Strategies to Reduce Cyber Crime in Bangladesh

Elias Khalil

Abstract

Advancement of technology not only widens scientific horizon but also poses constant challenges for the jurisprudence, legal system and legal world as a whole. Computers, internet and cyberspace together known as an information technology presents challenges for the law. Challenges, which are not confined to any single traditional legal category but in almost all established categories of law such as criminal law, contract, tort, as well as legal concepts of property, expression, identity, movement etc. Existing legal system and framework has shown the inadequacy of law while dealing with information technology itself as well as while dealing with the changes induced by the information technology in the way of our living. The courts throughout the world have been dealing with those problems. Presently, the law providing answers to these problems or dealing with the information technology is termed as 'computer laws' or 'Information technology laws' or 'cyber laws'.

A Term Paper on Strategies to Reduce Cyber Crime in Bangladesh Prepared by: Elias Khalil; Roll No. 103; Special Foundation Training Course for the Officers of Department of Textiles (1st Batch), 07 March – 07 May 2021; Date of Submission: 18 April, 2021; National Academy for Planning and Development Ministry of Planning, 3/A Nilkhet, Dhaka-1205

Table of Contents

1.0 Introduction

Advancement of technology not only widens scientific horizon but also poses constant challenges for the jurisprudence, legal system and legal world as a whole. Computers, internet and cyberspace together known as an information technology presents challenges for the law. Challenges, which are not confined to any single traditional legal category but in almost all established categories of law such as criminal law, contract, tort, as well as legal concepts of property, expression, identity, movement etc. Existing legal system and framework has shown the inadequacy of law while dealing with information technology itself as well as while dealing with the changes induced by the information technology in the way of our living. The courts throughout the world have been dealing with those problems. Presently, the law providing answers to these problems or dealing with the information technology is termed as 'computer laws' or 'Information technology laws' or 'cyber laws' [1].

2.0 Concept of Cyber Crimes

Any illegal activity committed using a computer and/or the internet can be called a cyber crime. Although the term is usually reserved for criminal activity wherein a computer or the internet is the location of the crime, it's also used to include traditional crimes in which computers or the internet are chief tools used in enabling the illegal activity. New technology in general creates new avenues for crime, but not necessarily new types of crime. Criminals could commit fraud, thievery, identity theft, etc. even without the help of tech. These atrocities existed long before the word "cyber" came along.

Thus, cyber crime is basically an extension of existing criminal activity, perhaps making it easier while also adding new dimensions to its execution. Broadly put, cyber crime could be defined as "an illegal act where a computer or a computer network serves as the location, means, target or source of the act". Legally also, this definition of cyber crime was agreed upon by most of the European and North American countries at the Budapest Convention on Cybercrime that entered into force on July 1st, 2004. [2]

Dr. Debarati Haldar and Dr. K. Jaishankar defined cyber crimes as such- "Offences that are committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as internet (chat rooms, emails, notice boards or groups) and mobile phone (SMS/MMS).''

Cyber criminals are most commonly known as hackers. The term “hacker” is now so overused that it has come to be applied to anyone who breaks into computer systems. But this is not entirely correct. There is a difference between hackers and crackers, although the term “cracker” has never caught on with general public [3].

3.0 The Common Types of Cyber Crimes

3.1 Web Attacks

A web attack affects the computer via the internet. These viruses can be downloaded from the internet and end up causing large-scale and irreversible damages to your system.

3.2 SQL Injections

SQL injection is a type of cyber crime that effectively employs malicious codes and manipulates backend databases to access information that is not intended to be displayed. These mostly involve private and sensitive data items including the likes of user lists and customer details, among others. SQLI can have long-term devastating effects such as deletion of tables, unauthorized viewing of any user list, and even administrative access to databases.

3.3 Cross-Site Scripting

Cross-Site is another type of injection breach where attackers send malicious scripts from websites that are deemed responsible or reputed. Attackers inject malicious codes into trusted websites and applications and when a user visits such infected web page, the malicious Java Scipt code is executed on the user’s browser. This code can be used to steal important information like username and password.

3.4 DDoS Attacks

These are the attacks that aim at shutting down services or networks and making them inaccessible to the intended users. These attacks overwhelm the target with a lot of traffic and flood the same with information that can cause the website to crash. DDoS Attacks are targeted primarily at web servers of high-profile organizations such as the government or trade firms.

