Subduing Cyber Threats to Secure the Financial Sector of Bangladesh

Md. Ashabur Rahman

1. Introduction:

The banking system of Bangladesh is being digitalized day by day to provide better and quick service to the customers. At present 59 scheduled banks, 5 non-scheduled banks, 41 private commercial banks and 34 financial institutions are working in Bangladesh to provide banking and financial services to the people of Bangladesh [1]. This sector is facing challenges to keep pace with the modern technological innovation, particularly maintaining its operation due to major security threats which are being faced by the banks as well as their customers.

2. Recent Cyber Attacks:

Fears of cyber-attack on banks have risen after the hacking of nearly $81 million from the central bank of Bangladesh in 2016. Three local private banks were faced cyber-attacks in June 2019 where a private bank lost as much as $3 million and two others were able to prevent financial losses [2]. A recent survey on certain banks about their ability to combat cyber threats shows that 28 percent banks have taken no effective steps to prevent cyber-attack although 38 percent are fully-equipped for combatting such an attack and left 34 percent are partially-prepared [3]. So, cyber security has become a burning issue for the banking sector of Bangladesh. Banks have always been main targets for the cyber-attackers because the assets are cash and customer’s information.

1 He is a contributor from legal sector, presently providing legal service to a reputed financial organization of Bangladesh.
3. Technological Actions for Cyber Security:

To ensure cyber security of the financial services organizations, introducing cutting-edge technologies, artificial intelligence and orchestration are essential. Cutting-edge technology means to use the most recent & high-level IT developments and orchestration is the automated configuration, coordination & management of computer systems and software. The proactive cyber security analysts should be appointed who can use the adversaries’ intelligence which can prevent attacks. The analysts can identify the attacks and components of an adversary campaign by using Tactics, Techniques, and Procedures (TTP). A proactive cyber security tool can also recognize probable adversary TTPs and signs which identify a threat or threatening behavior. The system can act on any traffic that can meet any attacks before reaching inside a network in a way invisible to adversaries. Using this basic model, a cyber-security tool can prevent common exploits and future not yet seen exploits. Moreover, this prevention can bring the real benefit of cutting-edge technologies. The highest threats that a bank faces from cyber-attacks include breach of customer data privacy, loss of reputation, assets and business information. Strong customer data privacy protection policy, cyber security law and cyber security policy of banks are essential to protect cyberspace.

4. Guideline of the Bangladesh Bank:

Bangladesh Bank as the main regulatory body of banking sector of Bangladesh has issued a guideline on ICT security for banks and non-bank financial institutions where ICT security management, prevention and policy implementation systems are discussed. It has also focused on providing ICT related training among the employees, raising technological awareness among the computer system users and using up-to-date security tools. The guideline has also mentioned about the Bring Your Own Device (BYOD) system, which is a latest practice accepted by banks and financial institutions to allow employees to access corporate email, calendars, applications & data from personal devices. It can be helpful in securing, monitoring and controlling employees’ personal devices. The guideline suggests establishing baseline standards to confirm security for
Operating Systems, Databases, Network equipment, portable devices and privacy of sensitive or confidential information [4]. Servers and workstations must be protected from malicious code; software must be regularly scanned. After all, the banks and non-bank financial institutions should create information & communication technology security policy internally to ensure better security against cyber-crimes.

5. Executing Digital Security Law:

The digital security laws applicable in Bangladesh should be executed strictly. The Digital Security Act 2018 has provided some provisions relating to punishment for the cyber crooks of financial sector. The Act says that e-transaction without legal authority through electronic and digital medium of any bank or financial institution is punishable with maximum 5(five) years imprisonment or fine with Tk. 5 (five) lac or both [5, Sec. 30]. If any person commits hacking will be punished with maximum 14(Fourteen) years imprisonment or with fine up to Tk.1 (One) crore or with both [5, Sec. 34]. The law also permits to take regional or international assistance if necessary in case of such crime investigation. Apart from this Act, it has become urgent to sign a Convention in international level to save the financial sector from gradually raising cyber-attacks.

6. Recommendations:

All of the techniques stated in this paper will have to be implemented as soon possible. Reflecting on the mentioned challenges, certain steps can be taken to curb the upcoming cyber-attacks on the financial sector. Such as-

a. Using machine-readable intelligence,

b. Sharing intelligence and security best practices,

c. Setting barriers on the approaches to the bank’s funds and depositors data,

d. Blocking websites and servers used by the cyber crooks as a media for attacks,

e. Using Tactics, Techniques and Procedures (TTP) to prevent attacks,
Using cutting-edge technologies, artificial intelligence and orchestration,

Increasing consciousness among the modern technology users,

Forming cyber security cops to arrest the attackers,

7. Conclusion:

Emergency response team can work to ensure the security of critical information infrastructure if there is any cyber-attack or to prevent possible and upcoming cyber-attacks. Installing anti-skimming solutions on ATM devices, conducting video surveillance for 24 hours, online monitoring for cash balance and disorders of machine can control cyber-attacks. Finally through cooperation, clear identification of the risks and bold action to combat the cyber crooks, the financial sector can address challenges of securing its networks and customers from cyber-attacks.

Reference: