Abstract

Cyber and technology related crime is gradually increasing in Bangladesh. The advancement of e-banking technology has made banking transactions very convenient. But the misuse of information technology has brought undesirable consequences in the form of diverse cybercrimes. This paper focuses on developing a conceptual framework regarding the problem of cyber-crime in the banking sector of Bangladesh by assessing the cyber-crime scenario. One of the most important aspect in the Bangladesh banking sector is to make banking transactions free from cyber-crime. The purpose of this study is to represents the concept of the basic crimes occurred in banks and financial sector- namely Automated Teller Machine (ATM) frauds, E-Money Laundering etc. The study found that by applying the updated technology and appointing skilled manpower and devices cyber-crime can be reduced from the banking transactions.

Keywords: Banking sector, Cyber-crime, Internet, ATM, E-money Laundering.
1. Introduction

In the present global scenario, information technology is the most critical and disputable term. It is the most intense innovation which is quick and precise in all areas. Expanded use of Information & Communication Technology, like computers, mobile phones, Internet, and other related developments are responsible for not only creative activities but destructive activities also. The destructive activities are considered as cyber-crime, which includes credit card fraud, spamming, e-money laundering, ATM fraud, Phishing, Identity theft, Denial of Service in the banking sector.

2. Problem Statement:

The dependency of individual as well as institutions on internet is raising the cyber-crime as a growing concern. The increased use of ICT is boosting the hazard of cyber-attacks across the globe. Since the incidents of cyber-crimes are on the rise, it is essential to explore the cyber crime scenario. Although, with the initiation of technologies, the banking sector has been able to reach more customers however, it has also increased the risk for customers who often feel hesitant and insecure in opting for such services. The objective of the study is to provide a conceptual overview about the cyber-crimes in the field of finance and banking sector of Bangladesh. This paper is an attempt in this direction to better understand the electronic crimes in the banking sector of Bangladesh and to take some precautionary measures.

3. Methodology:

The study is descriptive in nature. This study is conducted on the basis of secondary data. The secondary data are collected from the journals and research papers. Newspaper articles and the internet sources are also used. But the data has been interpreted in the light of the objectives mentioned earlier.

4. Review of Literature: Cyber-crime in Banking Sector

According to Douglas and Loader (2000), Cybercrime can be defined as computer facilitated activities accompanied through global electric networks either illegally or illicitly by definite entities.

In the banking sector, Illegal money transfer and removal from one to another account are identified as banking fraud according to Wall (2001). He has also classified cyber-crimes into four broad categories i.e. cyber-deceptions, cyber-violence, cyber-trespass, & cyber-pornography. The banking frauds are classified under cyber-deception which is termed as an immoral activities including credit card fraud stealing, and intellectual property violations (Anderson & Barton, 2012).

ATM frauds, E-money Laundering and Credit Card Frauds are the most witnessed cybercrimes in the banking sector. In general, all the frauds are executed with the goal of accessing user’s bank account, stealing funds and transferring it to some other bank account. In some cases the cyber criminals uses the banking identifications i.e. passwords, e-PIN, certificates, etc. to access client’s accounts; whereas in other cases they may want to steal and transfer money the funds into another accounts illegally. The intention of cybercriminals sometimes is just to harm the image of the banking firm and therefore, they block the bank servers blocking the access of clients’ accounts (Claessens et al., 2002; & Hutchinson et al, 2003).

The defense system of banking sector contains a lot of exposures, so there is always a need for investigation for increasing awareness about the procedures that can be undertaken to contest cyber related crimes in the banking sector. (McCullagh, 2005 & Florêncio, 2011).

Moore et al (2009) focused on the subject of online crime which generally occur from the annoyance came from sloppy hackers. They found that substantial developments are possible in the way dealing with online fraud and to study the online crime it is suggested that to understand its economic perspective. It also revealed the problems that banks and police forces face in governing the traditional law enforcement.

Nsouli. M and Schaechter. A(2002), states that online banking crime which is committed with the use of online technology to steal money illicitly from a bank account or means of shifting money. Cyber-banking crime can be considered as another method of identity theft which is regularly made imaginable via methods such as Phishing.