3.5 Password Attacks

These are simply meant to decrypt or even attempt to obtain a user’s password with the help of criminal intentions. Attackers can use Dictionary Attacks, Password Sniffers, or even Cracking programs in such cases. These attacks are conducted by accessing passwords that are exported or stored in a file.

3.6 Eavesdropping Attacks

Eavesdropping attack begins with the interception of network traffic. This type of cyber crime is also known as Sniffing or Snooping. In this type of cyber crime, individuals attempt to steal information that computers, smartphones, or other devices receive or send.

3.7 Brute-Force and Dictionary Network Attacks

These are networking attacks where attackers attempt to directly log into the user's accounts by checking and trying out different possible passwords until they find the correct ones.

3.8 Insider Threats

Not all of the network attacks are executed by outsiders. The inside attack is a very common type of cyber crime. It is performed on a network or a system by individuals who have authorized access to the same system.

3.9 Man-In-The-Middle Attacks

A man-in-the-middle attack occurs when attackers eavesdrop on the communication between two entities. This type of cyber crime affects both the communicating parties as the attacker can do anything with the interpreted information.

3.10 AI-Powered Attacks

Computer systems are now programmed to learn and teach themselves, and these AI-powered attacks mark a new type of cyber crime that is bound to get more sophisticated with time. AI is employed in many everyday applications with the help of algorithmic processes referred to as Machine Learning. This software is aimed at training computers to perform specific tasks all on their own. They can also accomplish these tasks by teaching themselves about obstacles that can potentially hinder their progress. AI can also hack many systems, including autonomous drones and vehicles, and convert them into potentially dangerous weapons. The AI-powered applications can be used for performing cyber crimes such as Password Cracking, Identity Theft, and automated, efficient and robust attacks.

3.11 Drive-By Attacks

Drive-by attacks are used to spread malware through insecure websites. Hackers first look for websites with lesser security parameters and then plant malicious scripts into PHP or HTTP code onto one of the pages. The script can then directly install the malware onto the computer of anyone who visits the site.

3.12 Phishing Attacks

The Phishing Attack is a Social Engineering attack that is used to steal precious data such as login credentials or credit card details as attackers pretend to be trusted individuals and trick victims into opening malicious links.

3.13 Spear Phishing Attacks

These attacks are aimed at specific organizations' data by individuals who desire unauthorized access. These hacks aren't executed by any random attackers but by individuals who are trying to access specific information like trade secrets, military intelligence, etc.

3.14 Whale Phishing Attacks

A Whale Phishing Attack is a type of Phishing that generally attacks people with high statures, such as CFOs or CEOs. It primarily aims at stealing information as these individuals typically have unlimited access and are involved with sensitive data.

3.15 Malware

Malware is an umbrella term for a code/program that is intentionally built to affect or attack computer systems without the user's consent.

3.16 Ransomware

Ransomware generally blocks victim's access to their own data and deletes the same if a ransom is not paid.

3.17 Trojan Horses

Trojan Horse is a type of malicious software program which attempts to disguise itself to appear useful. It appears like a standard application but causes damage to data files once executed.

3.18 Teardrop Attack

Teardrop attack is a form of attack that causes fragmentation in the general sequence of Internet Protocol (IP) packets and sends these fragmented packets to the victim's machine that is attacked.

3.19 Ping of Death Attack

The Ping of Death Attack is a type of cyber crime where IP packets ping target systems with IP sizes that are much over the maximum byte limit.

3.20 PUPs

PUPs is an abbreviation Potentially Unwanted Programs. These are a form of malware that is less threatening than other types of cyber crimes. This type of attack uninstall the required search engine and pre-downloaded apps in your systems. Therefore, it is a good idea to install antivirus software to prevent malicious download [4].

4.0 Categories of Cyber Crime

Cyber crimes are categorized into three broad categories, individual, property and government. Based on each category of cyber crime, cybercriminals use different levels and types of threats.

4.1 Individual

This cyber crime category includes disseminating malicious or illegal information via the internet and digital-applications by one person. Cyber speaking, pornography distribution, and trafficking are a few examples of this category of cyber crime.

4.2 Property

This cyber crime is similar to a real-life incident where a criminal keeps the bank or credit card information illegally. The hacker steals an individual's bank details to acquire money or makes phishing scams online to obtain information from people.

