital certificate) and customer satisfaction (Customer are fully satisfied about availability and reliability of branch internet connection).

Alternative hypothesis (H_1): There is association between e-security (network protocol security suit like IPSec or SSL or any digital certificate) and customer satisfaction (Customer are fully satisfied about availability and reliability of branch internet connection).

Table: Cross-tabulation of e-security (network protocol security suit like IPSec or SSL or any digital certificate) and customer satisfaction (Customer are fully satisfied about availability and reliability of branch internet connection.)

		Customer are fully satisfied about availability and reliability of branch internet connection		Total
		No	Partially	
Are you use network protocol security suit like IPSec or SSL or any digital certificate	No	7	18	25
	Yes	1	23	24
Total		8	41	49

Chi-Square Tests for SBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.091[a]	1	.024
Likelihood Ratio	5.653	1	.017
N of Valid Cases	49		

Interpretation: The Chi-square tests represent the Pearson Chi-Square statistics is 5.091 with df 1 and level of significance is 10% that is highly significant, thus

the null hypothesis that the table variables are independent can be rejected. Thus, we can conclude that there is a strong significance association between e-security (network protocol security suit like IPSec or SSL or any digital certificate) and customer satisfaction (Customer are fully satisfied about availability and reliability of branch internet connection).

		Customer are fully satisfied about availability and reliability of branch internet connection		Total
		No	Partially	
Are you use network protocol security suit like IPSec or SSL or any digital certificate	No	5	3	8
	Yes	35	7	42
Total		40	10	50

Chi-Square Tests for DBBL

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.823[a]	1	0.177
Likelihood Ratio	1.608	1	0.205
N of Valid Cases	50		

Comment: The Chi-square tests represent the Pearson Chi-Square statistics is 1.823 with degree of freedom 1 and level of significant is 10%, thus the null hypothesis that the table variables are not independent can be accepted. Hence, there is no significant relationship between e-security and customer satisfaction.

6.5 Pearson's Correlation tests

Researcher has also tested correlation coefficient of selected variables of the study and tried to find influence of each and every variable on others.

X_1 = What are the major security in your banking software?

X_2 = Do you think second factor authentication guarantee 100% protection theft of user credentials?

X_3 = What type of network you use in delivering your services to the customer?

X_4 = Are you use network protocol security suit like IPSec or SSL or any digital certificate?

X_5 = Any recovery tools (e.g. Acornis) are installed in bank PC

X_6 = Your data is transmit from one location to another as

X_7 = Data backup is taken regularly

X_8 = Customer can get access easily in your computer enclave

X_9 = You installed CCTV in all important branches to detect fraud and forgeries

X_{10} = IT audit are conducted by

X_{11} = Do you have any ICT security check list to maintain security?

X_{12} = You think your system has no vulnerabilities at all?

X_{13} = Do you think that security vulnerabilities have impact on your business profitability?

X_{14} = Do you think that IT security has an impact on business image?

X_{15} = Do you think secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank?

X_{16} = ICT (e-banking) security system has relationship with each and every mentioned core risks (i.e. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk

X_{17} =E-security can minimize the core risks of bank (e.g. ICT security risk, Internal control and Compliance risk, Assets – Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk)

X_{18} =There is no complain by the customers against existing software (i.e. general banking software, RMS+ or others)

X_{19} = You can provide your services timely (no delay) and error freely

X_{20} = Customer are fully satisfied about availability and reliability of branch internet connection

X_{21} = Existing laws and regulations in Bangladesh relating to e-banking are sufficient for banking operation and maintain security

X_{22} = Customer satisfaction is profoundly depending on e-security system adoption issue, do you think that?

Correlation Matrix of SBL

Variables		X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}	X_{22}
X_1	*r*	1	-.500	.156	.736	-.063	-.185	.913	-.058	.375	.000	-.266	-.500	.026	-.266	.156	-.250	.125	-.375	.167	-.375	.167	.425
	N		46	49	48	49	49	49	49	49	48	49	49	49	49	49	49	49	46	49	49	49	48
X_2	*r*		1	-.781	-.327	.500	.041	-.433	.173	-.058	-.600	.145	1.000	-.260	.048	-.156	.000	.000	.500	.333	.500	.333	-.365
	N			46	46	46	46	46	46	46	45	46	46	46	46	46	46	46	45	46	46	46	45
X_3	*r*			1	.136	-.351	.084	.106	-.459	-.009	.469	-.023	-.781	.268	.128	.187	.156	-.078	-.156	-.364	-.156	-.364	.335
	N				49	50	50	50	50	50	49	50	50	50	50	50	50	50	47	50	50	50	49
X_4	*r*				1	.014	-.229	.713	-.176	.453	.000	-.100	-.327	-.062	-.232	.364	-.218	.191	-.191	.145	-.191	.145	.261
	N					49	49	49	49	49	48	49	49	49	49	49	49	49	46	49	49	49	48
X_5	*r*					1	.357	-.049	-.303	.178	-.750	.004	.500	-.243	.105	.082	.146	-.063	.063	.250	.063	.250	-.037
	N						50	50	50	50	49	50	50	50	50	50	50	50	47	50	50	50	49
X_6	*r*						1	-.069	-.197	.159	-.206	.181	.041	-.045	.280	-.045	.330	-.082	-.330	-.426	-.330	-.426	-.085
	N							50	50	50	49	50	50	50	50	50	50	50	47	50	50	50	49
X_7	*r*							1	-.111	.335	-.062	-.188	-.433	.010	-.263	.171	-.248	.062	-.371	.165	-.371	.165	.359
	N								50	50	49	50	50	50	50	50	50	50	47	50	50	50	49
X_8	*r*								1	-.163	.403	-.075	.173	.111	-.214	-.189	-.202	.086	.058	-.058	.058	-.058	-.357
	N									50	49	50	50	50	50	50	50	50	47	50	50	50	49
X_9	*r*									1	-.173	-.075	-.058	-.189	-.214	.261	-.202	.086	-.086	.134	-.086	.134	-.007
	N										49	50	50	50	50	50	50	50	47	50	50	50	49
X_{10}	*r*										1	-.048	-.600	.364	-.048	.052	.000	-.100	.000	-.333	.000	-.333	-.041
	N											49	49	49	49	49	49	49	47	49	49	49	48
X_{11}	*r*											1	.145	.128	.068	-.123	.097	-.024	.024	-.145	.024	-.145	-.037
	N												50	50	50	50	50	50	47	50	50	50	49
X_{12}	*r*												1	-.260	.048	-.156	.000	.000	.500	.333	.500	.333	-.365
	N													50	50	50	50	50	47	50	50	50	49
X_{13}	*r*													1	.380	.051	.416	-.104	.234	.156	.234	.156	-.023
	N														50	50	50	50	47	50	50	50	49
X_{14}	*r*														1	.003	.941	-.145	.266	.177	.266	.177	.158
	N															50	50	50	47	50	50	50	49
X_{15}	*r*															1	.026	.026	.104	.156	.104	.156	.082
	N																50	50	47	50	50	50	49
X_{16}	*r*																1	-.125	.250	.167	.250	.167	.223
	N																	50	47	50	50	50	49
X_{17}	*r*																	1	-.250	-.167	-.250	-.167	.122
	N																		47	50	50	50	49
X_{18}	*r*																		1	.667	1.000	.667	-.020
	N																			47	47	47	46
X_{19}	*r*																			1	.667	1.000	.257
	N																				50	50	49
X_{20}	*r*																				1	.667	-.020
	N																					50	49
X_{21}	*r*																					1	.257
	N																						49
X_{22}	*r*																						1
	N																						49

Green Color Indicates: Correlation is significant (2-tailed) at the 0.01 level (2-tailed).
Blue Color Indicates: Correlation is significant (2-tailed) at the 0.05 level (2-tailed).
Orange Color Indicates: Correlation is significant (2-tailed) at the 0.10 level (2-tailed).
r = Pearson Correlation
***N*=** Number of Observations

Interpretation of Correlation:

Range of Correlation Coefficients	Degree of Correlation
0.80-1.00	Very strong positive
0.60-0.79	Strong positive
0.40-0.59	Moderate positive
0.20-0.39	Weak positive
0.00-0.19	Very weak positive
0.00-(-0.19)	Very weak negative
(-0.20)-(-0.39)	Weak negative
(-0.40)-(-0.59)	Moderate negative
(-0.60)-(-0.79)	Strong negative
(-0.80)-(-1.00)	Very strong negative

Source[153]

The correlation matrix of SBL represent X_1X_7, X_2X_{12}, $X_{14}X_{16}$, $X_{18}X_{20}$ and $X_{19}X_{21}$ have very strong and highly positive significant interrelationship between the variables that means when variable 1 increases, variable 2 increases simultaneously. Conversely, at what time variable 1 decreases, variable 2 decreases. In other words, the variables move in the same direction when there is a positive correlation.

