Cyber-crime Scenario in Different Sectors of Bangladesh

Dr. Real Chandra Modak
Advocate
Supreme Court of Bangladesh

ABSTRACT

Cyber and technology related crime is gradually increasing in Bangladesh. It is a significant issue in Bangladesh. It has already been seen that a glomming threat becomes visible in the arena of information technology. Recently the hacking of RAB website, ATM card skimming, Bangladesh Bank heist, Terrorist Activities in social Medias are few examples of them. In addition, Cyber bullying is becoming a major concern for parents on the subject of their children using the internet as majority of students in Bangladesh have experienced being bullied or disturbed online or being bullied by the same person both online or offline. Moreover, cybercrime is becoming a threat to government itself. Due to lack of necessary legislation to tackle such type of crime, cyber criminals are almost in the safe side to commit such crime. In the Information and Communication Technology Act-2006 and ICT (Amendment) Act-2013 there are several clauses against cybercrime. But this Information and Communication Technology act is not the concrete one. By enacting this act, there is a chance to become safe side after committing crimes. So, considering these facts a comprehensive Cybercrime Protection Act should be imposed. This research work incorporates the recent trend and issues of cybercrime in Bangladesh especially focus on the area of Personal life, Workplace as well as Policy making Bodies or Thinkers. I believe that this work would help all relevant concerns and especially policy makers.

INTRODUCTION

Computer crime or cybercrime is a form of crime where the Internet or computers are used as a medium to commit crime. When an online user accesses the Internet, personal information in his or her computer naturally carries valuable information into cyber space that attracts computer criminals. In addition, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyber space. The nature of visibility and accessibility within the cyber-environmental so allows the motivated cyber-offenders to detect crime targets and commit offenses from anywhere in the world. Any criminal activity that uses a computer an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime. Cybercrime may be "unlawful acts wherein the computer is either a tool or target or both".

Bangladesh is now advancing forward having its goal to become digital Bangladesh by vision 2021 with specific goal of using of e-governance in all government agencies.4 Criminals are using this technology to conduct new crimes and to commit traditional crimes in new ways. They can commit these crimes with access to countless victims, with anonymity and from anywhere in the world, making them difficult to detect and pursue. There is no doubt that Cybercrime crime has a global impact as it has had a short but highly eventful history globally.

There is sharp rise in the Cybercrimes in Bangladesh and the Law enforcement machinery is finding it really difficult to manage these technical crimes in Bangladesh. Cybercrime has already become a going concern in both private as well as public sector in Bangladesh. It has already been identified that especially Financial Institutions: private or public are in the most threading organization for cybercrime that at the same time reflects to the personal life.

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.

OBJECTIVES OF THE STUDY

The specific objectives of the study are as follows:

1. To explore the cyber crime issues of Bangladesh;
2. To examine legal protection relating to cybercrime;
3. To discuss the forms of cybercrime;

REVIEW OF LITERATURE

Since Cybercrime is a fast growing subject of discussion and research now-a-days, innumerable books and articles are written on this topic. On the legal relationship some other books, which bear much significance are; The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory by M. Yar, Criminology and Penology by N.V. Paranjape, Invisible Threat of Cyber-Terrorism by Dan Verton, Theoretical and Applied Criminology by Sheikh Hafizur Rahman Karzon, Criminology (Cybercrime) by Monjur Kader and Constitutional Law of Bangladesh by Mahmudul Islam.

Apart from these works, a list of other books, articles, documents, statutes, and journals on different aspects Cybercrime may be found but none of them has dealt with this research topic in the light and details as it has been intended to be done in this work. In none of them could be found an unbiased and in-depth treatment of this burning research area. Attempts will be made in this work to suggest reform where necessary and update the existing laws so that an effective and efficient enforcing mechanism is ensured in a fruitful way.

METHODOLOGY OF THE STUDY

The study was documentary analysis type. Data and information were collected from Books, research reports, journals, Internet etc.