4.3 Government

It is the least frequent cyber crime, but it is the most serious misconduct. A cyber crime against the government is also regarded as Cyber Terrorism. Government cyber crime involves the hacking of websites, military websites, or the distribution of government propaganda [4].

5.0 Cyber Attack Trend in Bangladesh

Bangladesh is a developing country. In most of the countries like Bangladesh have limitations in information accessing and it is because of having very less knowledge about the existing infrastructure. Cyber crime is a property related crime. Victims are not the priority here, only snatching of properties such as information, data etc. is the purpose of this crime. In our country most of the banks are at high security risk. According to Bangladesh Institute of Bank Management (BIBM), approximately Tk 1,793 crore was invested in the banking IT sector in 2016. Still this banking sector is not cyber crime free at all. A study of Bangladesh Institute of Bank Management (BIBM) says that, a total of 52% of the banks in our country are at high risk of cyber security issues (shown in Figure 1). Out of that 52% banks, 16% banks are at very high risk and 36% banks are high risk [5]. Risks in 32% banks are moderate, 12% banks are at low risk and the remaining 4% of banks are at very low risk region.

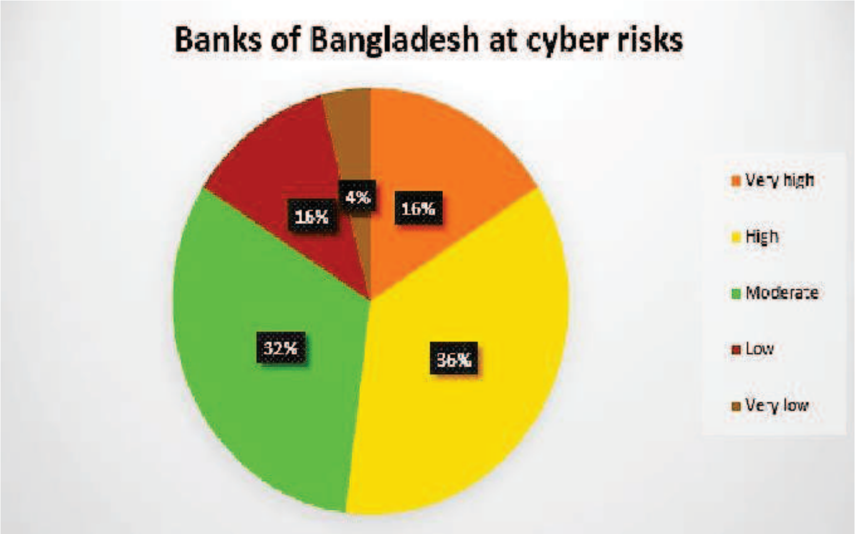


Fig. 1. Banks of Bangladesh at Cyber Risks.

Cyber security in the banking sectors is a burning question in recent times especially after the Bangladesh Bank Heist. The incident Bangladesh Bank Heist held on 4th February 2016, where the hackers (still unknown) tried to steal $1 billion. The hackers managed to get $81 million sent to Rizal Commercial Banking Corporation in the Philippines and PABC bank in the Srilanka via four different transfer requests and an additional $20 million sent to Pan Asia Banking in a single request. The malware's name was evtdiag.exe. The attackers are called Reuters [6]. The hacker did this through a malware which worked on swift messaging system. This malware deletes any incoming message and the confirmation message before sending the office printer [7]. On 4th February, Thursday after working hour, the malware was activated. As Friday was holiday in Bangladesh, there was no one for monitoring the transition message. The attacker gave many request for transition, not all succeeded. They kept trying to transition, after that they were able to transfer money though their fake accounts. After that when on Sunday the bank is opened after weekend, the officials noticed that something wrong had happened because the malware also stopped printer from printing the transition information. The malware also handled the log in and log out process and also controlled the server and modification. Then they said to Philippines bank to stop the transition, but that time in Philippines it was there weekend. The malware was programmed for activation up to 6th February. After identifying the attack, the transition has been stopped, but the attacker succeeded to transfer $81 million. Credit cards, debit cards etc are denoted as "plastic money" are the replacement of conventional financial components paper money in the current living time. The use of ATM is convenient but has a negative phase, which comes out in the form of "ATM frauds". "Internet fraud" is the use of internet services or software with internet access to defraud victims or to otherwise take advantage of them using various components of the internet, like chat rooms, email, forums, or websites - to execute fraudulent transactions. Bank criminals are making utilization of different electronic medium, for example, web, email, and encoded messages for their fraudulent activities [6]. Technology and related crimes are illustrated in following Figure 02.

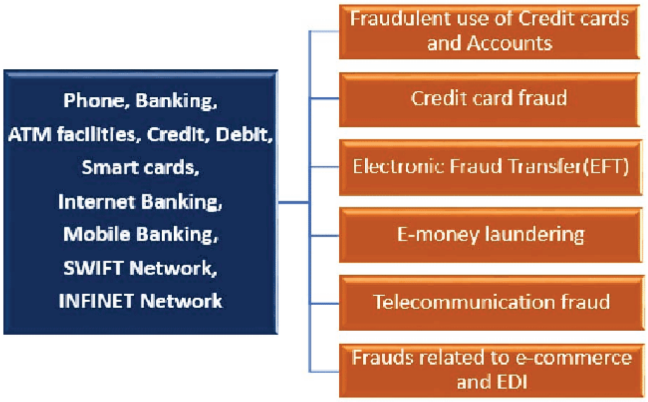
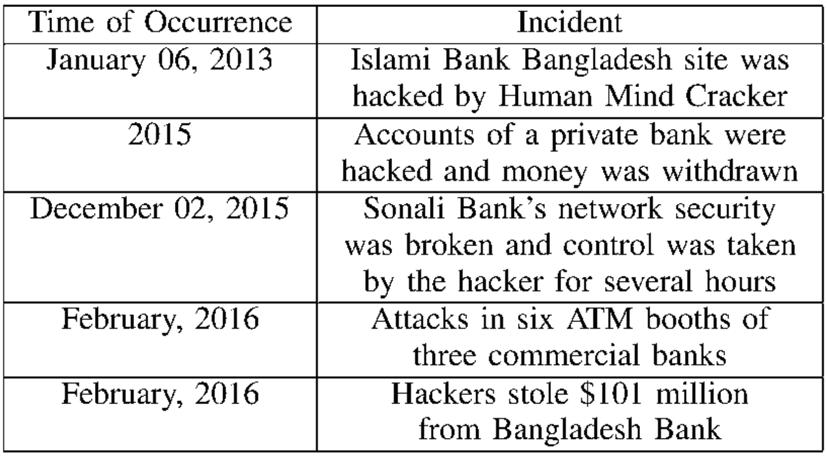


Figure 02: Technology and related crimes

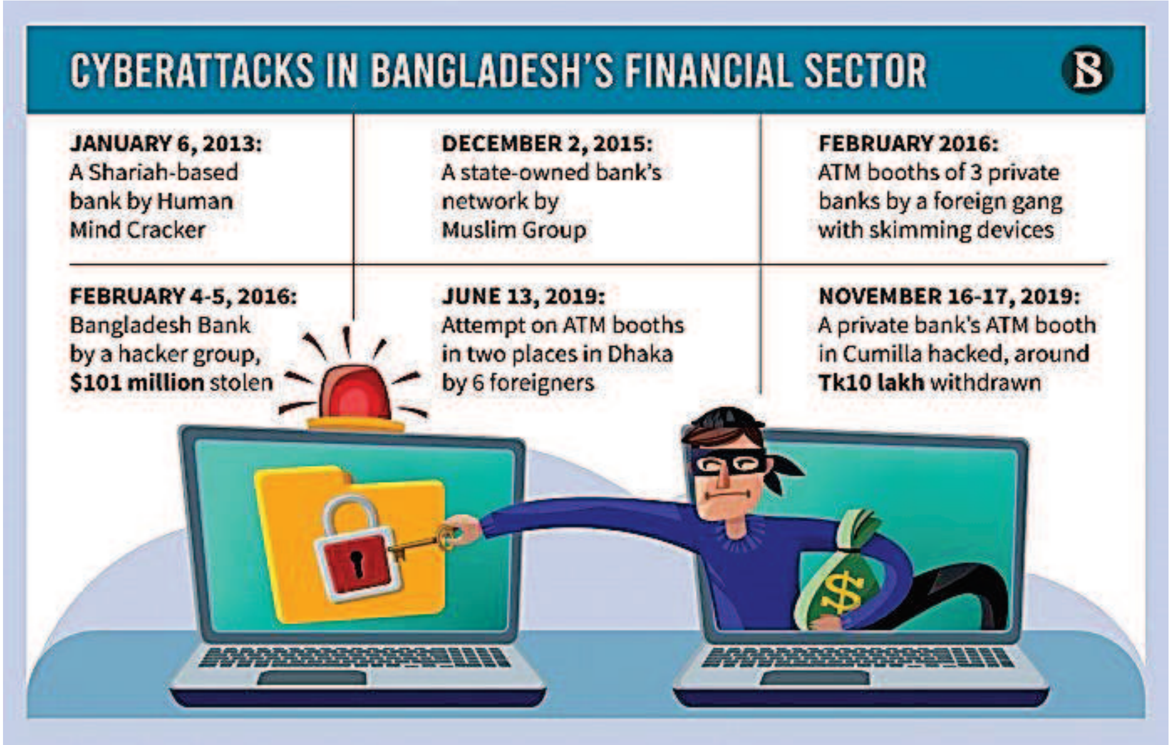
In the last few years, several security breaches had happened in the banking sector of Bangladesh [6], some of those are shown in Table 1.

Table 1: Security Breaches in Bangladesh



Time of Occurrence	Incident
January 06, 2013	Islami Bank Bangladesh site was hacked by Human Mind Cracker
2015	Accounts of a private bank were hacked and money was withdrawn
December 02, 2015	Sonali Bank's network security was broken and control was taken by the hacker for several hours
February, 2016	Attacks in six ATM booths of three commercial banks
February, 2016	Hackers stole $101 million from Bangladesh Bank

Most of the banks in the country have no updates on new strategies to fight cyber hacking and lack the security structure required for online transactions. Cyber attacks in Bangladesh's financial sector are shown in figure 3. [8]



CYBERATTACKS IN BANGLADESH'S FINANCIAL SECTOR

JANUARY 6, 2013: A Shariah-based bank by Human Mind Cracker

DECEMBER 2, 2015: A state-owned bank's network by Muslim Group

FEBRUARY 2016: ATM booths of 3 private banks by a foreign gang with skimming devices

FEBRUARY 4-5, 2016: Bangladesh Bank by a hacker group, **$101 million** stolen

JUNE 13, 2019: Attempt on ATM booths in two places in Dhaka by 6 foreigners

NOVEMBER 16-17, 2019: A private bank's ATM booth in Cumilla hacked, around **Tk10 lakh** withdrawn

Figure 3: Cyber attacks in Bangladesh's financial sector

6.0 Cyber Law in Bangladesh

6.1. The Information and Technology Act, 2006

The Penal code of Bangladesh contains very few provision regarding cyber-squatting. But in case of cyber-crime like Hacking, Internet time thefts, Email bombing- there is nothing contained in our penal code. So it can be said that it is not possible for our government to control cyber-crime by using some provision of the penal code. To controlled cyber-crime it is necessary to enact special law which only deals with cyber related matters. The Government of Bangladesh passed Information Technology Act on 2006. This is the most recent statute enacted by the government of Bangladesh with a view to consolidate Computer related matters and also prosecute computer and computer network related Offence. This statute contains several provisions regarding damage to computer and computer system. Cybercrime dictates that prohibits attacks or unauthorized access to computers and computer systems. According to Section 66 of the ICT Act provides Punishment for tampering with computer source documents. Section 66 says whoever intentionally destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs or with both. Section 67 Hacking with computer system. Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of "hacking". Section 68 of the ICT Act provides punishments for the hackers. Section 68 says that whoever commits hacking shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to taka two lakhs or with both. But the problem of this act is this act deals with so many things. The act is made to cover all the information technology related matters. But it is not possible to cover all the things by implementing just only one act. In order to control cyber-crime we need to have one specific cyber law in our country [1].

