International Journal of Multidisciplinary Education and Research
ISSN: 2455-4588
Impact Factor: RJIF 5.12
www.educationjournal.in
Volume 3; Issue 3; May 2018; Page No. 71-77

Critical discussion of victim, attackers and protectors for an e-banking organization in Bangladesh: Bangladesh Bank (BB)

Md. Abdul Baten
M.Sc Forensic Accounting, Sheffield Hallam University, (SHU), United Kingdom

Abstract
E-banking organization is the backbone of an economy. The attention to the e-banking security is appreciable. The types of attacks to the victim are fatally vulnerable and impede the whole banking system of a country. So that, based on three main key areas, chosen organization 'Bangladesh Bank' will be analysed by the practical tolerance of e-banking which recently affected by the present attack and vulnerabilities.

Keywords: e-banking, banking systems, security procedures, internal control system, perpetrator, cyber attack, victims, vulnerability, protection mechanism

1. Introduction

Current scenario of the business world, the use of internet and e-banking is remarkable within Bangladesh and global business. So that, internet brought some key opportunities for its users like saving of time, transfer of money and shopping online within the global market. On the contrary, these kinds of advantages created some kinds of opportunities to the bankers. In recent picture of business, organization who has the online banking service is the highest victims of fraudster rather than non e-banking organization. For that reason, though Bangladesh Bank (BB) has strong platform of online transactions system but because of its huge business infrastructures sometimes cyber criminals targeted Bangladesh bank as their scope of earning money.

To understand the impact of cyber-attack on Bangladesh Bank, it needs through discussion about existing attacks and some vulnerability which is badly affected on this chosen bank recently. Following this, the purpose of this paper is to analyse and implications of complex problem by electronic crime on Bangladesh bank throughout the victims, attacker and the protectors. The three key sections will find out the possible threats and protection mechanisms which will focuses by vulnerabilities within the Bangladesh bank.

So beginning with, this paper will focus on key areas of *Banking System* vulnerability. Following that, it will be discussed further about the *Security Procedures* of Bangladesh bank. *At last*, the final part of this paper will consider on the *Internal Control System* of Bangladesh bank which is the key important part of an e-banking organization.

In this paper, it will be discuss critically on the three main areas of victim, attackers and protectors on chosen organization: Bangladesh Bank (BB) in Bangladesh.

2. Banking System- Vulnerability

The preamble of e-banking introduces with various challenges, offer from acceptance, with financial restrictions process (Usman and Shah, 2013). These kinds of challenges are not only related to banking sector but also other national and international authorities are involved. Besides, these kinds of challenge also include the legal challenge, operational, reputational, and regulatory and most importantly security challenges. But, researcher carried various observation in this area and found that, the adoption process of e-banking is the key issues where security system, trust, social impact and user friendly system are constantly remarkable as a (CSF) for the greater success [1]. According to (BIBM, 2013) studied there are 50 fraud cases hit within 14 banks in Bangladesh [2].