X_4X_7, $X_{18}X_{19}$, $X_{18}X_{21}$, $X_{19}X_{20}$ and $X_{20}X_{21}$ have strong and highly positive significant interrelationship between the variables. Variables X_2X_3, X_2X_{10}, X_3X_{12}, X_5X_{10} and $X_{10}X_{12}$ have strong and highly negative significant interrelationship according to test result. A negative correlation means at what time variable 1 increases, variable 2 decreases or vice versa. In other words, the variables move in opposite directions when there is a negative correlation.

[153] http://picterest.info/V2FpbpdQ-pearson-correlation-interpretation/ (Accessed on: January 12, 2016).

Correlation Matrix of DBBL

Variables		X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}	X_{22}
X_1	*r*	1	-.081	.069	.174	.498	-.075	.258	-.137	.076	.102	.154	-.174	.142	-.282	.106	-.035	.132	.263	.227	.210	.177	.161
	N		50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_2	*r*		1	.161	-.297	.133	.301	.194	-.039	-.103	-.032	-.365	.338	.151	.256	-.252	-.114	.063	-.072	-.251	-.178	.433	.120
	N			50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_3	*r*			1	.093	.142	.386	.021	-.333	.240	-.119	-.413	.128	-.086	-.150	-.209	-.352	-.169	.248	-.011	-.331	-.123	-.085
	N				50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_4	*r*				1	.058	.306	-.010	.184	.401	.616	.330	.074	.107	-.058	-.004	-.067	.080	.036	.261	.322	-.126	-.103
	N					50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_5	*r*					1	-.092	.196	-.047	-.127	.006	.124	.014	.163	-.047	-.050	-.159	.024	.084	.323	.229	.287	.091
	N						50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_6	*r*						1	-.330	-.123	.155	.056	-.214	.214	-.179	.098	-.212	-.074	-.263	-.125	-.243	-.345	.069	.172
	N							50	50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_7	*r*							1	-.135	-.167	-.041	.041	-.041	.192	.167	.215	-.200	.136	.243	.125	.122	.223	-.162
	N								50	50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_8	*r*								1	.178	.226	.384	.043	.033	.038	-.105	.273	.140	-.117	-.032	.475	.158	.146
	N									50	50	50	50	50	50	50	50	50	50	50	50	50	50
X_9	*r*									1	.379	-.042	-.239	.131	-.287	.147	.046	.181	.078	-.181	.083	.056	-.163
	N										50	50	50	50	50	50	50	50	50	50	50	50	50
X_{10}	*r*										1	.291	.269	.016	-.125	-.165	.089	.200	-.108	.204	.433	.151	.141
	N											50	50	50	50	50	50	50	50	50	50	50	50
X_{11}	*r*											1	-.111	.237	.324	.272	.442	-.084	-.090	.084	.764	.198	-.003
	N												50	50	50	50	50	50	50	50	50	50	50
X_{12}	*r*												1	-.345*	.099	-.612	-.058	-.197	-.174	-.084	-.036	.106	.003
	N													50	50	50	50	50	50	50	50	50	50
X_{13}	*r*													1	.347	.079	.250	.234	.029	-.098	.434	.286	-.199
	N														50	50	50	50	50	50	50	50	50
X_{14}	*r*														1	-.147	.440	-.181	-.417	-.352	.147	.137	-.263
	N															50	50	50	50	50	50	50	50
X_{15}	*r*															1	-.082	.378	.228	.052	.189	-.112	-.104
	N																50	50	50	50	50	50	50
X_{16}	*r*																1	-.102	-.521	-.626	.296	.239	.083
	N																	50	50	50	50	50	50
X_{17}	*r*																	1	.032	.064	.349	-.042	-.104
	N																		50	50	50	50	50
X_{18}	*r*																		1	.468	.055	-.167	.061
	N																			50	50	50	50
X_{19}	*r*																			1	.110	-.150	.129
	N																				50	50	50
X_{20}	*r*																				1	.259	-.062
	N																					50	50
X_{21}	*r*																					1	.304
	N																						50
X_{22}	*r*																						1
	N																						50

Green Color Indicates: Correlation is significant (2-tailed) at the 0.01 level (2-tailed).
Blue Color Indicates: Correlation is significant (2-tailed) at the 0.05 level (2-tailed).
Orange Color Indicates: Correlation is significant (2-tailed) at the 0.10 level (2-tailed).
r = Pearson Correlation
***N*=** Number of Observations

Interpretation of Correlation:

Range of Correlation Coefficients	Degree of Correlation
0.80-1.00	Very strong positive
0.60-0.79	Strong positive
0.40-0.59	Moderate positive
0.20-0.39	Weak positive
0.00-0.19	Very weak positive
0.00-(-0.19)	Very weak negative
(-0.20)-(-0.39)	Weak negative
(-0.40)-(-0.59)	Moderate negative
(-0.60)-(-0.79)	Strong negative
(-0.80)-(-1.00)	Very strong negative

The correlation matrix of DBBL represent $X_{11}X_{20,}$ $X_{12}X_{15}$ and $X_{16}X_{19}$ have strong and highly positive significant interrelationship between the variables that means at what time variable 1 increases, variable 2 increases. Conversely, once variable 1 decreases, variable 2 decreases. In other words, the variables move in the same direction when there is a positive correlation. $X_{12}X_{15}$ and $X_{16}X_{19}$ have strong and highly negative significant interrelationship between the variables. A negative correlation means that once variable 1 increases, variable 2 decreases or vice versa. In other words, the variables move in opposite directions when there is a negative correlation.

X_1X_5, X_4X_9, $X_{14}X_{16}$, $X_{18}X_{19,}$ X_8X_{20} and $X_{10}X_{20}$ have moderate positive and highly significant interrelationship between the variables. Variables between $X_{14}X_{18}$ and $X_{16}X_{18}$ have moderate negative and highly significant interrelationship in accordance of test result.

6.6 Findings of the Study

Major findings of the study were as follows:

6.6.1 E-banking vulnerabilities and securities

(Technological, operational and compliance related)

- By applying Pearson's Chi-square test to investigate the association between e-security and vulnerabilities of SBL researcher found that e-security system has significant association with vulnerabilities as the calculated Chi-square is 2.862 (where p value is .091 which is less than 0.1 significance level). So the null hypothesis was rejected by result. That is this findings is true.

- By applying Pearson's Chi-square test to investigate the association between e-security and vulnerabilities of DBBL found that e-security system has no significant impact (influence) with vulnerabilities as the calculated Chi-square is 0.166 (where p value is 0.684 which is greater than 0.1 significance level). So the result was accepted null hypothesis. That is alternative hypothesis is rejected.

- **Data transmission mode of bank**

  Total 52% respondents of SBL opined that data are transmitting one location to another as plain text (not as encrypted). On the other hand 48% told data transfer from one location to another as cipher text (encryption mode). Result showed that system is vulnerable here.

Total 38% respondents of DBBL opined that data are transmitting one location to another as plain text (not as encrypted). On the other hand 62% told data transfer from one location to another as cipher text (encryption mode). Result showed that system is comparatively secured.

- **Retrieve backup data (test basis)**

About 38% respondents opined that they never retrieve backup data in test basis, where 28.6% told they retrieve backup data irregularly and 38.8% told the retrieve it in every month. Result showed that about 66.6% respondents opined that backup data do not retrieve regularly in test basis. It is proved that responsible people of SBL do not aware about data security.

About 60% respondents of DBBL opined that executives retrieve backup data in test basis after six months, where 40% told they retrieve backup data regularly. It is proved that responsible people of DBBL do not retrieve backup data regularly.

- **Performance of bank internet connection**

Respondent's opinion regarding internet performance of SBL found, 89.9% respondents told network have little bit problem and 10.2% told network response is slow. So that inter-branch transaction through internet influence customer service sometime.

Respondent's opinion regarding internet performance of DBBL found, 90% respondents told network have little bit problem and 10% told internet has

no failure. So that inter-branch transaction through internet influence customer service sometime.

- **Customer access in branch computer enclave**

  About 26% respondents of SBL told customers get access easily in computer enclave, 38% respondents told its depends on situation and rest 36% opined customer didn't get access.