Liao.Z and Cheung.H,(2008) revealed in their study that customer interaction with the internet assisted online banking are the ease of use, security convenience, and also responsiveness to services requirements. They also suggested, for preventing cyber-banking crime: protecting antivirus & firewall,
5. Cyber-crime - An Overview

Computers, Internet and other electronic medium are the tools that make possible the instant exchange and distribution of data, images, and materials. The fraudulent activities of IT are termed as cyber-crime, e-crime, hi-tech crime, or electronic crime. These practices involve the use of computer or internet as a medium, source, instrument, target, or place of a crime.

Computer and Internet plays a key role in various activities, such as, recording financial transactions, routing telephone calls, measuring power usage, monitoring medical treatments, etc. However, they also contribute to electronic crime, such as:

- **Cyber Stalking**: Cyber Stalking means following every moves of an individual over internet. It can be done with the help of many protocols available such as e-mail, chat rooms, user net groups etc.

- **Phishing**: It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.

- **Hacking**: Hacking is a simple term which means illegal intrusion into a computer system without the permission of owner/user.

- **Denial of Services**: This is an act by the criminal, who floods the bandwidth of the victim’s network or fill his e-mail box with spam mail depriving him of the services he is entitled to access or provide, or when internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

- **E-mail Spoofing**: A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

- **Spamming**: Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

- **Cyber Defamation**: This occurs when defamation takes place with the help of computers and or the internet. e.g if someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information

Although, Internet and web technologies are growing at a fast pace and are providing new opportunities, they are also consisting of certain threats like, email espionage, credit card fraud, spams, software piracy, etc.

6. Cyber-crime scenario throughout the world

The Global Economic Crime Survey 2016, indicates that cybercrime is the one of the economic crimes that has increased, jumping from 4th place to 2nd place globally, which is a sharp rise. Among the survey participants worldwide, reputational harm was viewed as the most damaging effect of a cyber breach - followed closely by legal, investment, or enforcement costs. A popular and effective strategy for targeting banks is to direct email phishing to clients. Mobile and online banking has opened new doors for cybercriminals. To counter these attacks, banks have established procedures to rapidly respond to any attacks and have also started the process of educating customers on security. Consequently, criminals have reacted by creating more sophisticated programs intended to breach online bank accounts, and by subverting the servers and programs to aid their phishing activities; a method known as infrastructure hijacking.

As indicated by the FBI, the most recent pattern by cybercriminals is to pick up employee username/password by utilizing spam and phishing messages, key loggers, remotely accessible trojans. Such attacks were found in September 2012, when the Bank of America and Wells Fargo were among those struck.

In the course of the most recent couple of years, cyber economic crime has developed to a point where it can be classified into the following two categories:

1. **Cyber fraud**: Money related cyber-crime, like, identity and credit card theft causing huge losses. In spite of their prominence, they hardly cause any danger to organizations.

2. **Transfer-of-wealth/IP attacks**: The more serious economic crime confronting businesses is that of internal cyber risk: the stealing of Intellectual Property - trade secrets, R & D information, company strategies, etc. The damage...
could lead to loss of billions of dollars and destroy a company or even a large economic system. These attacks are usually not being anticipated by a company and are difficult to detect.

7. Cyber-crime in Banking Sector: Concepts

According to Jaleshgarri (1999), Banking sector throughout the world was simple and reliable till mid-1990s; however since the initiation of technology, the banking sector experienced a paradigm shift in the phenomenon. In order to enhance their customer base banks introduced many platforms through which transactions could be done effortlessly (Vrancianu and Popa, 2010). These technologies enabled the customer to access their bank finances 24/7 and year around through, ATMs and Online banking procedures. Information Technology (IT) has become a vital part of the banking system. Just like banking is the backbone of the economy, IT has become the backbone of the banking system. It is nearly impossible for banks to provide new financial products without relying heavily on IT. The banking sector is coming up with various progressive changes to transform the "brick-and-mortar" bank branches to an advanced framework of "core banking solutions".