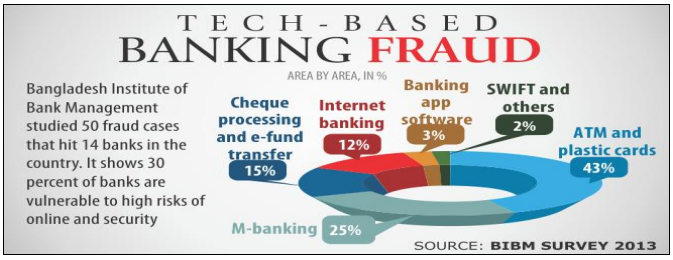


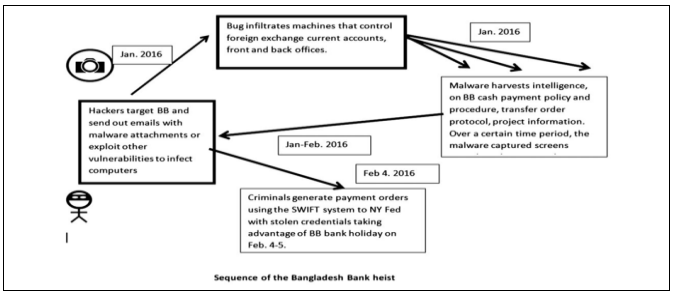
Fig 1

Following this, Bangladesh bank (BB) is a central bank and linked with other major banks in Bangladesh [3]. This is a central bank so it does high volume of transactions all over the world. For those reasons fraudsters main targets BB to earn huge amount of money. Obviously, there are various advantages of e-banking but sometimes these makes strong challenges in Indian reason including Bangladesh (Nigudge and Pathan, 2014). Bangladesh bank heist was happened in January-February, 2016 and causes enormous amount of money loss.

[1] Abu-Shanab, E and Pearson, J (2007). Internet Banking in Jordan. The United Theory of Acceptance and Use of Thchonology, (UTAUT) Perspective. Journal of Systems and Information Techonology, 9(1), 78-97

[2] Hackers active< http://www.thedailystar.net/hackers-active-12573> accessed on 13 May 2016

[3] Bangladesh Bank: Features <https://www.bb.org.bd > Is the central bank of Bangladesh and the member of Asian Clearing Union- accessed on 5 May 2016



***Source*:** The Daily Star 2016

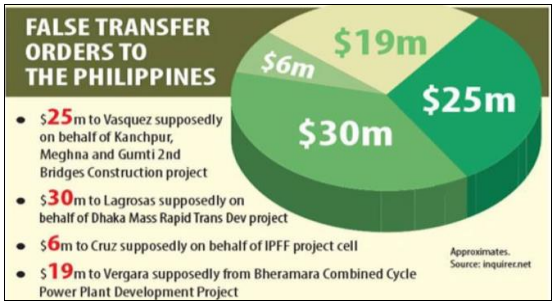
Fig 2

The short summary of Bangladesh bank heist is structured in *(Appendix: 1)*

Hence, though BB is a main bank in Bangladesh but the system of this bank was not standardized with modern banking system. This bank was using cheap £6 router which was a threat of huge damage on security system.

Starting with, financial institutions are the backbone of economic part of a country. If these organizations affected by such kind of security or corruption, the costs of this vulnerability are enormous. In this case, Bangladesh bank had to lose £71m which really a remarkable portion of money of this country's total economy. Following this, the banking system should emphasis on fraud detector with main issues (Kovach and Ruggiero, 2011). They mainly concentrate on some key areas where fraud prone to be happens. The principle areas are *'Device Identification' or* '*Device Control*' [4]. In addition, '*Global Behaviour'* which observes the usurer's position in the global position is also responsible for Bangladesh bank heist. In many cases, security systems are the main culprit where '*Deferential and Global Analysis'* are used to potent whole process of fraud detection. Sometimes, the fraud probability could be identified by *'Suspected list with exponential operation'* which helps to identify the fraud and move to black list from ideal strategy.

Therefore, illiterate, unskilful employees, limited or unstandardized equipment is inadequate for efficient banking system, such threats harmful for modern technology which leads to enormous loss. According to *(Telegraph, 2016)* Bangladesh bank lost about $1bln where $80mln in Philippines *Diagram below*, further details in *Appendix 2*.



***Source*:** Dhaka tribune 2016

Fig 3

And $20 mln transferred in Sri Lanka [5]. This affect will impact not only bankers but also other professionals, and investor in Bangladesh (Chowdhury 2016).

