Report for Professional Ethics

Case Study: Bangladesh Bank Heist

Antor Md Ahsan Habib

ID:2600170464-7

Date: 15th July,2017

1.Abstract

In February,2016 there was a hacking transaction worth of nearly $1 billion from Bangladesh Bank's account in New York Federal Reserve Bank. It was presumed that this transaction was made from an official computer of central bank of Bangladesh and it ordered to send these money to Philippine & Sri Lanka by making 35 transactions order. The hacking attempt was interrupted after completing five successful transactions worth of $81 million. Currently the origin of the attack has been connected to the hacker group Lazarus and North Korea.

2. Introduction

We are living in the era of information science. Nowadays, we are putting our all information in internet. It was said that knowledge is power. But if we look at the current world it should be said that information is power. In our digital world, we have made everything based internet such as e-society, e-commerce etc. We cannot go for a single second without internet. Our too much dependency on internet requires strong security system. Because if we fail to keep our information safe, our entire e-system will be collapsed.

Cyber-crime is the threat to our internet system. Day by day, the number of cyber-crime is increasing at random. The National Security Agency(NSA) of US experiences 300 million hacking attempts per day. Besides, 600k Facebook accounts are being hacked every day. Hacking is the culprit for our global village. It is not a problem for a single country, rather it is concerned with the whole world.

Hacking Bangladesh bank's account is a simple evidence how dangerous the cyber-crime can be for our economic world. Everyday our internet economic system is struggling with hacking attempt. Beyond all of the security protocols, banks themselves are responsible for their individual cyber security. This is where hackers are exploiting weaknesses in the system. For example: a hacker group called Lazarus with its subgroup Bluenoroff have targeted and successfully attacked smaller banks in poorer and less developed countries whose own cyber security measures and systems are poorer (Lennon, 2017). It is suspected that there might be inside hand in Bangladesh Bank to make the hacking successful.

3. Description

The first step for the Bangladesh bank attack were made in May 2015, when four bank accounts were opened in Philippine bank for being ready to future transactions. All of the accounts were not used until the day of attack and were clearly established for attack only. The first problem in the audit process was made as none of these accounts or their owners was authenticated in the process to either check the validity of their owners or transactions. During the opening of a bank account this kind of procedure is not unusual. The first corrupted attempt happened in here because the way these accounts were opened is illegal.

In January,2016 a problem detected in Bangladesh Bank firewall system. But they were reckless to mend the problem. After that, the attack itself was started in February, 4 in 2016 by making 35 payment instructions worth of $951M to New York Federal Reserve Bank. The first five transactions were completed without any trouble. After five transactions, it was stopped because of two reasons. The hackers did a spelling mistake & it drew attention of the authorities for the first time. When the money was sending to Sri Lanka, the authority of Sri Lanka bank was surprised to see this huge amount. They stopped the transactions and communicate with the source bank. Then they became sure that the transfer is indeed suspect. As the recipient turned out to be a fake entity, the bank was able to freeze the funds and ultimately return them to the originating bank. Out of the reported total sum $870m of all transactions, the attackers managed to transfer only $81 million.

The Bangladesh asked help from FBI (Federal Bureau of Investigation of US) for investigating this case. According to their repot:

Even though the attacker did try to remove any evidence from the bank's systems, Kaspersky (2017a) managed to access some of the data through backups of the systems. The recovered files indicate, that the techniques and tools used in the attack can be linked to a group known as Lazarus. Kaspersky (2017a) summarizes the activities of the Lazarus group as follows: "It's malware has been found in many serious cyberattacks, such as the massive data leak and file wiper attack on Sony Pictures Entertainment in 2014. Whiling hacking, it is suspected that the IP address is from North Korea. Hence, it is not entirely believable because criminals usually mask their real location and IP addresses by using VPN services and proxies .

4. Application of Theory:

(a) Duty & Right Ethics: The duty & right ethics are divided into two sector for this case study. They are:

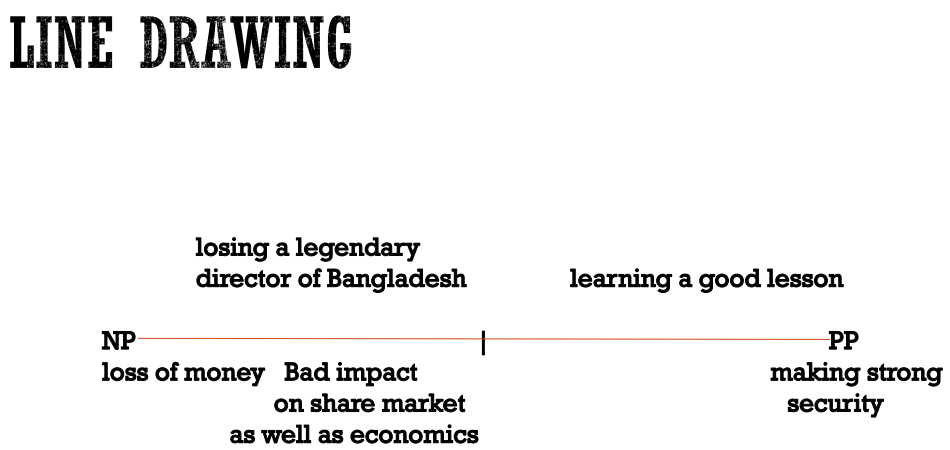
1.What Philippine Bank should do: The way they opened the four account without proper authentication is illegal. Besides, when this huge amount of $81 million was transferred into their bank, they should check & double check those accounts again just like Sri Lanka did. The notable point is that those accounts of Philippine were never used before this huge transaction. Hence, they did not take any step for stopping the transactions. We all know, the best way for money lounging is to put money in Casino because it is the easiest way to turn black money into white money. The Philippine Bank helped the hacker by sending those whole moneys to some casino according to the hacker's order. They didn't have any professional ethics in them. How could they do it? They were entirely corrupted. They should stop the transactions & return it to the main account.

2. What Bangladesh bank should do: The were reckless to the problem of firewall. We all know the proverb "Little should not be neglected". Their lack of professional duty causes $81 million robbery. Besides, according to FBI report, there was inside helper that indicates that some corrupted person was also there to help the hackers. They should be honest to their duty.

(b) Virtue Ethics:

Lack of honesty: People keep their money in bank for safety. They do have faith in the bank that's why they put their money in there. But in this case, it is found that there were some illegal activities in Bangladesh Bank & Philippine bank. They broke the trust of people. They should not do this.

5. Line Drawling:



Explanation of Line Drawing:

Negative Paradigm:

(a) Bangladesh bank has lost $ 81 million money. What else can be more negative point than this?
(b) This accident hampers the aspect of Bangladesh bank to the other countries.
(c) After this accident, the legendary person in the field of the economy of Bangladesh, Dr Atiur Rahman, was compelled to resign because of this.

Positive Paradigm:

(a) The Bangladesh government enhances the security system after this accident.

(b) The investigation is still running to identify the inside helper of the hacking which will help to reduce the corruption. Overall, this incident teaches a good lesson to Bangladesh bank as well as other bank who have a vulnerable security system.

6. Conclusion:

The professional person should have professional ethics in them. In this case study, we have seen that there was a lack of professional ethics in the authority of Bangladesh Bank & Philippine Bank. If they were honest and sincere to their duty, an event such as this would never be happened.

7. References

The Guardian. (2016 a). “Bangladesh central bank governor resigns over $81m cyber heist”. [online] Available at: https://www.theguardian.com/world/2016/mar/15/bangladesh-central-bank-governor-r esigns-over-81m-dollar-cyber-heist [Accessed 21.4.2017].

The Guardian. (2016 b). “Spelling mistake prevented hackers taking $1bn in bank heist”. [online] Available at: https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank -heist . [Accessed 21.4.2017].

The Guardian. (2016 a). “Bangladesh central bank governor resigns over $81m cyber heist”. [online] Available at: https://www.theguardian.com/world/2016/mar/15/bangladesh-central-bank-governor-r esigns-over-81m-dollar-cyber-heist [Accessed 21.4.2017].

The Guardian. (2016 b). “Spelling mistake prevented hackers taking $1bn in bank heist”. [online] Available at: https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank -heist . [Accessed 21.4.2017].

The Guardian. (2016 a). “Bangladesh central bank governor resigns over $81m cyber heist”. [online] Available at: https://www.theguardian.com/world/2016/mar/15/bangladesh-central-bank-governor-r esigns-over-81m-dollar-cyber-heist [Accessed 21.4.2017].

The Guardian. (2016 b). “Spelling mistake prevented hackers taking $1bn in bank heist”. [online] Available at: https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank -heist . [Accessed 21.4.2017].

BDNews24. (2017), CID delays Bangladesh Bank heist report for 13th time,

http://bdnews24.com/bangladesh/2017/04/18/cid-delays-bangladesh-bank-heist-repo rt-for-13th-time , [Accessed 21.4.2017]