Indentification of Evolving Cyber Threats in the Financial Sectors of Bangladesh

☐ Nadeem Ahmed ☐ Md.Shamsujjoha ☐ Rossi Kamal ☐ Hafiz Md. Hasan Babu

The financial services sector is the largest in the world in terms of earnings. Financial services are enabling businesses to start up, expand, increase efficiency, and compete both in the local and international markets. General people can manage their own assets and able to generate income and options by the help of financial institutions – ultimately creating paths of prosperity. But with the advancement of technologies the financial sectors are losing money and data by the cyber-attacks. This paper identifies the recent cyber threats that are major concerns to us and then follows by preclusion mechanism particularly in the perspective of Bangladesh.

The Financial Sectors of Bangladesh

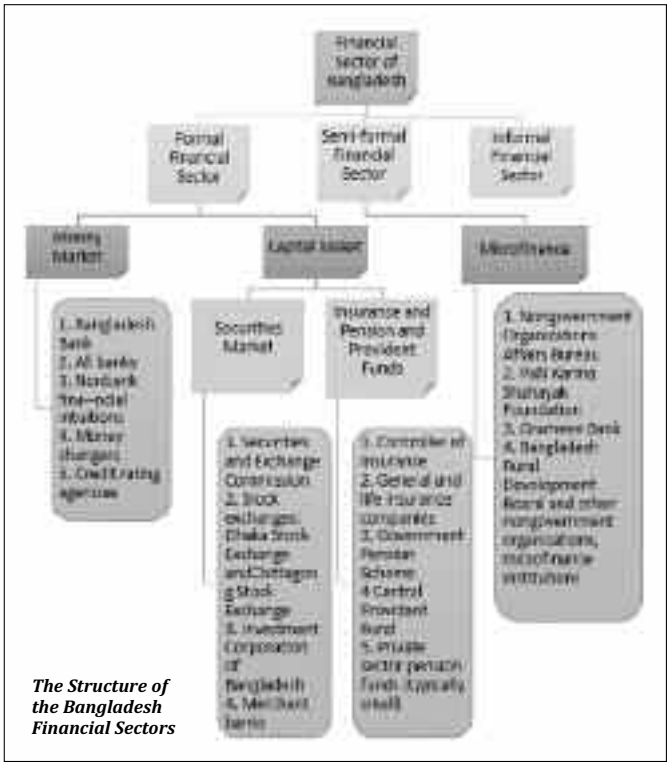
These sectors have been dominated under the stringent directives of government and the Central Bank of Bangladesh (Bangladesh Bank) after the independence of the country on December 16th, 1971 until December 1989. In 1990 the Financial Sector Reform Program was introduced and the Bangladesh Bank almost closed both the refinance and rediscount windows with a vision to developing an inter-bank market. Banking sector always has a dominating role in Bangladesh financial system, which fundamentally depends on short - and medium-term deposits for financing their lending portfolios.

There are three main sectors in the financial system of Bangladesh. The categorization is based on the extent of regulation in the sectors. The first category the formal financial sector is comprised of money market (comprising operations of the banking system, microcredit institutions, nonbank financial institutions, interbank foreign exchange market), the capital market (stock markets), bond market and the insurance market. Operational activities of these institutions in the formal financial sector are governed by a number of regulators such as Bangladesh Bank (banking system), Securities and Exchange Commission of Bangladesh (regulating the stock market operations), Insurance Regulatory Authority (for insurance institutions), and Microcredit Regulatory Authority (micro credit institutions). Ministry of Finance also has some oversight role in certain aspects.

There are 77 insurance companies currently operating in Bangladesh. Although the study found that awareness about insurance had increased in comparison with 2010, the services provided by insurers continued to be relatively limited.