2.1 Incompatible technology in banking sector

Incompatible banking sector means banking system which is not updated with modern technology. Bank is a place of money matter so it should be protected with modern security system. The banking system of Bangladesh is very poor where they used £6 routers and no firewall [6] to run their banking system. For that reason, Cyber criminals found it easy target to get in and rob the money from this bank. As a result, hackers stole £71mln (Economic Times, 2016) from BB in 2016. Moreover, the target of that attack was to gain £700 mln (BBC, 2016). Bangladesh Bank has huge reserve over £19 bln where cybercriminal often targets to embarrass the government, triggered violence, country's development and sometimes raises concern against the foreign exchange reserve. Cyber perpetrator is a part of advanced patient in long-term destiny within a system where hackers stay inside the goal for a period of times, and even for a year. For instance, the cyber offender managed to found that Bangladesh bank has billions of pounds in its current account with other organizations which they used for international transactions around the global ecommerce. In addition, Arun Devnath (2016) noted, hackers took two weeks to investigate the loophole of BB and two bites [7] to earn £663Mln. unfortunately; they were able to swallow £71mln in two big transactions, (*Appendix: 3)* for details information. Obviously, there are lot of ways (who understand cyber world) to steal money from the bank where perpetrator intervene the multifactor authentication. Besides that, Bangladeshi governmental institution and its banking sector are notoriously corrupted where bank frauds are prone to happen. For that reason, people from inside or outside the bank are really questionable. Furthermore, Bangladesh bank heist was enormous and difficult for an individual to drag on while every investigator is suspecting there were other groups or individual like, 20 foreigners [8] were involved in this bank heist.

Hence, the investor of BB unaware about the security system of this bank but if they knew they are aware they would not keep the money onto this bank. Apparently, the weak security system and lack of strong protection equipment it causes this incident. So that, *Jeff Wichman* (cyber firm Optiv consultant) commented, *"You are talking about an organization that has access to billions of dollars and they are not taking even the most basic security precautions,"* Adding to this, the bank which has billions pound of money in reserve and does enormous transaction around the world, how come they have

[4] L.Peotta et al., "A Formal classification of Internet Banking Attack and Vulnerabilities [2011] International Journal of Computer Science & Information Technology 4 (1) (at 193)

[5] Bangladesh Identifies 20 Foreigners as Suspects in Cyber Heist< http://www.bloomberg.com/news/articles/2016-04-18/bangladesh-identifies-20-foreigners-as-suspects-in-cyber-heist-in5qq2eb> accessed in 14th3th of May 2016

[6] Thrifty bank's $10 routers lead to $81 million heist< http://bgr.com/2016/04/22/bangladesh-bank-heist-hackers/> accessed on 14the May 2016

[7] Two Bytes to $951M <http://baesystemsai.blogspot.co.uk/2016/04/two-bytes-to-951m.html?m=1 accessed on 7 May 2016

[8] 20 foreigners linked to $81m Bangladeshi bank heist <http://www.globaltimes.cn/content/979062.shtml > accessed on 10th May 2016

these silly security systems (investigator said).

2.2 Protection Mechanism

It is without saying that, the main reason of this occurrence was poor and unsuitable security system. If the Bangladesh bank has strong protection discipline to this bank then it would not happen. Protection of cyber-crime is implausible in cyber world but it could be eliminated by taking some efficient steps.

Starting with, e-banking system should follow some efficient security pattern which is capable to recognise and mitigate these types of fraud. But researcher suggested that, it is better to take actions before occurrence happen. According to Peotta, L *et al* (2011) presented and discussed many current security models on online banking system where they suggested *"avoid the unauthorised individuals transaction from others account where they are not authorised"*. Bangladesh bank follows the *'ICT* [9] security system guide as a protection method. While response to the attackers, BB followed the (2FA) authentication method. These kinds of protection method can secure the online transaction more secure. But investigation found that, the attacker found the weak point on this area and able to manipulate the system to hack it. However, another protection method is *'Physical Security'* where data centre access should be controlled. Moreover, Bangladesh bank has the '*Environmental security'* where protection of data from the fire, flood, explosion and other form of disaster should be controlled. *At last,* BB has the '*Fire Protection*' when everybody leaves the room, power supply must be switched off.