RESULTS AND DISCUSSION

Legal Protection against Cybercrime in Bangladesh

We have several laws to deal with cybercrimes such as The Information and Communication Technology (ICT) Act 2006, the Penal Code 1860, the Pornography Control Act (PCA) 2012 and among them two enactments are important for practical purposes: the ICT Act 2006 and the PCA 2012. Cyber pornography can be prosecuted by section 8 of the PCA and also by section 57 of the ICTA. It will be extremely difficult to prosecute an act of morphing if the morphed image/video does not fall within the meaning of pornography. Acts of cyber stalking will probably continue to be immune from legal process as these laws do not specifically define them and our trial judges will rationally be reluctant to convict a person for acts not defined as crimes. A characteristic of the ICT Act 2006 is that it deals with the both purpose, substantive as well as procedural.

B. Legislation in Bangladesh to Tackle Cybercrime

Inventions, discoveries and new technologies widen scientific horizons but also bring new challenges for the legal world. Information Technology is brought by computers, computer networks, internet and cyberspace. It also brought many new problems in jurisprudence. There was insufficiency of legislation while dealing with the information technology. Throughout the world the judiciary dealing with the new problem like cybercrime, adjudication and investigation of cybercrime, intellectual property Rights issues in cyber world etc. The United Nations Commission on Internet Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996. Model Law provides that all Nation should give consideration to it, when they enact and revise their laws.

The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Hence the most important enactment of the Bangladesh Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 has been done (Sec. 4 of the ICT Act, 2006).

Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to penal laws of a country. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the special laws enacted to penalize these crimes. For example, in Banlgadesh Tatha O Jogajog Projukty Ain 2006 "Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 defines certain offences which does not cover by the Penal Code. And so it can be said that the Penal Code, 1860 is not effective enough in dealing with cybercrimes.

1. Information and Communication Technology Act, 2006: The parliament of Bangladesh has enacted Information and Communication Technology Act, 2006 which defines certain activities as crime. The activities

which made punishable under the Information and Technology Act of 2006 shall be the cybercrimes for the territory of Bangladesh. The following table describes cybercrime and its punishment:

Table 1: Cybercrime and its punishment

Section	Name of Crime	Punishment
54	Mischief of computer and computer system	10 years imprisonment or Tk.10 lacs or both
55	Alteration of source code of commuter	3 years or Tk.3 lacs or both
56	Hacking with computer system	Extend to 3 years or fine extend to Tk. 1 crore or both
57	Publication of false, indecent and defamatory statement or information in electronic form	Extend to 10 years or fine extend to Tk. 1 crore or both
61	Unauthorized access to protected system	Extend to 10 years or fine extend to Tk. 10 lacs or both
62	False representation and hiding information	Extend to 2 years or fine extend to Tk. 2 lacs or both
63	Disclosure of confidentiality and privacy	Extend to 2 years or fine extend to Tk. 2 lacs or both
64	Publishing false digital signature certificate	Extend to 2 years or fine extend to Tk. 2 lacs or both
65	Publishing false digital signature certificate for fraudulent purpose	Extend to 2 years or fine extend to Tk. 2 lacs or both
66	Using computer for committing offence	
67	Offences committed by company	

a) Cyber tribunal: According to section 68 of the Information and Communication Technology Act, 2006 for the speedy and effective disposal of cases under this Act, Government shall establish one or more cyber tribunal. The tribunal shall try only the offences under this Act and the Government shall determine the local jurisdiction of the tribunal. In consultation with the Supreme Court, Government shall appoint on Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal.

Cyber tribunal shall take a case for trial –
a) upon the report of a police officer not below the rank of sub-inspector or
b) upon a complaint made by a controller appointed under this Act or by any other person authorized by the controller.

The trial procedure of cyber tribunal shall follow **chapter 23 of Criminal Procedure Code, 1893 (trial procedure by the Court of Sessions)** so far it is consistent. If the accused is absconded, tribunal can try the case in absentia. In this case tribunal has to circular an order in two bangla newspaper to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall have the same power, a Sessions Court empowered to apply in its original jurisdiction. Public prosecutor shall conduct the case on behalf of the

Tribunal shall conclude the trial within six months from the date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

b) Cyber appellate tribunal: The Government shall establish one or more cyber appellate tribunal. The appellate tribunal shall be constituted by one chairman and two members appointed by the Government. To be appointed as a chairman of Cyber Appellate Tribunal, he must be either a former judge of the Supreme Court or existing judge of the Supreme Court or is eligible to be appointed as a judge of the Supreme Court. One of the two members of the tribunal shall be a retired District Judge or employed in the judicial service and the other member must be an experienced and skilled person in information and communication technology. They shall be appointed for 3-5 years.