IT Architecture of Bangladesh Financial Sector

At present, just like the advanced world Bangladesh financial sector is heavily dependent on the usage of Information technology. The use of IT is a part and parcel in every section of any financial sector. Every level of employees and as well as customers are the consumers of IT in the financial sector. Detail information of in-depth IT architecture of any financial industry is highly confidential and private. In general, IT architecture is created and maintained by two methods. For multinational financial organizations like HSBC, Standard Chartered, Bank of Ceylon etc., core IT setup, maintenance and control are done by respective regional offices with the help of in-house IT stuffs. For other financial institutions essential IT arrangement and operation are maintained by third party vendor and in-house IT people. In this paper general gestalt of IT design emphasizing on banking industry of Bangladesh is represented.



The Structure of the Bangladesh Financial Sectors

InformationTechnology and the Banking Sectors

There are several departments in the banking sector. The dominant departments are Retail Banking, Corporate Banking, Treasury, Finance, HR, Marketing, Risk and Operation. These departments have further sub-divisions. A local area network (LAN) is formed with these departments.

These departments are centrally connected with the core banking system through an application server and formed a Ring network. There are specialized software systems installed in the application server to connect with the servers. There are branches of a bank all over the country. Local branches are connected area office, area office are connected to divisional office and in turn divisional office are connected to head office. Most of the communications and transactions from local office to head office are done through internet. There are many services provided by the bank for different types money transaction. Cash machine, also known as an automated ▸

teller machine are connected with core banking system with dedicated network. Point of sale (POS) or point of purchase (POP) terminal is connected to core banking through VISA server. General users are connected through internet to the online banking services. Lastly, every bank's core system is connected with Bangladesh Bank.

Threats in the financial Sectors

There are multiple dimensions of threats around the financial sector. Lack of standardization in overall system put the organization in the emergence of different kinds and levels of threats Between 2008 and 2009, U.S. businesses lost more than $1 trillion worth of intellectual property to cyberattacks [8]. These threats in the financial sector can be broadly divided into two categories. 1. The Internal Threats 2. The External Threats. Both types of threats have been described thoroughly.

A. The Internal Threat Components

An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, company or agency. The term may refer to a former employee, service provider, authorized user of internal systems, or contractor. The term also can apply to an external person who poses as an employee or officer by gaining false credentials. The cracker obtains access to the computer systems or networks of the enterprise, and then conducts activities intended to cause harm to the enterprise.

Insider people pose greater threat than remote criminal because generally organization trusts its people and doesn't take or even think that measures are also required from own people. Insiders—company employees as well as contractors and business partners—can present a significant risk for misappropriation of sensitive information and intellectual property. Insiders can knowingly or unknowingly can bring damages to company reputation, make significant loss to company profits and hamper the establishment of future plans.

B. The External Threat Components

External threat is originating outside a company, government agency, or institution which is not belonging the organization itself. It is more challenging to prevent as anyone can attack from any part of the world in an absolute novel fashion where IT experts might be totally unware of such attack and mechanism behind the attack may remain undisclosed.

Threat Management

There should be a proper guideline how the threats can be minimized. Bangladesh Bank published a guideline in last year for Banks and Non-Bank Financial Institutions. This guideline provides a detailed recommendation that how the financial organizations should interact with information technology. Hackers, like all other predators will attack the weakest prey. Security measures should be strong enough so that hackers cannot penetrate the system. Some of the measures have been described.

Most adverse consequence	Loss of confidential/ proprietary data 11%	Reputation al harm 11%	Critical system disruption 8%	Loss of current or future revenue 7%	Loss of customer s 6%
Mechanisms used	Social engineering 21%	Laptops 19%	Remote access 17%	E-mail 17%	Copy data to mobile device 16%
Characteristics displayed	Violation of IT security policies 27%	Misuse of organizatio n's resources 18%	Disruptive workplace behavior 10%	Formal reprimands/ disciplinary action 8%	Poor performa nce reviews 7%
Reasons for committing cybercrime	Financial gain 16%	Curiosity 12%	Revenge 10%	Non-financial personal benefit 7%	Entertainm ent 6%

The causes and consequences of cybercrime committed by insiders.