The notable point is that regarding protection of malicious software [10] in opposition to consumer (*Appendix: 4)* for further details. Nevertheless, Bangladesh bank security protection method was backdated against all the customers and perpetrator are using the most updated software.

3. Security Procedures-Vulnerability

According to (Gordon and Loeb, 2002) information security should care with three kinds of character: confidentiality, integrity and availability within the use of technical decision and corporate deeds. Every business operating systems have kinds of vulnerabilities which are also known as weaknesses within the computerised systems (Landrwhr, 2001). This kind of weakness leads to possible threat and introduces the danger within the security systems. For that reason (Loch, *et al*, 1992; Whitman, 2003) discussed the security threats into various categories such as internal, external, human, non-human and national and international threats. (Table 1) below is the example of such kinds of security threats.

But from the previous studies, researcher found that two third threats are external (McCrohan, 2003) and other fifty to seventy percent threats comes from within the organization (D'Arcy *et al*, 2009). Besides, external threats are not common as internal; they are different and depend on organizational structure. In external threats may include viruses, hack the systems, denial of services attack and block or hang the network systems. In external threats sometimes natural disaster are also hampers the organizational security systems. Moreover, among the all kinds of external threats the main threats concentrates on information security which is the threats happen by hackers and viruses. These kinds of acts are often seen on the security of information systems and ornery process.

Furthermore, in Bangladesh bank heist, the attack was come from external threat. Some unknown hackers managed to install the malware in the Bangladesh central bank's central computer systems and able to spying the all transactions before they attack the banking systems. According to (Quadir, 2016) while they were watching the all transactions they were able to manage some fake transactions by using malware and withdrawing money from the US accounts. The whole process was completed within two weeks and two bites of cyber-attack. Another investigator said that, hackers took more than two months to breach the Bangladesh bank's security systems and tried to steal £700mln from its federal reserve bank of New York.

Table 1: Possible security threats

		Accidental	Intentional
Internal	Human	- Acts by employees - Accidental entry bad data - Accidental destruction of data by employees - Administrative Procedures - Weak/ineffective physical control	- Acts by employees - Intentionally destroy data by employee - Intentional entry of bad data by employees - Unauthorized access by employees
	Non-Human	- Mechanical and Electrical - Program problems	- Mechanical and Electrical - Program problems
External	Human	- Competitors - Media	- Hackers - Denial of Service Attacks - Social Engineering
	Non-Human	- Fire - Earth - Wind - Water	- Computer Virus - Worms - Trojan - Spyware

3.1 Lack of expertise and out-date technologies

In current business world every organization has to use the modern technologies otherwise organization has to face various types of problem. Every threat causes problem where some occur for user error and some occurs the malicious purposes. According to (Kovacich, 2003), the malicious threats occurs by the motivation and capability of agent's threat, where actor modified by access, catalysts, inhibitors and amplifiers the opportunities, (*Appendix: 5)* for possible attack stricture. The motivation could be carried on for various purposes such as personal gain, curiosity, revenge, political and religious reasons. In Bangladesh bank attack case the actor's main goal was to earn enormous amount of money. It is important for the actor capability and motivation while they are attacking any target. At Bangladesh bank case the attacker was so powerful and found weak security system compared any other banks and that is why they attack Bangladesh bank, for them it was an easy attack to earn huge amount of money.

On the other hand, capabilities could depend on the actor's opportunity which includes personality, access to facilities, software, technologies and area of expertise. If the protectors may consist of increasing security level, then the offender cannot perform within malicious acts or more consequences to of improper use of harmful or manipulate higher level data. If the motivator can take control on malicious acts then they could increase the threats on agents to perform on these

[9] Guideline on ICT Security For Scheduled Banks and Financial Institutions< http://www.basis.org.bd/resource/ICT-Security.pdf. accessed on 15 May 2016