Cyber Appellate Tribunal shall have no original jurisdiction. It shall only hear and dispose of appeals from the order and judgment of the Cyber Tribunal and Sessions Court in appropriate cases. The decision of the appellate tribunal shall be final and it shall have the power to alter, amend, and annul the order and judgment of the cyber tribunal. The appellate tribunal shall follow the appellate procedure of High Court Davison of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

B. The Penal Code, 1860
Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to penal laws of Bangladesh. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the special laws enacted to penalize these crimes.

ICT Act 2006 defines certain offences which are not covered by the Penal Code. In this regard, I would like to say that the Penal Code 1860 is not effective enough in dealing with cybercrime in Bangladesh.

C. The Pornography Control Act, 2012
The Parliament has enacted a law by the title of Pornography Control Act, 2012. The preamble says this Act has been enacted to prevent deterioration of moral and ethical values of the society.205 Information technology with its immense benefits has got some disadvantages as well if it is used by mischief people with criminal intention. It has been seen in our country that video clips, MMS etc of sexual intercourse or behaviour relating to sexual activities have been recorded on camera by a section of people and then used to blackmail, cheat, defame girls and women.

The Act has been enacted upon those who produce pornography using a child, man or woman, taking their still pictures, video or film with or without their consent and print, distribute and publish such materials or sell, supply or exhibit child pornography.207 This Act convicts a person if any pornography is being transmitted through the internet, website, mobile phone, or any other electronic device and the punishment is prescribed of imprisonment for up to 5 years and fine up to BDT. 5,00,000.208 Government may constitute Tribunal which is yet to be established for trial of offences under the Act209 and No Rules have been made by the Government as of now.

OVERVIEW OF CYBER-CRIME
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:

1) **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.
2) **Phishing:** It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.
3) **Hacking:** Hacking is a simple term which means illegal intrusion into a computer system without the permission of owner/user
4) **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.
5) **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.
6) **Spamming:** Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
7) **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.

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.

CYBER-CRIME IN BANKING SECTOR-CONCEPTS

According to Jaleshgari (1999), Banking sector throughout the world was simple and reliable tillmid-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 cardholders as well as online sellers. Charge card fraud can be conducted by assuming control over the record, skimming, or if the card is stolen. The expression "Internet fraud" usually refers to any type of fraud scheme consisting of various components of the Internet, like chat rooms, email, forums, or websites - to execute fraudulent transactions or

distribute to other associated with the plan. Banking criminals are utilizing different electronic medium, for example, web, email, and encoded messages for their fraudulent activities.