  About 86% respondents of DBBL told customer didn't get access in computer enclave, rest 14% respondents told its depends on situation. So that customers are restricted to enter into computer enclave.

- **Providing services timely and error freely**

  94% respondents of SBL opined branch cannot provide service to the customer timely and system has some error where only 6% told customer gets services timely. 90% respondents of DBBL opined branch tried to render services to the customer timely but system has some error where only 10% told customer gets services timely. That means both banks faced some problems technologically or operationally to render services to the customer.

- Respondents of SBL perception regarding system vulnerabilities found that about 90% told system has vulnerabilities. On the other hand, 50% respondents of DBBL told that system has little bit problem and 50% said there is no system vulnerabilities.

- From observation it is found that ATM and core banking operation of SBL appear to be vulnerable. ATM card holder didn't get SMS about its transaction. Even card like VISA can easily be debited at POS without PIN number. On the other hand, ATM and core banking solution of DBBL is more secured compare to SBL. DBBL offer EMV chip based secure card that contains microprocessor. On the other hand, SBL offer traditional magnetic stripe based card to their customer. MagStripe card is insecure compared with a chip card and it can easily be read by reader.

- **Existing laws and regulations in Bangladesh relating to e-banking security**

  Respondent's (SBL) opinion regarding existing laws and regulations relating to e-banking security found, 74% respondents told it can be amended and 26% told no need to do so.

  Beside rrespondent's (DBBL) opinion regarding existing laws and regulations relating to e-banking security found, 90% respondents told it can be amended or added and 10% told no need to do so.

6.6.2 E-security systems and commercial success of bank

- By applying Pearson's Chi-square test to investigate the association between e-security and bank commercial success of SBL found that e-security system has significant association with bank commercial success as the calculated Chi-square is 2.457 (where p value is .103 less than 0.1

significance level). So the result was rejected null hypothesis. That is alternative hypothesis is true or accepted.

By applying Pearson's Chi-square test to investigate the association between e-security and bank commercial success of DBBL found that e-security system has no influence with bank commercial success as the calculated Chi-square is 0.101 (where p value is 0.750 greater than 0.1 significance level). So the result was accepted null hypothesis. That is alternative hypothesis is not true or rejected.

- **Facing communication failure during distance transactions**

Respondents opinion regarding communication failure during distance banking among branches showed that about 10% told most of time they faced communication failure and remaining 90% opined some time faced communication error during transaction hour. So percentage of frequency distribution resulted that any communication failure can affect commercial success of bank. So this error influenced business reputation and competitiveness of SBL.

On the contrary, DBBL respondents opinion regarding communication failure during distance banking among branches showed that about 90% told most of time system faced communication failure and remaining 10% opined no communication error during transaction hour. So percentage of frequency distribution stated that any communication error can influence customer transaction. So this error can be influenced business reputation and competitiveness for DBBL.

- **Security has an impact on business image**

  66% respondents of SBL strongly agreed that security has an impact on business image and only 34% told moderately influenced according to frequency table results. That means commercial success of bank depends on e-security. On the contrary, respondents of DBBL have given same statement.

- **Security vulnerabilities have impact on your business profitability**

  Respondents of SBL perception about security vulnerabilities impact on business profitability found 56% moderately, 34% strongly and rest 10% told no impact. Beside, respondents of DBBL have given positive consent about above mentioned issue.

6.6.3 Relationship between e-security system and bank core risks

- By applying Pearson's Chi-square test to investigate the association between e-security and bank core risks of SBL found that e-security system has significant association with bank core risks as the calculated Chi-square is 6.144 (where p value is 0.046 less than 0.05 significance level). So the result was rejected null hypothesis. That is alternative hypothesis is true or accepted.

- By applying Pearson's Chi-square test to investigate the association between e-security and bank core risks of DBBL found that e-security system has no significant association with bank core risks as the calculated Chi-square is 0.104 (where p value is 0.850 greater than 0.10

significance level). So, the result was accepted null hypothesis. That is alternative hypothesis is not true of rejected.

- 86% respondents of SBL strongly supported association between core risks and e-security is to be present and 14% told there is little bit relation between two. Table results showed that e-security affected core risks.

  About 100% respondents of DBBL strongly supported association between core risks and e-security is to be present. Frequency distribution results of both banks validated e-security affected bank's core risks.

6.6.4 Relationship between e-security system and bank's customer satisfaction

- By applying Pearson's Chi-square test to investigate the association between e-security and bank customer satisfaction of SBL found that e-security system has significant association with customer satisfaction as the calculated Chi-square is 5.091 (where p value is .024 less than 0.05 significance level). So the result was rejected null hypothesis. That is alternative hypothesis is true or accepted.

- By applying Pearson's Chi-square test to investigate the association between e-security and bank customer satisfaction of DBBL found that e-security system has no significant association with customer satisfaction as the calculated Chi-square is 1.823 (where p value is 0.177 greater than 0.1 significance level). So the result was accepted null hypothesis. That is alternative hypothesis is not true or rejected.

- According to frequency table result of SBL demonstrated that about 94% opined e-security has strong influence on bank core risks and rest 6% told little bit influence. But 80% respondents of DBBL said that e-security is interrelated with core risks and rest 20% told little bit.

6.6.5 Security risk management process of bank

- According to Risk Management Guidelines for Banks (secondary source of data) prepared by Department of Off-site Supervision of BB, where central bank of Bangladesh emphasized on principles for effective banking supervision published by the Basel Committee on Banking Supervision (BCBS) in October 2006. The CP2 on 'Risk Management Processes' (CP7) requires that banks and banking groups must have comprehensive risk management processes (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their risk profile.[154] According to guidelines ICT security risk is a vital risk out of rest seven core risks. This can be used in reducing ICT risk. CBs of Bangladesh claimed that it has done almost all initiatives according to risk management guidelines of BB but the picture is exactly different. Observation found that it is concluded only in written form. There is no practical implementation in reducing electronic risks by e-bankers. Even CBs didn't follow risk management guidelines properly. Deficiencies have been found (during observation) to implement the direction of BB. Recently 502 CBS branches of SBL have been hanged due to security

[154] Bangladesh Bank, *Risk Management Guidelines for Banks (*February, 2012),1.

vulnerabilities for long time (three consecutive days)[155] Risk management division of SBL have been running without top rank IT executives. The bank is far behind from implementation of IT risks. There is no proper business continuity management (BCM) framework, incident management (IM), infrastructure security management, separate e-banking security team and chief ICT security officer or database administrator in SBL. On the other hand, DBBL has well set up in this regard compared to SBL. Guide Line on ICT Security for Bank's & Non-Bank Financial Institutions (Version-3.0) was issued by BB to mitigate ICT risk in sustainable level. But some improper initiatives have been seen in this regard during observation. However, observation also found that in some cases BB did not meet the standards relating to the surveillance of e-security risks.

- Observation found that there is no IT security team in SBL head office or in controlling office level. On the contrary, security team was found in DBBL head office level headed by a Senior Assistant Vice President (SAVP). According to IT policy (3.1.15) of SBL the Bank is required to ensure regulatory compliance at all levels; therefore, ICT audit is aimed at ensuring an acceptable standard for security on all SBL servers, workstations, routers, switches, and other ICT systems. But the bank was failed to ensure it commitment according to IT policy of its own. Hence, SBL didn't exercise to implement manpower development policy in an acceptable standard according to bank IT policy. The bank has organogram for promotion of IT personnel which is indecorous. The discrimination regarding stated issue was observed in SBL.

[155] *bdnews24*, January 5, 2016

6.6.6 Correlation between e-security and vulnerabilities, e-security and commercial success of bank, e-security and core risks, e-security and customer satisfaction

- Correlation coefficient of e-security and vulnerabilities, e-security and commercial success, e-security and core risks, e-security and customer satisfaction of SBL was found negative and positive significant relationship or influence between the variables. Here r= -.500, -.266, -.250, and .425, respectively. It is shown from the analysis there is a positive and negative linear significant relationship between the variables.

- Correlation coefficient of e-security and vulnerabilities, e-security and commercial success, e-security and core risks, e-security and customer satisfaction of DBBL was found positive and negative significant relationship between the variables. Here r= -.174, -.282, -.035, .161 and -.282 respectively. It is said that except set X1 X2 (r= -.282) are not significant according to Correlation coefficient results. That is the Correlation coefficient result of SBL and DBBL was found dissimilar.