A. User-Awareness Campaigns

Users should be trained and give proper guidelines so that users take necessary security practices to minimize risks. In this regard social-engineering tests can be conducted.

B. Accepting without Reading

One of the common ways to become infected is to accept license agreement without much attention. For instance: while browsing over the Internet, a pop up window might appear and say that the computer is infected or a unique plug-in is required. By accepting the computer may be infected with malicious program. Users should be aware what is installing in his system.

C. Downloading any Infected Software

Users should be well informed while downloading the software (programs, utilities, games, updates, demos, etc.) via the Internet. Users should run the antivirus and spyware scanners upon completion the downloads. Users can help verify if a website is reliable by using tools such as WOT (Web of Trust).

D. Inserting or Connecting an Infected Hard Disk/Disc/Drive

Any disk, disc, or thumb drive connected or inserted into the computer can be infected with a virus. As long as something is writable, a virus can move from a computer to that disk, disc, or drive. This same rule applies to any networked drive or computer. A common approach used by hackers to gain access to a network is by leaving out a thumb drive with malicious code on it. Then, when a user puts the thumb drive into their computer, it becomes infected with malicious program.

E. Pirating Software, Music, or Movies

Users should aware of using a bit torrent program or some other unlawful exchange of copyrighted music, movies, or software, because there is a high potential of getting infected. There is high chance that these files and programs contain viruses, spyware or malicious software.

F. Use of Antivirus/Adware/Firewall Program

Users should use latest antivirus and adware software with updated patches. Inclusive firewall program should be used that it can pinpoint unauthorized programs attempting to transmit data over the internet. At the same time, there should be a set of rules to allow traffic through the firewall that business transaction requires. A firewall must have its own configurations depending upon the security aspect of organization.

G. Running the Latest Updates

User should original operating system particularly Microsoft Windows. Thus users can update the system on timely basis, particularly those associated security and safety. The plug-ins associated with the browser can also contain security vulnerabilities. Users need to make sure that they have the latest versions of system. Computer Hope tool can check installed plug-ins and their versions. And it is always better to use highly secure Linux based operating system because malicious code cannot be easily and accidently installed in the system. But even people with strong IT expertise face difficulty and discomfort to use Linux base OS.

H. Password Policy

Passwords should be changed on online banking passwords several times throughout the year. Passwords should be mixing of capital-lower case letters, symbols, alphanumeric and non-dictionary word.

I. Monitoring Policy

Business transaction activity should be checked on daily basis. There should be trigger mechanism so that any unusual transaction should be notified immediately either by email or SMS messaging. Also there should be a user monitoring system to observe suspicious user activities.

J. Emails from Unfamiliar Sources

Users should aware of unfamiliar email. Email server should be configured to identify spam email. Spam email contains malicious virus, spyware, botnet or Trojan horse. Even if the message is from a co-worker, friend, or family member, always caution should be taken before opening a link or downloading an attachment.

K. Preformation of Attack and Penetration Tests

By running the attack and penetration tests, vulnerable points in the network can be easily accessed from both external and internal users. The test must be done from both the internal as well as external perspectives to detect all the vulnerable points. It is better to take the help of skilled ethical hackers who have taken special network security training to perform this task successfully.

L. Use Password-less Authentication

Regardless of the policies above, passwords are less secure than SSH or VPN keys so think about using these or similar technologies instead. Where possible, use smart cards and other advanced methods.

M. Use of Proper Hardware Devices

Organization should buy proper hardware devices such as hardware firewall, router, switch, monitoring devices.