The present contemporary age has replaced conventional financial instruments from a paper based currency to "plastic money" in the form of credit cards, debit cards, etc. This has brought about the vast use of ATM everywhere throughout the world. The use of ATM is convenient but has a negative side, which is manifested in the form of "ATM frauds". Credit card fraud has gotten to be conventional on the internet which affects card holders as well as online sellers.

8. Cyber-crimes in Banking Sector: Across the globe

However, in the last few years, banks all across the globe have perceived cyber-crime as among their top five risks (Stafford, 2013). Some of the major incidents of cyber-crime in past few years are as follows:

- Stealing of personal information of almost 2.9 million credit card customers of Barclays and Santander Banks UK in 2013
- Missing $ 450,000 from bank account of a Pennsylvania school district in 2008
- Transfer of approximate $3 million from bank account of a New York school district in 2009. Some transfers were recovered but $500,000 was withdrawn from the account before the transaction could be reversed.
- Over 400 corporate account takeovers in 2011, which cyber criminals initiated through unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million.
- Creation of fake debit cards and withdrawal of more than $9 million from automated teller machines (ATMs) worldwide by breaching the U.S. payment processor’s computer systems and stealing personal data in November 2009. (Source: FBI Data)

9. Cyber-crime scenario in banking sector of Bangladesh:

In the last few years, the banking sector was the victim of several security breaches:

- On January 06, 2013, Islami Bank Bangladesh site was hacked by Human Mind Cracker.
In 2015, bank accounts of a private bank were hacked and money was withdrawn from them.

On December 2, 2015, Hackers breached the network security of Sonali Bank and took control of its website for a couple of hours. The programmer distinguished himself as a ‘Muslim Hacker’.

In February, 2016, skimming attacks in six ATM booths of three commercial banks.

And the largest e-money laundering in the history of banking occurred in February 2016, when hackers stole $101 million from the Bangladesh bank’s account with the Federal Reserve Bank of New York.

Evidence of hacking in commercial banks demonstrates corruption in the government’s procurement framework where unqualified vendors were selected without proper evaluation of skills and consultation of IT experts.

8.1 Case Study 1: ATM card skimming

The initial shock came after the revelation and complaints recorded because of abuse of ATM machines fitting in with some banks and withdrawal from various private accounts of a lot of cash without approval of the record holders. 14 persons were arrested by the police on 4 March, 2016. It included 12 foreign nationals who were individuals from worldwide cyber-crime fraud-gang. They had deceitfully utilized online networking media furthermore hacked information of individual clients.

Skimming is a procedure utilized by digital lawbreakers to duplicate individual information from the magnetic strip on an ATM card. The criminal fits a skimming device in the card slot of ATM booth. Once a card is swiped through a skimmer, individual data contained on the magnetic strip is perused and put away on the gadget or transmitted remotely to the criminals.

With the card information, they can lead value-based misrepresentation, make new cards with the stolen character and individual data, or offer the cardholder information on the underground market.

The disappointing aspect of this occurrence from the Bangladesh Bank was that, while giving necessary advice to all concerned, they had forgotten to heed their own suggestions and neglected to take satisfactory safety measure of their own institution and its relationship with other associated financial partners abroad, which lead to the largest e-money laundering in the banking sector of Bangladesh.

8.2 Case Study 2: Bangladesh Bank Heist

In February 2016, the stealing of $101 million from the reserves of the Bangladesh Bank has raised question on the exposure of financial institutions to cyber-crime groups. This incident have challenged the ability of existing mechanisms in preventing such incidents. Besides, this theft signified the need for strengthening the international co-operation in tackling cyber-crime.

The hackers retrieved the central bank’s transfer codes and sent payment transfer requests worth $1 billion to the Federal Reserve Bank of New York. They requested the funds of Bangladesh be transferred to a bank in the Philippines. From there, the cash was transferred to at least three Filipino casinos. At the casinos, someone converted the cash into chips for betting and then reconverted the chips into cash. This money was then sent to bank accounts in Hong Kong. An additional fund of about US$ 21 million was also transferred illegally to a third party in Sri Lanka.