Chapter VII
Summary, Recommendations and Conclusion

Introduction

This section of study considered as the most motivating and also important part of the current research where the entire study are presented the solutions to the problems are offered in the form of recommendations and finally it is summarized and generalized the study properly in the form of conclusion. Current study almost covered the different sorts of security vulnerabilities of e-banking here in Bangladesh. There are several issues which need to be considered to improve the situation of e-banking security vulnerabilities of CBs. Results indicated that most of the banks are disquiet about their data privacy and security. Even their system found vulnerable in certain context which is precisely talked over in chapter six of the dissertation. This chapter basically concise the outcomes of the study on the basis of designed research questions and objectives.

7.1 Summary

The main purpose of the study is to find out the security flaws of e-banking and it is done based on core objectives of the study. In order to achieve the goal the whole study is divided into seven important chapters. In first chapter researcher is given an overview of the research including problems of the study, major definition relating to e-banking security vulnerabilities, research questions, objectives of the study, drawn relevant hypothesis, mentioned limitation of the study and elaborated layout of the dissertation. In second chapter, important and applicable literatures have been reviewed to make study affluence. Third chapter discussed how to conduct the research to reach into ultimate outcomes. In order

to do so, researcher selected applicable variables and indicators, population, samples, respondents, sources of data, appropriate methods of research and various analytical tools.

In forth chapter important theoretical and conceptual models and mechanisms have been illustrated and a proposed conceptual model was presented for secured e-banking which is reduced core flaws or risks and attains customer satisfaction and commercial success of bank. Fifth chapter portrayed important laws, acts and regulations relating to the e-banking security vulnerabilities here in Bangladesh and as well as abroad. In the sixth, collected data ware analyzed using applicable statistical tools and find out the main findings of the study based on research questions, objectives and hypothesis. Finally in the seven chapter, important recommendations are suggested on the basis of findings.

7.2 Recommendations

The result of this research has certain consequences for sample banks SBL and DBBL. Yet the suggestions that have to be considered by e-bankers of financial service industry of Bangladesh for execution to the benefit from the outcome of this particular study has discussed in this section.

- The average over all perceived vulnerabilities and securities of SBL was followed much below standard compared to DBBL. Therefore, SBL may attempt to improve average securities status and try to assess vulnerabilities using vulnerabilities assessment tools and resources.

- Test result for the impact of e-security system on e-banking vulnerabilities of SBL found significantly positive, where result of DBBL showed adverse

picture regarding relationship between vulnerabilities and securities. However, SBL should carefully be considered the issue to keep itself safe and sustain.

- It was found that 52% respondents of SBL opined that data is transmitting one location to another as plain text (not as encrypted). On the other hand, 62% respondents of DBBL told data transfer from one location to another as cipher text (encryption mode). Although DBBL is more secured regarding data transmission compare to SBL, but both banks are not following complete cryptographic mechanisms during transmition of data observation found it. According to respondents opinions in some context technological security is perceived vulnerable for both banks. Hence, this study recommends both banks to customize its system fully cryptographic oriented.

- About 64% respondents of SBL told generally customer gets access in computer enclave and 14% respondents of DBBL told its depends on situation. Percentage distribution results indicated that operational security of SBL was perceived more vulnerable compare to DBBL. However, SBL should be more careful in this regard and by any cost both banks need to maintain secrecy of its system and transaction.

- Opinion regarding existing laws and regulations relating to e-banking security found that about 74% respondents of SBL told it can be amended. Beside, 90% respondents of DBBL opined it can also be amended or added. So, in order to conduct e-banking operation effectively the existing laws and regulations could be amended or added by the regulatory

authority and concern state authority. Even to develop the all over control culture and minute irregularly (e.g. IT, ICC and other related matters) in the branch level both banks need to take necessary measures. About 90% respondents of DBBL opined it. SBL status regarding ICC was observed almost same. So, this study revealed that compliance related vulnerabilities were present in both banks. Hence, the related internal compliances have to be improved to keep its operation secured.

- Since from the study it was observed that the effect of e-security system on commercial success of SBL was positive, that is e-security system has significant effect on bank commercial success as the calculated Chi-square is 2.457 (where p value is .103 less than 0.1 significance level). It is proved that SBL security condition was much worse compare to DBBL. So, SBL is needed to improve all sorts of security measures to gain commercial success.

- Respondents of both banks (100% of SBL and 100% of DBBL) were opined during distance banking most of time system faced communication failure. It is proved that status of broadband connection (used by banks) was perceived weak, that's why banks have been facing communication error during transaction hour. Banks are recommended to use such broadband line that has comparatively good reputation compare to other ISP and in this regard, this study also recommended to the ISP offering convenience packages in terms of cost and technology to CBs followed by other sectors.

- About 66% respondents of SBL strongly agreed that security has an impact on business image and only 34% told moderately influenced according to frequency table results. That means commercial success of bank depends on e-security. On the contrary, respondents of DBBL have given same statement. So, host study recommended to both banks keeping its security procedures (technological, operational and compliances) at a sustainable level.

- E-security system has significant influence on bank's core risks. The statistical result depicted that e-security system has significant association with bank core risks as the calculated Chi-square is 6.144 (where p value is 0.046 less than 0.05 significance level). So, given results implied that for SBL e-security may affect core risks. Hence, SBL should be taken measures to mitigate core risks.

- Around 86% respondents of SBL strongly supported association between core risks and e-security is found positive. But 100% respondents of DBBL strongly agreed security has strong coordination with core risks. So, respondents consent ascertained that ICT (e-security) security issue can be affected others six core risks declared by BB that is very much risky for both banks. Hence, improvement and innovative measures have to be taken in this regard.

- Statistical test represents calculated Chi-square is 5.09 (where p value is .024 less than 0.05 significance level) for SBL regarding relationship between customer satisfaction and e-security. That means customer

satisfaction is significantly depending on e-security system. On the other hand, same test result for DBBL on this particular issue was found adverse (the calculated Chi-square is 1.823 (where p value is 0.177 greater than 0.1 significance level). According to result no influence was seen for DBBL regarding the issue. So, the host study recommended SBL that by any cost the bank should be decreased its system vulnerability level for the benefit of bank as well as other valued party, then the study also recommended DBBL to continue its e-security measures scale at a workable level that the bank can be made themselves secured.

- This study recommended sample banks have to follow and exercise all possible directions of regulatory authority to reduce e-security risks. Beside, surveillance regarding control and compliances should strictly be maintained by both CBs as well as central bank from their respective end to mitigate e-security risks.

- Correlation coefficient of e-security and vulnerabilities, e-security and commercial success, e-security and core risks, e-security and customer satisfaction of SBL found positive and negative both in certain range. However, overall security level should be improved and vulnerabilities level should be reduced by using different sorts of tools and techniques.

Furthermore, based on study and analysis of the answers of questionnaires and physical findings some other important recommendations are added to the policy maker and management of the banks operating e-banking here in Bangladesh:

- Internal control and compliances should strictly be maintained in different division of SBL head office (e.g. IT Division, Risk management Division, MIS division, etc.) as well as at branch level to mitigate e-risk particularly. It is said that serious compliance related problems are found in SBL by the researcher during observation. In this regard DBBL has better condition compare to SBL.

- Designation wise training and professional course is required for IT officer. However, proper training is needed for employees on e-security to investigate different heist. The researcher found weakness in following bank circular by officers. So, circulars should properly be followed and maintained by the branch managers and officers both in SBL and DBBL. On the other hand, it is suggested that both banks need to follow related IT policy for recruiting IT manpower.

- In order to improve efficiency of IT people separation of tasks is required in bank that they acquire specialized capabilities to take advantages about their task. In SBL researcher found discrimination regarding function of IT executives. One people do different tasks that they hinder expertise. In order to increase productivity, dexterity, skill, innovation and saving time the idea can be introduced in bank's IT sector. This study strongly recommends technical division of labor in this particular section that work may be divided into complete tasks like operating, networking, hardware, software etc. Technical division of labor is obvious feature of modern digitized age.

- Installation of switching software or tools for vulnerability assessment, intrusion detection and data leakage prevention is needed. It is found that most of the bank didn't use such third party software to assess flaws in

their system. This study intensely recommends both banks should be used vulnerability assessments tool to avoid internal and external possible heist. Maintain multi-factor authentication instead of one-time password (OTP) authentication is also important operation in case of high value transaction.

- Dedicated PC's or system unit (such as interbank transaction settlement software BACH, cross border transactional tool SWIFT, etc.) should not use for other purposes. Through this habit or operation malware can easily be infected to the system. Yet, general banking system units must not connect with such dedicated system through ordinary networking devices. If necessary secured networking devices can be installed between the systems and routine monitoring is necessary in this concern. Networking between dedicated system and any general system could be escaped if possible. Hackers can easily be attempted to target dedicated system to heist information through the specific unit of the general system.