[10] Malware suspected in Bangladesh bank hacking< http://news.abs-cbn.com/business/03/11/16/malware-suspected-in-bangladesh-bank-hacking> accessed on 15 May 2016

activities. The peer pressure, fame, and easy access to information may lead by amplifiers which will increase the result in higher strength. According to (Miglani *et al*, 2016) Bangladesh bank became more vulnerable while technicians from the SWIFT connected a new transaction system to messaging. It was happen before three months before £700mln cyber heist which accused by Bangladeshi police. If Bangladesh bank has their own expertise that can fix the transactions to the SWIFT and can control the whole system then the chance of these incident were very less. Obviously, these technicians started the vulnerabilities while they connected SWIFT to Bangladesh's real time gross settlement (RTGS) system noted by Shah Alam (head of the investigation department).

3.2 Protection Mechanism

Every organization must follow some efficient protection policy to prevent their corpora information and increase awareness within their employees. This should be include the companies technological advancement, financial information, customer information and other important sensitive information which could causes to organizational reputations. According to (Barlas *et al*, 2007) importance of security management is the highly remarkable area where technology should give more priority within the organizational security model since 2002. For that reason (Oppliger, R 2003) emphases five categories of security such as Security Policy, Network Security, Host Security and Organizational Security. Following this, all of the aspects of security must introduce its own identity and followed by together to measure security and control the threat over corporate information.

Therefore, Bangladesh bank should follow some necessary steps to protect its own corporate information. In financial organization, the appropriate expertise is considered as key elements of success. If Bangladesh bang has highly qualified people on corporate level or who understands the technology properly they could identify this problem earlier and could avoid this kinds of trap. Obviously, for that reason Bangladesh bank has to spend some amount of money but still it can save them from various kings of external cyber related danger. Bangladesh bank can introduce some potential model for security which will save them from the future attack. The *(table: 2)* below can save any organization from any kinds of attack and save from danger.

Table 2: Security Methods

		Accidental	Intentional
Internal	**Human**	- Policies and Procedures - Security Awareness Training - Employee education - Ethics training	- Policies and Procedures - Audit procedures strengthened - Monitor computer usage - Reporting violations encouraged - Ethics training
	Non-Human	- Update Software	- Company provided software only
External	**Human**	- Security Awareness Training - No outside BBS connections	- Use of passwords - Encryption - Authentication (images, text, etc.) - Security questions - Auto terminal/account logoff - Install and Properly Configure a Firewall
	Non-Human	- Backup procedures schedules - Implement Physical Security Measures - Backup Power Supply	- Authentication (images, text, etc.) - Use of virus scanning software - Protect against Viruses, Worms, and Trojans

If Bangladesh bank follow these kinds of security methods then it will be easier for them to avoid all kinds of danger. Along with, BB has to use up-to-date software and modern technologies which can protect from any kinds of dangerous incident.

4. Internal Control System-Vulnerability

Obviously, it is important to have the effectiveness and efficient information systems for the organization though it depends upon on the culture and the nature of the organization (Smith and Salter, 1992). But it also depends on the appropriate systems or tools and the techniques which will be used for the security reason. Following this, internal control system is a backbone of an e-banking organization. If it is not covered by modern technology then it will be causes to potential vulnerabilities. According to Bangladesh bank guidelines [11] "*internal control is a system or process, frame to give logical commitment about the success of aim in the feasible and efficiency in activities, the authenticity of economic report and consent with contextual laws, rules, and internal policies*". Internal control system is linked with some policies and procedure which are verified that the procedure is compiled with. Internal factors are correlated to external control where one factor causes to threat. But, within the internal control the most vulnerability is come from the organizational changes. Along with, the structure of organization is dependents on the success of the organization. The employees and nature of bank activity are the most important part of an organization. If the employees are not train properly with modern system then it will be very difficult to communicate within the organization. According to FireEye Inc's Mandiant forensics, the Bangladesh bank heist was a sophisticated attack and it was happened within ***'Zero Day'*** by advanced technological power. If the employees of Bangladesh bank are well skilled with this rea of then it would not happen. According to (BBC, 2016) expert, if the better network and hardware would set up within the banking activity system then it would possibly avoid these kinds of attack. *Moreover*, investigator also pointed that there was a lack of enough expertise causes to this huge attack. The connection of financial network is very important to secure because it provides the all private and confidential information