The attempt could not be fulfilled in totality following a typing error that alerted one of the routing banks and transaction was stopped. Instead of “foundation” the hackers had spelt it as “fandation”. This prompted a routing Bank—Deutsche Bank to seek clarification from the Bangladesh Bank, which stopped the transaction.

Spelling mistake prevented the illegal shifting of money. But the hackers were successful in siphoning $81 million in the initial four transactions.

The theft of such a large amount from national reserves astonished many in Bangladesh and abroad. Doubts are being expressed about the country’s readiness to protect its financial infrastructure, which is undergoing digitization. Different investigations are being carried by various enquiry commissions like FBI, Bangladesh Banks appointed committee & CID officials of Bangladesh. Bangladesh investigators have identified at least 20 foreign nationals who they claimed were involved in the cyber heist till date.
10. Is it an Alarming issues for banking sector?

Recurrence of such incidents will affect the economy. Protecting financial sectors from future cyber-crimes is of greatest concern at this moment. Given the rising occurrences of cyber-crimes in Bangladesh, there is critical requirement for redesigning the nation’s monetary groundwork offering administrations over the electronic network.

The government has also formulated a cyber security law. Despite that, there are uncertainties over preventing the culprits of such violations may be difficult unless it gets assistance from international community. The global cooperation can be focused on areas like international safety standard, training and information sharing. An international Cyberpol can be established more in the line of the Interpol. Unfortunately, it appears that the regulatory regime regarding control of cybercrime or server management (in the case of e-commerce) is weak in Bangladesh. For this, easily exploitable laws, cyber-criminals use developing countries like Bangladesh in order to evade detection and prosecution from law enforcement. Laws against cyber-crime in our country is weak or sometimes nonexistent.

11. Ensuring Cyber Security Governance:

This incidents persuaded the Bangladesh Bank recommending to all Banks and financial institutions to ensure cyber-security governance i.e.:

- Taking measures for ascertaining existing technical gap assessment and vulnerability through a comprehensive cyber security risk study.
- Treating cyber security as a collective responsibility by all financial institutions.
- Installing Anti-skimming devices to the ATM booths.
- Use of EMV (Europay, Mastercard & Visa) Standard card to avoid skimming.
Such measures were recommended by the Bangladesh Bank because such cyber-attacks were seen as being capable of causing financial loss and creating a reputational risk. They should also emphasize on:

- Provide IT related training for skill development
- Monitoring over the IT related issues
- Testing hazard incident
- Mandatory adoption of IT related precaution to avoid such incidents.
- Creating customer awareness

A model can be followed for cyber risk identification and mitigation. Any organization as well as banks can follow this model:

12. Conclusion

The present conceptual framework has provided a brief overview of ongoing efforts to prevent and control technology and computer related crime, highlighting general trends and development within and outside the banking sector of Bangladesh. The banking industry is constantly experiencing cyber-crimes like ATM fraud, E-money laundering, Credit card fraud, Phishing etc. Since there was no noteworthy incidents of cyber-crime took place in the banking sector of Bangladesh before 2016, there was no
urge for such protective measures against those crimes. But now it is high time for the banks to concentrate on cyber risk management and mitigation. So, new technologies and services must be adopted to cope with the situation as well as competition and security governance must be complied with. Technological and legal advancement in the area of banking sector is necessary to overcome the cyber-threats in banking industry. Bangladesh Bank should take necessary steps discussed above to create awareness among the banks and their clients as well as making the application of the laws more rigorous to check crime. As the regulatory authority of the banking sector, Bangladesh Bank should also ensure mandatory compliance of cyber risk management and cyber security governance for the operating banks. There is also a need to bring changes in the Information Technology (ICT) Act to make it more effective to combat cyber-crime.

References:


Federal Bureau of Investigation, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit Washington, D.C. September 14, 2011

Global economic crime survey, 2016,

"How cyber-criminals targeted almost $1 bn in Bangladesh Bank Heist", available at https://next.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8#axzz46NHKzCwH

Jaleshgari, R. (1999). Document trading online. Information Week, 755:


Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: 1