- Security in software database is essential thing. Implementation a proactive data protection strategy in database and continuous monitoring can mitigate database vulnerabilities. Bank management should buy and install such software which one has very strong default database security mechanisms because any alternation or changes in database means massacre of stored data. In this regard, the role of security team of bank is very much important to assist their respective management. The study suggested purchasing local (domestic) banking software (both front and back end) with source code to get more support from vendor and if necessary bank can customize software as they desired. SBL is better condition followed by DBBL in this concern.

- Management is very much concern for proper e-banking operation. Weaknesses are found in this regard during conducting the research. So, this study recommended that Business continuity management, Change management, Incident management, ICT Endpoint security system management is important for e-banking operation. Both banks are suggested to follow this particular recommendation.

- Separate IT audit team with the combination of digitally-savvy or tech-savvy officers in audit division and central oversight IT security team in head office level is desirable. Researcher found serious deficiencies in this regard in both banks.

- This is common trend here in Bangladesh that banks invested more to digitize their system but comparatively didn't increase security fund to protect different type of heists. So, the study strongly recommends that there should adequately be creation of security fund or information security budget in every single bank to keep their system safe and secured. Even it should be a part of their self-security strategy.

- Passing proper legislative relating to cyber security acts and amendment or addition of some important clauses or sections of banking acts is a core demand to today's e-banking operation. The ICT division, ministry of ICT is prepared a draft to make cyber security acts to protect heists. The state should take immediate steps to pass the associate legislatives. In order to improve customer satisfaction government has to provide basic infrastructure required to access online banking services by the banks.

- Finally, CB's of Bangladesh need to make public awareness regarding secured e-banking operation like online banking, ATM (Debit card, Credit

card, Utility card, etc.) operation, Mobile banking, and so on. Trustworthiness of customer is very important thing for bank commercial success. Similarly the Central bank of Bangladesh needs to take proper initiatives minimizing threats or e-risks and attain customer trustworthiness as a regulatory authority in favour of CBs.

Conclusion

The leading issues of the research are to explore e-banking security vulnerabilities and the indicators that influence Bangladeshi CBs to adopt e-security system for smooth operation. The findings of the research were summarized according to research questions, major objectives and hypothesis tests of the study. This study found and revealed a significant role of financial service industry in boosting money market as well as whole economy of the country. Yet the study found insufficient investment and very deprived budget allocation to ensure e-security of CBs.

This research mainly exposed existing e-banking security vulnerabilities status of CBs here in Bangladesh and suggested a model conducting secured e-banking operation.

The study found that SBL is not properly complying with standard security norms and the bank is walking far behind from standard security mechanism and its system proven vulnerable. The bank has been suffering from serious technological, operational and compliance related vulnerabilities since its digitization. On the contrary, DBBL has some operational and compliance (other than technology) related vulnerabilities, but their technological security is up to standard level. it can be notable that these existing security vulnerabilities are appropriately enough to paralyze whole operation of this particular bank which is injurious for the banking services as well as for stakeholders of bank.

Therefore, the all banks need to mitigate vulnerabilities through diverse security measures recommended by the host study.

7.3 Final Remarks

Researcher has emphasized on e-banking security vulnerabilities of CBs in Bangladesh. Different sorts of technological, operational and laws related security vulnerabilities were explicitly found and exposed in this complete work. An attempt has been made to make a comprehensive model to mitigate security risks that can be made e-banking operation safe and sustainable to attain customer satisfaction and commercial success of CBs.

7.4 Suggestions for further research

There are number of suggestions for further research possible on the following dimensions. It can be extended in different directions. Firstly, e-securities and vulnerabilities of two CBs was studied, so a further study may be carried out on more CBs and schedule of respondents can be enlarged. Secondly, a separate research may be carried out on core technological security issues of e-banking or about local and cyber security nature of online banking here in Bangladesh and remedies. Finally, a research can be conducted on the e-security policies and strategies designed for e-banking operation by the bank in Bangladesh.

Appendices

Appendix- I
Respondent Schedule (Questionnaire)
on

E-banking in Bangladesh: Vulnerabilities and Securities

2016

Dear Sir:

I am a PhD fellow in the institute of Bangladesh Studies (IBS), University of Rajshahi. I have currently been conducting research on “E-banking in Bangladesh: Vulnerabilities and Securities”. The attached questionnaire is a significant part of my study. One of the important objectives of this questionnaire is to reveal empirical evidence on e-banking vulnerabilities and securities of commercial banks. I am hopeful and carrying out the questionnaire with you, as experienced personnel in this area. Therefore, I would be extremely grateful if you would contribute and cooperate toward the successful result of this particular research, which will hopefully lead to the improvement of the security system of electronic banking in Bangladesh by completing this questionnaire.

Finally, I wish to confirm that the information and personal opinion that you share with me will be treated as confidential. Please accept in advance my best regards and appreciation for your cooperation.

Yours Faithfully,

(Md. Nokib Uddin)
Ph D fellow (2013-14)
Institute of Bangladesh Studies (IBS)
University of Rajshahi, Bangladesh.
Cell: 01711895358, 01977895358
E-mail address: mct_nokib@yahoo.com

Identification of Respondent

Name of the respondent :
Designation :
Bank and Branch :
Contact number :
E-mail address :

It is said that this questionnaire set is exclusively for Dutch Bangla bank Ltd. personnel. This questionnaire consists mainly of two sections. This section aims to collect information about major e-banking vulnerabilities and securities, bank's commercial success, bank's core risks and customer satisfaction. Please answer by circling the appropriate number.

Section (1): Major Vulnerabilities and Securities, (security relating to) bank's commercial success, core risks and customer satisfaction related information of e-banking

i) What are the major securities that used in your banking software?

0. First Factor Authentication
1. Second Factor Authentication
2. Third Factor Authentication

ii) Do you think second factor authentication guarantee 100% protection against theft of user credentials?

0. Not sure
1. No
2. Yes

iii) What types of authentication do you use?

0. Service (Software)
1. Token (hardware)
2. Both/Hybrid

iv) Did you install antivirus software?

0. Just installed after purchased from vendor
1. Configured correctly after purchased from vendor

v) What type of network you use in delivering your services to the customer?

0. Internet
1. VPN
2. PN with encryption

vi) What about performance of your internet connection?

0. Slow response
1. Have a little bit problems (Sometime)
2. Completely error free (No delay)

vii) Do you use network protocol security suit like IPSec or SSL or any security certificate?

0. No
1. Yes

viii) What are the solutions to the security issues for securing end-to-end transaction?

0. Hardware-based solutions
1. Software-based solutions
2. Hybrid of two

ix) Did you install any recovery tools (e.g. Acornis) in bank PC?

0. No
1. Yes

x) Do you clean and check (physical security) branch computer and other digital devices regularly?

0. When problem occurred
1. After 6 months
2. Regularly

xi) In which form your data transmit from one location to another?

0. Plain text
1. Cipher text (data encryption)

xii) Do you take data backup regularly?

0. In the Server
1. In the secondary device (DVD/Pen drive/Any other device)
2. Combination of two

xiii) Where do you preserve your data backup?

0. Inside of branch
1. Outside of branch
2. Both

xiv) Do you retrieve backup data (test basis)?

0. Never
1. After six months
2. Regularly

xv) Where is your disaster recovery site?

0. At your HO
1. Outside of bank premise

xvi) Can customer get access easily in your computer enclave?

0. Yes
1. Depend
2. No

xvii) Do you install CCTV in all important branches to detect fraud and forgeries?

0. No, it is available at some branches
1. Yes, it is available at all branches

xviii) Doesn't branch face any communication failure during distance transactions?

0. Yes, most of time
1. Yes, sometime
2. No, never

xix) Do you think that short and test audit on IT operation are conducted in branch level regularly?

0. No
1. Yes

xx) Do you conduct IT audit?

0. General executives
1. IT executives
2. Combination of two

xxi) Do you have any ICT security check list to maintain security?

0. No
1. Yes

xxii) Do you think that IT audit team checks banking specific software security system (e.g. Officers' User name and password nomination, cancelation, password change timely, database security, network security etc.)

0. No
1. Yes

xxiii) Do you check daily transaction list of branch after transaction?

0. No, we don't check
1. Yes, check by the officer of IT section
2. Yes, check by the other officers

xxiv) Who check the list?