N. Delete Comments in Website Source Code

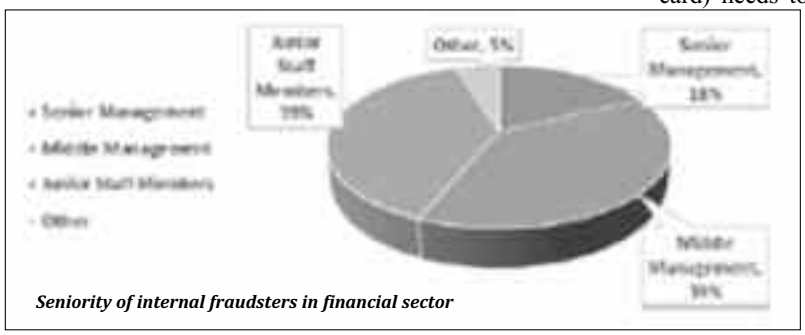
Comments used in source code may contain indirect information that can help to crack the site, sometimes even usernames and passwords. All the comments in source code that look inaccessible to external users should also be removed as there are some techniques to view the source code of nearly all web applications.

O. Beware of Public Wi-Fi

There are simple ways to prevent data loss via public Wi-Fi for mobile devices. Check it's legitimate: It's easy for hackers to set up a fake Wi-Fi network that looks like an official one. Before signing on to any Wi-Fi, the best way to check if the network name is legitimate is by asking an employee of the place.

P. Ensure Physical Security

Apart from ensuring the internal security of the network, users need to think about the physical security of the organization. Until and unless the organization is secured, any intruder can simply walk in the office premises to gain whatever information he wants. Hence with technical security, you must also ensure that the physical security mechanisms of your organization are fully functional and effective.



Seniority of internal fraudsters in financial sector

Conclusions and Further Recommendation

As yet we have discussed present scenario of different kinds threat activities and its preclusion mechanisms. Financial institutions should create a proper IT Governance Body who will be responsible to create and maintain secured IT infrastructure.

The body should design a detail IT policy. The policy has to be documented and should be reviewed and updated on timely basis. The structure should be able to foster answerability and accountability, has effectiveness and transparency with well-defined objectives and action plans and explicit targets for each level in the institute. The body needs to pay attention to adequate and quality trainings and certification courses to its people and vendor personnel for delivering efficient, competent and capable human resources that can ensure effective IT establishment. The body should convince the Board Members to sanction of adequate IT annual budget for implementing the IT policy. The body must adopt international IT Governance standards such as COBIT, ITL, PRINCE 2, ISO, MMI that suit most for that institution. Another important issue is that there should be a procedure to authenticate the information for every new member especially extensive background and credit check is required for sensitive and delicate jobs. The data in the organization should be encrypted so even if the system is under attack; the hackers will not be able to recover meaning. There should be regular basis robust system security testing such penetration testing, Flaw hypothesis methodology technique, ITHC, or IT Health Check for determining any system vulnerability. IT department must consider evaluating the IT maturity level with standard international principles so that organizational IT maturity level can be judged and improved according to the international standard. Magnetic stripe in the smart payment card (i.e. debit/credit card) needs to be replaced modern day EMV (Europay, MasterCard and Visa) card which stores the data on integrated circuits rather than magnetic stripes. There are two key advantages to shifting: enhanced security (with associated fraud reduction), and the possibility for finer control of "offline" credit-card transaction approvals. No new devices or technologies should be introduced without proper scrutiny. It should be thoroughly check for threat and fraud vulnerabilities with the help of proper trained people. There should be specific guideline where to put complain if in case any fraud activity occurs. Cybercrime cells need to stablish in main cities of the country with the help of police department and other law enforces.

In conclusion, latest technologies and international level trend should be introduced in the organization. There is a growing need for thorough research in security of banking technology and bringing out advanced, innovative, safe and secure banking products in association with alleged academic institutes like Bangladesh Institute of Bank Management (BIBM), public universities and institutes. An exclusive forum for CIO and senior IT officials of Bangladesh Bank, BIBM and other financial institutes particularly public and private banks can be encouraged to enable sharing of knowledge, experiences, current trends and discuss issues of present-day relevance for the benefit of the industry as a whole ■