[11] guidelines on internal control & compliance in banks< https://www.bb.org.bd/aboutus/draftguinotification/guideline/icc_riskmanagementguideline.pdf> (page-5) accessed on 13 May 2016

from one place to another place. So that, if this kinds of issue is not consider with updated computerised system then it will causes to huge loss. Investigator of February's attack in Bangladesh bank also found that cyber thieves was able to manipulate and gain access to the Bangladesh bank network because of poor security monitoring system.

Furthermore, quality of personnel (employees) can affect to organizational performances such as limited knowledge on It sector can causes cyber-crime related incident. It is important to secure all of the organization's central system as it always connected to other important part of the organization. Otherwise, it affected negatively with other internal systems within the organization. In addition, the bank security experts believe that the bank should more consider or spent money on the protection of network for its own central system.

4.1 Poor qualified employees

Employees are the most important part of an organization. At Bangladesh bank heist, security expert are saying that the perpetrators had dense information on Bangladeshi organization's internal working activities by the spying of bank workers. According to Mallet and Jakarta (2016), the governor of Bangladesh bank, *Mr Atiur Rahman* [12] resigned and other two officials were fired after the incident happen. Along with; there are various reasons which are directly related to this bank heist. Considering the Bangladesh bank heist, it found that, they were using cheap second-hand router which give them access for the clever hacker into secure computer systems. Another investigation noted that the attack was so vulnerable because it had no firewall. According to SWIFT [13] global payment network, the whole system was so easy for the attacker to understand the poor security system and steal user's credentials. Furthermore, SWIFT servers serve the 5000 computer on the same network rather than being on a walled where all the computer was monitored by one bank employee at all times [14]. On the other hand, the room was so tiny and no window for ventilation ***(Appendix: 6),*** another investigation found that this employee works over the weekend as well and does not take any day off. Reuters also expressed that all transactions are automatically printed by the printer and it was very easy to g*et al*l previous transactions records which was happed prior days where it should be trace by all transaction about its all customers and able to use market appropriate products. The problem is that case bank did not have effective monitoring system of all record of transactions. To secure the banks transactions (Prahalad, 1999) pointed that some of the bank of this days does not have any cross sell products which will secure their confidential records. In this case police also believe that the SWIFT [15] also breaks the laws so they should also take the condemnation.

4.2 Protection Mechanism

While talk about the protection method of internal control system the first thing will come up about the awareness of employees. There are various internal control system could be protected but if the human factor does not properly trained the chance of this attack will be still remain on the cyber world. According to (Basel committee, 2003) on banking supervision suggest for international banks, in three main key area where board and management, security controls, legal and reputational risk management were considered. Among them, in security control area, some key point was mentioned. For example:

- Authentication of e-bank consumers.
- Segregation of duties
- Proper control of e-banking systems
- Data integrity , records and information
- Clear trail of e-banking transaction
- Confidentiality on banking information was considered.

Furthermore, Bangladesh bank revised and expanded on some activities to protect their internal control system. They can take some necessary steps to protect these kinds of huge loss.

Firstly, Bangladesh bank can find out who are responsible for this heist. If any internal people are involved then they need to find out these people and why they are involved this kings of incidents. From the fraud triangle by (Cressey, 1953) it could be learn that why employees are involving these kinds of criminal activities.

Fig 4

The organization has to make sure what the main reason behind this occurrence is.

Secondly, the employees of the organization should give effective training based on their job role. Obviously, if they are not aware or limited knowledge about their duties then these kinds of incident prone to be happen. It is clear that while they should be given the training, organization has to spent some money but organization have to consider how much money are spending on the training purpose and how much is causes to such kinds of incident loss. In the case of Bangladesh bank heist, the estimated loss is up to £71 mln where if they would get proper training from Bangladesh bank, it could cost only couple thousand in a year.

Thirdly, Organization has to use the updated technological equipment to run their work activity. For instance they have to spent money which will make sure their internal control system. Bangladesh bank used only £6 router to connect the computer network which is not enough to securing the modern computing system while all they cyber-criminal and other

[12] Mr Atiur Rahman- he has limited knowledge on technology and had economical background, so that it was difficult for him to follow the efficient technological security systems.

[13] Bangladesh Bank Attackers Hacked SWIFT Software< http://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061> accessed on 13 May 2016

[14] Bangladesh Bank heist: Hackers used bank's $10 routers to steal $81M | BGR< https://steventorresramos.com/2016/04/22/bangladesh-bank-heist-hackers-used-banks-10-routers-to-steal-81m-bgr/> accessed on 13 May 2016

[15] Messaging solutions for banking and payments< https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management. accessed on 14 May 2016

users are using expensive modern routers for their target. One of the investigators of Bangladesh bank noted that, if Bangladesh bank used highly powerful router it could not possible for the hacker to hack the Bangladesh bank and could save millions of pounds.

Therefore, Bangladesh bank heist could be lessens for other within the same industry. Thrifty security control system could lead to huge vulnerability. So that if the organization cautious about their potential security, they could avoid lot of criminal occurrence which could affect not only national but also international level of cyber-attack.

Conclusions

Bangladesh bank is a central bank which supervises the banking system in Bangladesh. Its key activities not only control the countries internal money matter but also it maintains the foreign exchange reserve as well.

The attack of Bangladesh bank causes to fatally harmful for the Bangladeshi economy. *Obviously*, Bangladesh is a developing country within Asian reason so that it will impact on not only in this area but also around the world. The number of cyber-attack is increasing within the developing countries because of limited expertise. But it ominous for every country and every organization. From this type of electronic crime the world can understands and learn the awareness of potential vulnerability within the e-banking organization.

From the above discussion it is clear that all the attack result in a vulnerability which causes to business in financial loss and reputational loss. Besides that, organization that has online banking in particular is spending money to expand their business and sometimes ignoring the securities. Along with, some of the organization is considering the external threat as more priority while internal security is being a higher risks that the external security.

The first issue was found on Bangladesh bank heist is *' banking systems'* not standardized or not up-to-date with current business systems. As a central bank it has to do lots of transaction around the world so that its old banking systems lead to this incident. For that reason Bangladesh bank has to suffer a lot to overcome this situation. If the bank was more cautious about their systems then it would not happen and would not face these kinds of financial loss.

The last vulnerability was mention on poor internal control system with limited skilled employees. These kinds of vulnerabilities are easy to find and take actions against this. In addition, Bangladesh bank is capable to spent money on to recruit skilful human power to do their work activity. Moreover, organization like Bangladesh bank is important part of economy so that, the corporate level management should consider deeply taking necessary steps to avoid these kinds of loss.

At last, though people have different opinion about the security policies of an organization despite them are not following these accordingly though this type of incident could see often. Bangladesh bank should take argent steps to recover this enormous loss by following some regulatory aspect. *Moreover*, Bangladesh bank should aware of future threat and vulnerability by improving their security policy and modernised internal control systems by taking lessons from current phenomenon.