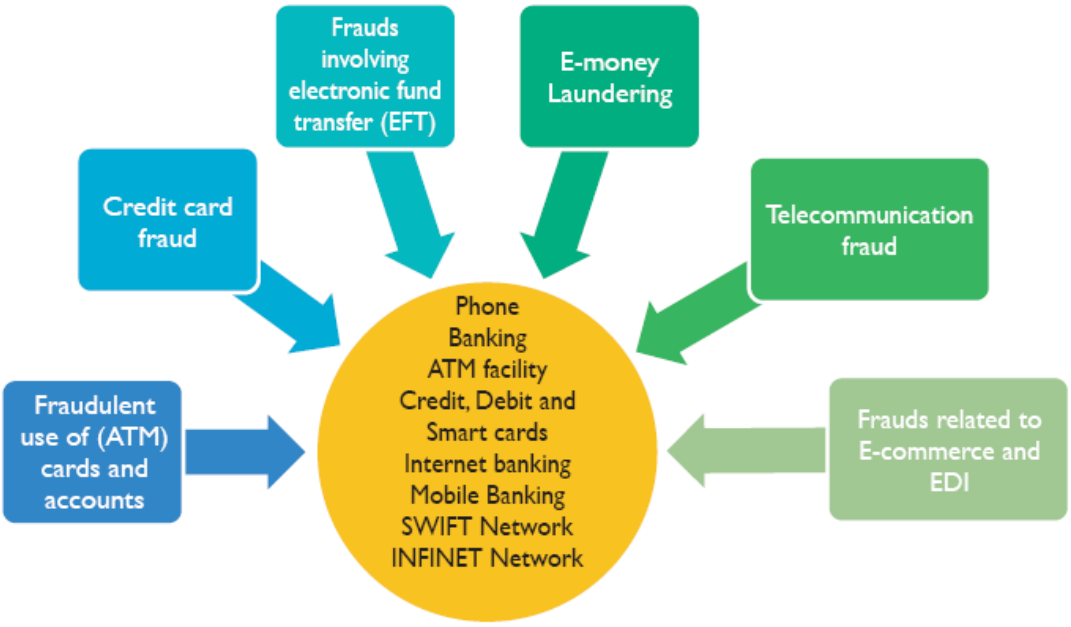

Figure 1: Technology & related crimes

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:

1) Stealing of personal information of almost2.9 million credit card customers of Barclays and Santander Banks UK in 2013
2) Missing $ 450,000 from bank account of a Pennsylvania school district in 2008
3) 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.
4) Over 400 corporate account takeovers in2011, 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.
5) 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)

CYBER-CRIME SCENARIO IN BANKINGSECTOR OF BANGLADESH

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

1) On January 06, 2013, Islami Bank Bangladesh site was hacked by Human Mind Cracker.
2) In 2015, bank accounts of a private bank were hacked and money was withdrawn from them.
3) 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'.
4) In February, 2016, skimming attacks in six ATM booths of three commercial banks.
5) And the largest e-money laundering in the history of banking occurred in February2016, 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.

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.

RECOMMENDATIONS

The findings from this study have led the authors to recommend a holistic approach to deal with cybercrime. The proposed holistic and collaborative approaches comprise of three categories namely: legal, strategic and technical perspectives in predicting, preventing, identifying, and responding against cybercrimes.

A. Legal perspective

i. The Government of Bangladesh should have cybercrime laws for dealing with cybercrime and there should be collaborations of different stakeholders (i.e. within organization, national wide and worldwide).
ii. There should be forensic bureau (competent in IT security) for investigations/ collection of digital cybercrimes evidences.
iii. High penalties should be enforced for cybercrime committed and for those who do not report the incident of cybercrime.
iv. Training and awareness to citizens, organizations, the Government and public in general regarding the collection of digital forensics evidences; and how to report cybercrime.
v. Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

B. Strategic perspective

i. The Government should revise the National ICT policy to accommodate new ICT developments in the industry.
ii. The organizations/Government should have Internet usage and security policies in specific
iii. Standards and procedures should be enacted with regard to usage of information systems in cyberspace.
iv. Use multi-factor authentications (something you know: personal identification number (PIN) or password; something you have: such as Auto Teller Machine (ATM) card or smart card; something you're: biometric characteristic such as a fingerprint) for accessing information systems.
v. Perform Information systems audits.
vi. Perform penetration test (ethical hacking) for information systems (simulating malicious attacks from an organization's internal and external users).
vii. Training and certifications in cyber security, information systems assurance, information systems security and other related risks management certifications or professional. The education system curricula should be reviewed to incorporate training in the field of information systems security and cyber security.
viii. Carry out researches in the field of cyber security, information systems security, and information systems assurance.
ix. Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
x. Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

C. Technical perspective

i. Use of firewalls, IDS, IPS, updated antivirus and anti-spyware.
ii. Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

iii. Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or User Account Control (UAC) password, ensure that the program asking for administration-level access is a legitimate application.
iv. Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
v. Turn off file sharing if not needed. If file sharing is required, use Access Control List and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
vi. Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
vii. If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
viii. Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), mail, and DNS Domain Name System (DNS) services.
ix. Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files. x. Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
x. Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
xi. If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices.
xii. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
xiii. Encryption of data on transit, processing and storage.
xiv. Maintain the disaster recovery room containing all important information management resources.
xv. Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.
xvi. Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

Case studies and the trend of crimes

Case 1: In June 2003, Cyber pirates hacked into the Internet account of Barisal DC office marking the first cybercrime in the Barisal region. The computer hacking incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Telegraph and Telephone Board (BTTB), which is the internet service provider for the DC office. The hackers, who somehow got hold of the password of the account, accessed it from several places in town including an IT firm, residences of an ADC and a joint secretary, and a Pharmaceutical company.