0. No checking
1. Yes, checking by the officer of IT section
2. Yes, checking by the general officer of other section

xxv) Do you hold branch meeting on regular basis to develop the all over control culture (e.g. IT, ICC and other related matters) in the branch level?

0. No
1. Not regularly
2. Yes, regularly

xxvi) Would you send IT experts to monitor ATM booth/Fast Track during servicing by the vendor?

0. No
1. Sometime
3. Regularly

xxvii) Do you think your system has no vulnerabilities at all?

0. A little bit vulnerabilities
1. Yes, no vulnerabilities

xxviii) Do you think that security vulnerabilities have impact on your business profitability?

0. No
1. Yes, moderately
2. Yes, strongly

xxix) Do you think that IT security has an impact on business image?

0. No
1. Yes, moderately
2. Yes, strongly

xxx) Do you think secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank?

0. No
1. Little bit
2. Yes, of course it is

xxxi) Do you think that e-security can minimize the core risks of bank (e.g. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk)?

0. No
1. Little bit
2. Yes, strongly

xxxii) Can you provide your services timely (no delay) and error freely?

0. No
1. Yes but sometime we faced technical problems
2. No delay at all

xxxiii) Do you think that customers are fully satisfied about availability and reliability of branch internet connection?

0. No
1. Partially
2. Fully

xxxiv) Do you think that existing laws and regulations in Bangladesh relating to e-banking are sufficient for banking operation and maintain security?

0. No, it can be amended or added
1. I/We don't know
2. Yes

Section (2): Impact of e-banking security adoption issues for the commercial bank (Semi-Structured interview question)

This section aims to collect information of e-security system adoption by e-bankers and its impact on bank business. Please answer the most appropriate reason for these questions.

1. Do you thing e-banking is a new trend in Bangladesh and it has been facing serious vulnerabilities (open for possible attack)?
2. Do you thing that proper e-security system adoption has positive impact on e-banking vulnerabilities?
3. ICT security risk is interrelated and interconnected with other core risks (i.e. credit risk, money laundering risk, environmental risk, internal control and compliance risk etc.). Make your comment.

4. Do you think nowadays banks' commercial success is depending on proper e-security system adoption issue for automated commercial bank?
5. Customer satisfaction is profoundly depending on e-security system adoption issue, do you think that?
6. Customers are not adopting e-banking in our country because improper security measures taken by the e-bankers, do you think that?
7. What is your perception regarding existing e-banking securities, which one is first either security or service?
8. Do you follow all the e-banking related security instructions given by regulatory authority and do you have own ICT guideline or policy to follow it?
9. Is NI Act 1881 support virtual cheque? What is the legal basis of such banking?
10. How to increase e-banking security level?

Appendix- II

Identification of Respondent

Name of the respondent :
Designation :
Bank and Branch :
Contact number :
E-mail address :

It is said that this questionnaire set is exclusively for Sonali bank Ltd. personnel. This questionnaire consists mainly of two sections. This section aims to collect information about major e-banking vulnerabilities and securities, bank's commercial success, bank's core risks and customer satisfaction. Please answer by circling the appropriate number.

Section (1): Major Vulnerabilities and Securities, (security relating to) banks commercial success, core risks and customer satisfaction related information of e-banking

i) What are the major securities in your banking software?

3. First Factor Authentication
4. Second Factor Authentication
5. Third Factor Authentication

ii) Do you think second factor authentication guarantee 100% protection against theft of user credentials?

0. Not sure
1. No
2. Yes

iii) What types of authentication do you use?

0. Service (Software)
1. Token (Hardware)
2. Hybrid (Combination of both)

iv) Did you install antivirus software in every single PC?

0. Just installed after purchased from vendor
1. Configured correctly after purchased from vendor

v) What type of network do you use in delivering your services to the customer?

0. Internet
1. VPN
2. PN with encryption

vi) What about performance of your internet connection?

0. Slow response
1. Have a little bit problems (Sometime)
2. Completely error free (No delay)

vii) Do you use network protocol security suit like IPSec or SSL or any security certificate?

0. No
1. Yes

viii) What are the solutions to the security issues for securing end-to-end transaction?

0. Hardware-based solutions
1. Software-based solutions involve the use of encryption
2. Hybrid (Combination of the two)

ix) Do you install any recovery tools (e.g. Acornis) in bank PC?

0. No
1. Yes

x) Do you clean and check (physical security) branch computer and other digital devices regularly?

0. Vendor takes the responsibilities
1. When problem is occurred
2. Yes, regularly

xi) In what form data transmit from one location to another?

0. Plain text
1. Cipher text (encryption)

xii) In which device do you use to take data backup regularly?

0. In the server only
1. In the secondary device (DVD/Pen drive/Any other device)
2. Combination of two

xiii) In which site do you preserve your data backup?

0. Inside of branch
1. Outside of branch
2. Combination of both

xiv) Do you retrieve backup data (test basis)?

0. Never
1. After three months
2. In every month

xv) Where is your disaster recovery site?

0. At HO premise
1. Outside of bank premise

xvi) Can customer get access easily in your computer enclave?

0. Yes
1. Depend
2. No

xvii) Do you install CCTV in all important branches to detect fraud and forgeries?

0. No, it is available at few branches
1. Yes, it is available at all branches

xviii) Does branch face any communication failure during distance transactions?

0. Yes, most of time
1. Yes, sometime
2. No, never

xix) Do you conduct short and test audit on branch IT infrastructure regularly?

0. No
1. Yes

xx) Who conducts IT audit?

0. General executives
1. IT executives
2. Combination of two

xxi) Do you have any ICT security check list to maintain security?

0. No
1. Yes

xxii) Do you think that IT audit team checks banking specific software security system (e.g. Officers' User name and password nomination, cancelation, password change timely, database security, network security etc.)?

0. No
1. Yes

xxiii) Do you check daily transaction list of branch after transaction?

0. No, we don't check
1. Yes, we check

xxiv) Who checks the list?

0. Checking by the IT officers
1. Checking by the general officers

xxv) Do you send IT experts to monitor ATM booth during servicing by the vendor?

0. No
1. Sometime
2. Regularly

xxvi) Do you think that your system has no vulnerabilities at all?

0. A little bit vulnerabilities
1. Yes, no vulnerabilities

xxvii) Do you have sufficient security measures to render services?

0. No, not sufficiently, it is necessary
1. Yes, absolutely

xxviii) Do you think that IT security has an impact on business image?

0. No
1. Yes, moderately
2. Yes, strongly

xxix) Do you think secured e-banking can simultaneously minimize transaction costs, increase profit and reputation, gain competitiveness and accountability of bank?

0. No
1. Little bit
2. Yes, of course it is

xxx) Do you think that e-security can minimize the core risks of bank (e.g. ICT security risk, Internal control and Compliance risk, Assets - Liability risk, Money Laundering risk, Credit risk, Foreign Exchange risk and Environmental risk)?

0. No
1. Little bit
2. Yes, strongly

xxxi) Can you provide your services timely (no delay) and error freely?

0. No
1. Yes but sometime we faced technical problems
2. No delay or error at all

xxxii) Do you think that customers are fully satisfied about availability and reliability of branch internet connection?

0. No
1. Partially
2. Fully

xxxiii) Do you think that existing laws and regulations in Bangladesh relating to e-banking are sufficient for banking operation and maintain security?

0. No, it can be amended or added
1. Yes, it is sufficient

Section (2): Impact of e-banking security adoption issues for the commercial bank (Semi-Structured interview question)

This section aims to collect information of e-security system adoption by e-bankers and its impact on bank business. Please answer the most appropriate reason for these questions.

i) Do you thing e-banking is a new trend in Bangladesh and it has been facing serious vulnerabilities (open for possible attack)?

ii) Do you thing that proper e-security system adoption has positive impact on e-banking vulnerabilities?

iii) ICT security risk is interrelated and interconnected with other core risks (i.e. credit risk, money laundering risk, environmental risk, internal control and compliance risk etc.). Make your comment.

iv) Do you think nowadays banks' commercial success is depending on proper e-security system adoption issue for automated commercial bank?

v) Customer satisfaction is profoundly depending on e-security system adoption issue, do you think that?

vi) Customers are not adopting e-banking in our country because improper security measures taken by the e-bankers, do you think that?

vii) What is your perception regarding e-banking, which one is first either security or service?

viii) Do you follow all the e-banking related security instructions given by regulatory authority (i.e. e-banking risk management guideline presented by Basel committee)?

ix) Do you think you have ensured security in every layer of OSI (seven layers of open system interconnection) architecture? What is your comments regarding e-banking of SBL?

x) Do you think that security measure is necessary to minimize banks core risks and gained commercial success or competiveness?