References

1. Basel Committee on Banking Supervision. Risk Management Principles for Electronic Banking[Online]. Available at, 2003. http: //www.bis.org/publ/bcb98.pdf. Accessed on.
2. Barlas S, Queen R, Radowitz R, Shillam P, Williams K. Top 10 Technology Concerns. Strategic Finance. 2007; 88(10):21-23.
3. BBC. $10 router blamed in Bangladesh bank hack [Online], Last update 22 April. Available at, 2016, http://www.bbc.co.uk/news/technology-36110421
4. Chowdhury A. The Bangladesh Bank heist and pitfalls of hasty digitalisation [Online]. Last update 19 March. Available at, http://opinion.bdnews24.com/2016/03/19/the Bangladesh-bank-heist-and-pitfalls-of-hasty-digitisation/
5. Corkery M. Bangladesh bank heist: How hackers mounted an $81-mn sneak attack on a super-safe payment system. [Online]. Last update 1 May, available, 2016. at, http://articles.economictimes.indiatimes.com/2016-05-01/news/72748610_1_swift- worldwide-interbank-financial-telecommunication-Bangladesh-bank
6. Donald RC. Other People's Money: A Study in the Social Psychology of Embezzlement, (Montclair, NJ: Patterson Smith, 1973-1953.
7. Devnath A. Hackers Stalked Bangladesh Bank for Two Weeks Before Big Heist [Online]. Last update 18 March, available at , 2016, http://www.bloomberg.com/news/articles/2016-03 8/hackers-stalked-bangladesh-bank-for-two-weeks-before-big-heist
8. Darcy J, Hovav A, Galleta D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research. 2009; 20(1):79-98.
9. Gordon L, Loeb M. The Economics of Information Security Investment. ACM Transactions on Information and System Security. 2002; **5**(4):438-457.
10. Kovach S, Ruggiero W. Online Banking Fraud Detection Based on local and Global Behaviour. The Fifth International Conference on Digital Society, Guadeloupe, France, 2010, 166-171.
11. Landwehr C. Computer Security. International Journal of Information Security. 2001; 1(1):11.
12. Loch K., Carr H, Warkentin M. Threats to Information Systems: Today's Reality, Yesterday Understands. MIS Quarterly. 1992; 17(2):173-186.
13. Mallet, Jakarta. Bangladesh central bank governor quits over $101m cyber heist. [Online]. Last updated 15 March, 2016. http://www.ft.com/cms/s/0/eee9ba54-ea7d-11e5-888e- 2eadd5fbc4a4.html#axzz492HwvwWV
14. Miglani S, Quadir S, Finkle J. Exclusive: Technicians from SWIFT left Bangladesh Bank exposed to hackers - police. [Online]. Last updated, 9, 2016; Available at http://in.reuters.com/article/usa-fed-bangladesh-swift-idINKCN0Y00KH
15. Mccrohan K. Facing the Threats to Electronic Commerce. Journal of Business and Industrial Marketing.

2003; 18(2):133-145.
16. Nigudge S, Pathan M. E-banking: Services, Importance in Business, Advantages, Challenges and Adoption in India. Asian Journal of Management Sciences. 2014; 2(3):190-192.
17. Oppliger R. Security Technologies for the World Wide Web. 2nd ed. Boston: Artech House, 2003.
18. Peotta L, Holtz M, David B, Deus F, Sousa Jr R. A Formal Classification of Internet Banking Attacks and Vulnerabilities. International Journal of computer science and Information technology (IJCSIT). 2011; 3(1):186-197.
19. Prahalad CK, Krishnan MS. The new meaning of quality in the Information Age'. Harvard Business Review. 1999; **25**(6):109-118.
20. Smith LM, Salter SB. The Impact of Emerging Information Technologies on the Information Flow of Multinational Enterprises'. Southwest review of international Business Research. Proceeding of the southwest Academy of International Business Annual meeting, http://acct.tamu.edu, 1992, 255.
21. The Telegraph. Billion dollar bank heist foiled by hacker's typo, 1992.
22. Quadir S. Malware suspected in Bangladesh bank hacking [Online]. Last updated 12 March, Available at, 2016. http://news.abs-cbn.com/business/03/11/16/malware-suspected-in-Bangladesh-bank-hacking
23. Usman A, Shah M. Critical Success factors for preventing e-banking Fraud. Journal of Internet banking and Commerce. 2013; 18(2):1-13
24. Whitman M. Enemy at the Gate: Threats to Information Security. Communications of the ACM. 2003; 46(8):91-95.