Case 2: An e-mail message was sent to Bengali daily Prothom Alo, issuing a life threat to Awami League president and Leader of Opposition Sheikh Hasina on August 23, 2004. Another mail was sent to the police headquarters Aug 25, threatening Prime Minister Khaleda Zia, her son Tarique Rahman and Bangladesh Nationalist Party (BNP) lawmakers. The police department took the mails seriously and decided to set up a cybercrime control unit, which will be the country's first policing unit against cybercrime. Two young men, a private university student and a software engineer, were arrested in connection with the e-mail threatening the prime minister and another youth for threatening Sheikh Hasina.

Case 3: In 2008 a pretty hacker of Bangladesh named Shahee Mirza hacked the RAB‟s website. Moreover, he confessed to police that not only RAB‟s website but also other national govt., non govt. and international sites had been hacked by him for a long time. Totally he hacked 21 websites together with Army’s website. So it is clear to us that the cyberspace of Bangladesh is not secured58 as there is no nationwide computer infrastructure, no watchdog or security system has yet been developed in Bangladesh.

Case 4: On 15/02/2012 a group of alleged Bangladeshi hackers named „Black Hat Hackers‟ hacked more than 25000 Indian websites which included important sites such as the website of the Border Security Forces (BSF). Propaganda activities are also considered as cyber-crimes in some instances. Propaganda is information which is biased and misleading in nature used to promote or publicize a particular political cause or ideology. It creates agitation and panic among the public.

Case 5: We can mention the 2012 Ramu Violence in Cox‟s Bazar. Someone with a fake Facebook account posted a photo of desecration of the Holy Quran on its wall. The fake account was under a Buddhist male name. This post agitated the common Muslim people of that area and they, without verifying the authenticity of the Facebook account, attacked innocent Buddhist dwellers of that area. Many Buddhist temples, monasteries and households were destroyed.

Case 6: Bangladesh war crimes tribunal chief quits over Skype scandal: The head of a Bangladeshi tribunal which has been dealing with crimes committed during Bangladesh's 1971 war of independence against Pakistan resigned on 10th December 2012 amid controversy over the leak of his Skype conversation with an expatriate Bangladeshi legal expert.59 International Crimes Tribunal-1 chairman Justice Md Nizamul Huq mentioned "personal reasons" for his resignation, then State Minister for Law and Justice Quamrul Islam told The Daily Star 10th December 2012 evening. His resignation would not hamper the proceedings at the tribunal set up in 2010 to try the cases over crimes against humanity, said sources concerned. Although 2006 Information and Communications Technology (ICT) Act covers many of the legal aspects to prosecute cybercrime, but it has not been effectively implemented since its ratification.

Case 7: In Bangladesh, contexts had become worse within a very short period with the killings of the bloggers and journalists even in daylight and shortcoming of the government to bring the murderers before Justice. Till 2013, four journalists named Shahidul Islam, Shahriar Rimon, Abu Raihan, Aftab Ahmed and one blogger named Ahmed Rajib Haider were killed while exercising their right of freedom of expression61 in various social Medias. Besides, the acknowledgements of violent killings of bloggers Niloy Neel, Avijit Roy and Washiqur Rahman in social medias by Ansarullah Bangla team show serious cybercrimes persist in the country.

Case 8: Bangladesh is also facing same type of attack few years ago. During the year 2004 to 2006 JMB killed so many people in Bangladesh. They also used latest technology. The recent killings IS has accepted the responsibility, the authority thinks that these Jihadists belong to the notorious JMB and Ansar-ul-Islam team. Many political observers think that Jamaat and Shibir are the main forces behind it. In this drive how did police arrest so many people overnight? Perhaps they had a big list of suspected criminals. The question naturally arises that why the police did not take this step when these gruesome killings started a long time ago? This new wave of killings started in the month of January last year. Till date 47 people have been brutally murdered.