Appendix- III

Section (3): Major Vulnerabilities and Security related information of e-banking for bank customers

Identification of Respondent

Name of the respondent :

Bank & Branch :

Contact number :

Kind of Customer : Depositor/Borrower/Remitter/Remitter

The questionnaire set is exclusively for the customers of Sonali bank ltd. and Dutch Bangla bank ltd. This section aims to collect information on existing e-banking transactions related vulnerabilities and security of e-banker (commercial banks). Please answer by circling the appropriate number.

1. Do you think that electronic banking or online banking is fully safe and secured?
    I. No/ I don't know
    II. Partially safe and secured
    III. Yes, safe and secured
2. Do you think that you have a safe transaction through e-banking?
    I. No/ I have no idea
    II. Partially safe
    III. Yes fully safe
3. Are you able to send/receive your money timely by e-banking?
    I. No
    II. Sometime it is
    III. Yes timely
4. Do you think that there is no threat for banking transaction by e-banking?
    I. Yes
    II. Partially
    III. No

5. Are you satisfied with e-banking service providing by banks?
    I. No, not fully satisfied
    II. Partially satisfied
    III. Fully satisfied
6. Types of difficulties faced by you regarding transaction.
    I. Transaction never response timely or employees are not co-operative
    II. Yes, there is no difficulties
7. Do you face any difficulties regarding interest imposed against your account?
    I. Yes
    II. No
8. E-banking is better than manual banking but what the problem within the system you felt?
    I. I/We fear about security and it is not user friendly
    II. Sometime we faced communication failure
    III. It should be more user friendly and time oriented
9. What type of problem you faced during transaction?
    I. Operational (communication failure, bank people, environment etc.)
    II. Technological
    III. Others
10. Do you have any comment regarding e-banking security?

Bibliography

Books:

Andress, Jason. *The Basics of Information Security, Understanding the fundamentals of InfoSec in Theory and Practice.* New York: John Wiley & Sons, *1998.*

Ferrell, O.C., Fraedrich, John and Ferrel, Linda. *Business Ethics: Ethical Decision Making and Cases*. Boston: Houghton Mifflin, 3rd ed., 1997.

Gasser, Morrie. *Building a secure computer system.* New York: Van Nostrand Reinhold, 1988.

Kondabagil, Jayaram. *Risk Management in Electronic Banking: Concepts and Best Practices*. Singapore: John Wiley & Sons (Asia), 2007.

Lehtinen, Rick and Sr. Gangemi, G.T. *Computer Security Basics.* Gravenstein Hwy N Sebastopol: CA O'Reilly Media, 2006.

P.fleeger, Charles and Pfleeger, Shari Lawrence. *Security in Computing.* New Jersey: Pearson Education Inc., 2003.

Parker, Donn B. *Fighting Computer Crime: A new Framework for Information Security.* New York: John Wiley & Sons, 1998.

Sekaran, Uma. *Research Methods for Business: A Skill Building Approach*. New Delhi: Shakti Packers, 2009.

Stallings, William. *Cryptography and Network Security- principles and practice.* New Jersey: Pearson Education Inc, 2006.

Journals and Articles:

Ahmad, Dhurgham T and Hariri, Mohammad. “User Acceptance of Biometrics in E-banking to improve Security.” *Business Management Dynamics* 2, no.1 (2012):01-04.

Ahmed, S.M. Sohel et al. “Problems and prospects of mobile banking in Bangladesh.” *Journal of Information Engineering and Applications* 1, no.6 (2011).

Alam, Mohammed and Khokhar, Atiq ur Rahman. “Impact of the Internet on Customer Loyalty in Swedish Banks.” *Department of Business Administration and Social Sciences Division of Industrial marketing and e-commerce,* Lulea University of Technology (*2006).*

Al-Amin, Syeedul. and Rahman, Sk. Saifur. “Application of Electronic Banking in Bangladesh: An overview.” *Bangladesh Research Publications Journal* 4, Issue. 2 (July-August 2010).

Ali, Muhammad Mahboob. “E-business and on-line banking in Bangladesh: an analysis.” *Banks and Bank Systems,* Volume 5, Issue 2 (2010).

Bairagi, Anupam Kumar *and* Nahid, Abdullah-Al.” A new approach of e-banking through the use of mobile, post-office and VPN in the perspective of Bangladesh.” *International Journal of Computer and Information Technology* 2, Issue.1 (July 2011).

Biswas Shyamapada, Taleb, Abu and Shinwary, Salman Salem. “Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges.” *Canadian Journal on Scientific and Industrial Research* 2 no. 5 (May 2011).

Brar, Tejinder Pal Singh. Sharma, Dhiraj and Khurmi, Sawtantar Singh.” Vulnerabilities in e-banking: A study of various security aspects in e-banking”. *International Journal of Computing & Business Research.* ISSN (Online): 2229-6166, 2012.

French, Dr. Aaron M. “Case Study on E-Banking Security – When security becomes too sophisticated for the user to access their information.” *Journal of Internet Banking and Commerce* 17, no.2 (2012).

Frimpong, Twum and Kwaku, Ahenkora. “Internet Banking Security Strategy: Securing Customer Trust.” *Journal of Management and Strategy* 3, no. 4 (2012).

Gupta. Ankur. “Data Protection in Consumer E-banking.” Journal of Internet Banking and Commerce, *11. no.1 (April 2006).*

Haq, Shamsul and Khan, Bilal Mustafa. “E-banking challenges and opportunities in the Indian banking sector.” *Innovative Journal of Business and Management* 2, no. 4 (July-August 2013.

Hertzum, Morten et al. “Usable security and e-Banking: Ease of use vis-a-vis security.” *Australasian Journal of Information Systems* 11, no. 2 (2004).

Ian Ndlovu and Mlungisi Sigola. “Benefits and Risks of E-Banking: Case of Commercial Banking In Zimbabwe.” *The International Journal of Engineering and Science* 2, Issue. 4 (15 April 2013).

Kabir, Md. Ekramul et al. “Uniform payment system for banking industries: A case study in Bangladesh.” *International Journal of Computer and Electronics Research* 2, Issue 2 (April 2013).

Kasemsan, M. L. Kulthon and Hunhgam, Nantana. “Internet Banking Security Guideline Model for Banking in Thailand.” *IBIMA Publishing* 2011 (2010).

Khan, Saadullah. “Adoption Issues of Internet Banking in Pakistani’ Firms.” *Department of Business Administration and Social Science Division of System Sciences,* Lulea University of Technology *(2007*).

M.L.Kulthon Kasemsan and Nantana Hunngam. “Internet Banking Security Guideline Model for Banking in Thailand.” *Communications of the IBIMA* 2011 (2011).

Malami, Abu Bakar. “Security Threats of Computerized Banking Systems (CBS): The managers’ participation in Malaysia.” *International Journal of Economics and Finance studies* 4, no. 1 (2012).

Maruf, Ashiquddin Mohammad, Islam, Md. Rabiul and Ahamed, Bulbul. “Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies.” *The Northern University Journal of Law 1 (2010).*

Mhamane, Sunil S and Lobo, L.M.R.J. “Use of Hidden Markov Model as Internet Banking Fraud Detection.” *International Journal of Computer Applications* 45, no.21 (2012).

Omariba, Zachary B., Masese, Nelson B. and Wanyembi, Dr. G. “Security and Privacy of Electronic Banking.” *International Journal of Computer Science* 9, no. 3 (July 2012).

Peotta, Laerte et al. “A formal classification of internet banking attacks and vulnerabilities.” *International Journal of Computer Science & Information Technology* 3, no 1 (February 2011).

Rahman, Dr. Md. Habibur. Uddin, Dr. Mohammed Nasir and Siddiqui, Sayeed Ahmed. "Problems and Prospects of E-Banking in Bangladesh." *International Journal of Scientific and Research Publications* 2, no. 7 (July 2012).

Rajpreet, Kaur Jassal and Ravinder, Kumar Sehgal. "Online Banking Security Flaws: A Study." *International Journal of Advanced Research in Computer Science and Software Engineering* 3, Issue 8 (2013).

Ramakrishnan, Ganesh. "Risk Management for Internet Banking," *ISACA* 6 (2001).

Redwanuzzaman, Md. and Amirul Islam, Md. "Problematic Issues of E-Banking Management in Bangladesh." *Asian Business Review* 3, no. 3 (2013).

Roy, Mihir Kumar, Hassan, Sk.Kamrul.; and Bhuiyan, M.M. "Online Banking in Bangladesh: An Empirical Analysis." *ASA University Review* 5, no. 2 (July–December 2011).

Sarma, Gunajit and Singh, Pranav Kumar. "Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication." *International Journal of Pure and Applied Sciences and Technology* 1, Issue 2 (2010).

Shafei, Reza. and Mirani, Vala. "Designing a model for analyzing the effect of risks on e-banking adoption by customers: A focus on developing countries." *African Journal of Business Management.* 5, no.16 (18 August 2011).

Shazmeen Syeda Farha, Prasad Shyam. "A Practical Approach for Secure Internet Banking based on Cryptography." *International Journal of Scientific and Research Publications* 2, Issue 12 (December 2012).

Sheikh, Bilal Ahmad and Rajmohan, P. "Interne Banking, Security Models and Weakness." *International Journal of Research in Management & Business studies* 2, Issue 4, (October-December 2015).

Singh, Supriya. "The Social Dimensions of the Security of Internet banking." *Journal of Theoretical and Applied Electronic Commerce Research* 1, Issue 2 (August 2006).

Sokolov, Dmitri. "E-Banking: Risk Management Practices of the Estonian Banks." *Institute of Economics at Tallinn University of Technology (*2007).

Solanki, Prof. Virender Sing. “Internet banking: A study of regulatory, supervisory & management issues.” *ZENITH International Journal of Business Economics & Management Research*.2, Issue 5 (May 2012).

Tshinu, Simon Mukenge. and Botha, Gerrit. “An Integrated ICT Management Framework for Commercial Banking Organisations in South Africa.” *Interdisciplinary Journal of Information, Knowledge, and Management* 3 (2008).

Usman, Ahmad Kabir. “Strengthening E-Banking Security Using Keystroke Dynamics.” *Journal of Internet Banking and Commerce 18, no.*3 (*December 2013).*

Vrincianu Marinela and Popa Liana Anica, **“**Considerations regarding the security and protection of e-banking services consumers’ interest,” *Amfiteatru Economic* 12, 28 (2010).

Xin, Tong and Xiaofang, Ban. “Online Banking Security Analysis based on STRIDE Threat Model.” *International Journal of Security and Its Applications* 8, no.2 (2014).

Organizational Reports & Documents:

Bangladesh Bank, *Bangladesh Payment and Settlement Systems Regulations-2014,* Dhaka: Published by Bangladesh Bank, 2014.

Bangladesh Bank, Banking *Regulation & Policy Department,* BRPD Circular no.02, February 2011. Dhaka: Published by Bangladesh Bank, 2011.

Bangladesh Bank, *Guideline on ICT Security For Scheduled Banks and Financial Institutions*, Version 2.0, April, 2010*.* Dhaka: Published by Bangladesh Bank, 2010.

Bangladesh Bank, *Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions*, *2005.* Dhaka: Published by Bangladesh Bank, 2005.

Bangladesh Bank, Risk *Management Guidelines for Banks, February*, Dhaka: Published by Bangladesh Bank, 2012.

Bangladesh Computer Council, *Information Security Policy Guideline, Bangladesh (Draft) 2013. Dhaka: Published by* BCC and MoICT, 2013.

Bank for international settlement, Bessel Committee on banking supervision, *Risk Management Principles for Electronic Banking,* 2003.

Bank for international settlement, Bessel Committee on banking supervision, *Core Principles for Effective Banking Supervision,* September, 2012.

Dutch-Bangla Bank Ltd., *annual report* , 2013, Dhaka: Published by Dutch-Bangla Bank Ltd.

Ministry of Information and Communication Technology (MoICT), Government of the People's Republic of Bangladesh, *E-service Rule -2013. Dhaka: Published by* Ministry of MoICT, 2013.

Reserve Bank of India, *IT Governance Series: Information Security Governance for the Indian Banking Sector,* Version 1.0, November, 2011.

SANS Institute, *Understanding Security Using the OSI Model*, March 2002.

Sonali Bank Limited, *Guideline on Information & Communication Technology,* 2010, Dhaka: Published by Sonali Bank Limited, 2010.

The World Bank, *Electronic Safety and Soundness: Securing Finance in a New Age,* October 2003.

The World Bank, *Electronic Safety and Soundness: Securing Finance in a New Age,* October 2003.

The World Bank, *Electronic Security: Risk Mitigation In Financial Transactions*, June 2002.

Sub-Group on Information Security Governance

The World Bank, *Electronic Security: Risk Mitigation In Financial Transactions,* June 2002.

United State Computer Emergency Readiness Team (US-CERT), *Ten Ways to Improve the Security of a New Computer,* USA: US-CERT 2012.

Conference Paper

Lasheng, Yu and Placide, Mukwende. “Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services.” *International Computer Science and Computational Technology* Huangshan, P. R. China, 26-28 December 2009.

Roundtable Discussion

Chowdhury, Professor S A et al. “Electronic Payment System in Bangladesh: Pros and Cons.” A Roundtable discussion organized by Eastern Bank Ltd. and The Daily Star at Dhaka Bangladesh, June 05, 2014.

Periodicals:

“Cyber humki mokabilai projon tathogen o prostuti.” *The daily Prothom Alo, Dhaka.* October 28. 2015.

“New vulnerability discovered in common online security.” *ScienceDaily* March 2. 2016.

BBC Online. “Public apology for data theft.” *The daily Star, Dhaka.* January 21, 2014, 16.

Byron, Rejaul Karim. “Sonali’s treasury blamed for illicit cash transfer.” *The daily Star, Dhaka.* March 2, 2014, sec. Business

FE report. “BD banks face 300 malware attacks every day.” *The Financial Express, Dhaka.* May 7, 2016, sec. Economy.

Hasan, Sohrab and Islam Fakhrul. “Krendio bank-er karmokotara jorito,” *The daily Prothom Alo, Dhaka.* March 18, 2016.

Hashim, Syed Mansur. “Ill prepared to face cyber crimes.” *The daily Star, Dhaka.* February 4, 2014, 6.

https://www.sciencedaily.com/releases/2016/03/160302084557.htm

Huda, Shamsul. “Central bank to take actions against unauthorized money transfer.” *The Financial Express, Dhaka.* April 28, 2015, 1.

Islam, Khairul. “Plan to craft strategy as cyber crimes crank up.” *The Financial Express, Dhaka.* May 14, 2015, sec. Trade & Market.

Khaier, Abul and Ahsan, Jamiul. “Krendio bank reserve server-er data gayab,” *The daily Ittefaque, Dhaka*. March 17, 2016.

Kline, Alan. “Fifth Third CEO: Social Media Keeping Banks Honest.” *American Banker, USA.* September 24, 2013.

Lucas, L Daxim. “$100-M laundering via PH banks, casinos probed.” *Philippine Daily Inquirer,* March 8, 2016.

Mmun, Abdullah. “Internet domain.bd vulnerable to hacking.” *The daily Star, Dhaka.* May 6, 2014, sec. Business

Rahman, Sajjadur and Byron, Rejaul Karim.”Hackers active.” *The daily Star, Dhaka.* February 23, 2016, 1.

Rahman, Sajjadur. “Hackers steal $100m from BB account.” *The daily Star, Dhaka.* March 8, 2016, 1.

Reuters, Dhaka/Boston. “SWIFT technicians left BB vulnerable to hackers.” *The daily Star, Dhaka.* May 9, 2016, p.1

Reuters. “Bangladesh Bank exposed to hackers by cheap switches, no firewall: cops,” *The daily Star, Dhaka.* April 22, 2016, sec. business, banking

Reuters. “Hackers compromised SWIFT software, warning to be issued,” *The Financial Express, Dhaka.* April 25, 2016, sec. economy

Sarkar, Tapan Kanti. “Star Business Report. “Cyber threats and security.” *The daily Star, Dhaka.* May 3, 2016, Sec. Business

Sposito, Sean. “Digitally ID'ing Customers: An Inexact Science.” *American Banker, USA,* October 7, 2013.

Staff report. “Tin bank-er chai booth-e jaliater jantra,” *bdnews24.com.* February 2, 2016.

Star Business Report. “Atiur seeks help to beef up banks' IT security.” *The daily Star, Dhaka.* October 16, 2011.

Star Business Report. “Banks, telcos seek access to national ID database.” *The daily Star, Dhaka.* May 11, 2014, Sec. Business

Star Business Report. “How infected ATMs gave away millions of dollars.” *The daily Star, Dhaka.* October 13, 2014, sec. Business.