Case 9: Another 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.

Case 10: 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 has 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 $1 billion to the Federal Reserve Bank of New York. They requested the funds of Bangladesh be transferred to a bank in the Philippines. From there, the cash was transferred to at least three Philipino casinos: At the casinos, someone converted the cash into chips for betting and then reconverted the chips into cash. This money was then sent to bank accounts in Hong Kong. An additional fund of about US$ 21 million was also transferred illegally to a third party in Sri Lanka.

Case Study 11: 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. Itincluded 12 foreign nationals who were individualsfrom 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 askimmer, individual data contained on the magnetic strip is perused and put away on the gadget or transmitted remotely to the criminals.

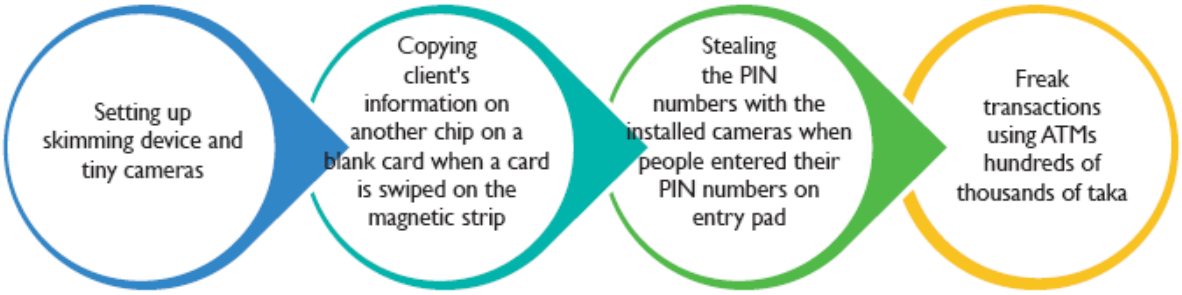

Figure 2: Assumed incidents of Card skimming at Six ATM booth

With the card information, they can lead value based misrepresentation, make new cards with the stolen character and individual data, or offer the card holder 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.

Case Study 12: 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 has 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 $1billion to the Federal Reserve Bank of New York. They requested the funds of Bangladesh be transferred to a bank in the Philippines. From there, the cash was transferred to at least three Philipinocasinos: At the casinos, someone converted the cash into chips for betting and then reconverted the chips into cash. This money was then sent to bank accounts in Hong Kong. An additional fund of about US$ 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 "foundation". 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.

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 sectoris 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 amendments in the Information Technology (ICT) Act to make it more effective to combat cyber-crime.

REFERENCES

Books

1. Karzon, Sheikh Hafizur Rahman, Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, 2008, page-411-418
2. Yar, M., The novelty of "cybercrime": An Assessment in Light of Routine Activity Theory, European Society of Criminology, 2005, page 407-427
3. Edwin H. Sutherland, Principles of Criminology, Second Edition, Philadelphia: Lippincott, 1934, page 3
4. Paranjape, N.V., Criminology and Penology, Central Law Publications, Allahabad, 2009
5. Verton, Dan, Invisible threat of cyber-terrorism, McGraw-Hill Osborne Media; First Edition, August 19, 2003
6. Islam, Mahmudul, Constitutional Law of Bangladesh, Mullick Brothers, Second Edition, 2006

Online Journals

1. Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70
2. Goodman, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3
3. ABA International Guide to Combating Cybercrime, 2002
4. Entertainment Law Review, 2002
5. In Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408
6. Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889
7. Virginia Journal of Law and Technology, Vol. 9, 2004
8. S. J. Ross and R. Masters, "Creating a Culture of Security". ISACA journal, Vo.1.No.1, pp.1-140, 2011.
9. E.H. Dalla, and M. Geeta. "Cyber Crime A Threat to Persons, Property, Government and Societies". International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3. No.5, pp.997-1002, 2013
10. Y. Joshi, and A. Singh. "A Study on Cyber Crime and Security Scenario in India". International Journal of Engineering and Management Research, Vol.3. No.3, pp.13-18, June 2013