6.2 Digital Security Act 2018

Bangladesh enacted the Digital Security Act in September 2018. Passed with the objective of curbing cyber-crime and ensuring digital security, the Digital Security Act creates a wide range of cyber-crime offences. These provide punishment for "propaganda or campaign against the Liberation War, the Father of the Nation", posting offensive content, cyber-terrorism and defamation, amongst others. Significantly, it has extra-territorial application. It also establishes a "Digital Security Agency", empowered to regulate content and request the Bangladesh telecom regulator remove/block the same. Significantly, the Digital Security Act provides safe harbor protection for intermediaries, and penalizes illegal use of "identity information"[9]. Former Cabinet Secretary Mohammad Shafiul Alam said "The aim of the new law is to check cybercrime." A wide range of cyber-crime offences with its punishment are shown below [10]:

- Life imprisonment or Tk 1 crore fine for spreading propaganda against Bangabandhu and Liberation War
- 14 years in prison and a fine of Tk 1 crore for hacking or attacking important websites
- 14 years jail and Tk 1 crore fine for cyber terrorism
- 10 years jail or Tk 10 lakh fine for circulating pomographic materials on the internet
- 5 years jail or Tk 3 lakh fine for committing crimes using digital device O 5 years' jail or Tk 3 lakh fine for cheating or committing forgery digitally
- 2 years jail and Tk 2 lakh fine for defamation and hurting religious sentiment
- 7 years jail and Tk 7 lakh fine for creating enmity and deteriorating law and order
- Crimes committed from outside Bangladesh will be punished under this law
- Digital Security Agency to be formed to regulate broadcasting any information digitally

7.0 Strategic Approach to Reduce Cyber Crime in Bangladesh

7.1 National Cybersecurity Strategy of Bangladesh [11]

Bangladesh needs to build confidence and security in the use of ICTs because of the growing sophistication, frequency and gravity of cyber threats. Cyber threats are a concern because the disruption or destruction of critical information infrastructure could potentially have severe economic, social and national security impacts.

7.1.1 Purpose of Strategy

This Strategy recognizes the impact of cyber threats, risks and challenges to our national values and interests. The Strategy underlines the need for concerted effort to counter these fast evolving threats. This fully integrated approach leverages the resources of the Government, organizations across all sectors, individual private citizens and international partners in mitigating threats to our cyberspace. The Strategy defines the organizational structures required to address this embryonic risk to our prosperity and national security.

7.1.2 Cyber Security Priorities

National Cyber security Strategy should have three national priorities:

Priority 1: Legal Measures

Action 1: Cybercrime Legislation

Action 2: Government Legal Authority

Priority 2: Technical and Procedural Measures

Action 1: National Cybersecurity Framework

Action 2: Secure Government Infrastructure

Action 3: Critical Information Infrastructure Protection

Priority 3: Organizational Structures

Action 1: Government's Cybersecurity Role

Action 2: National Cybersecurity Council

Action 3: National Incident Management Capacity

Action 4: Public-Private Partnerships

Action 5: Cyber security Skills and Training

Action 6: National Culture of Cybersecurity

7.2 Investments in Cyber Security Aspects

Observing the cyber-crime trend in Bangladesh it is needless to mention that both private and public sector need to invest substantial amount of their budget for enhancing cyber security measures. Bangladesh government has invested 40 crore BDT to build up cyber security branch in the ICT division [6]. At the same time private sectors are need to be encouraged to invest in cyber security aspects of their business.

7.3 Legal Framework

Our government has passed various legal acts to fight back the cyber-attack and also stop digital harassment. We have ICT acts 2006, 2009, 2013(amendment), Digital Security Act 2018. All these acts combine the cyber security in our country.

7.4 Seminar and Training

The government arranges various seminars, workshops at college, university and institution level to make people aware about the cyber crime issues. These seminars or workshops enlighten people about cyber-crime happening around the world and also in our country and how to fight back them. In supervision of bdCERT many training programs are held [6]

7.5 CERT Group Formation

CERT means Computer Emergency Response Team. This team's responsibility is to deal any instant devastating situation arisen due to cyber attack. Bangladesh government has given us a 24*7 hours CERT assistance named bdCERT [6]. Each organization and institution need to form their individual CERT.

7.6 Cyber Security Strategy

Each and every organizations must have a strategy to combat cyber crime and take immediate decisions when needed. This strategy should be made as per the National Cyber Security Strategy [6].

7.7 Code of Ethics

Each organizations should have a culture of complying with code of ethics (ACM code) by their employees [6]. ICT education in universities and institutions need to include courses on engineering code of ethics in their curriculum. Bangladesh government has already made ICT education compulsory in its secondary and higher secondary level. In this curriculum code of computer ethics (ACM) may be incorporated.

7.8 Awareness of Cyber Crime

Educational institutions may include curriculum comprise with moral and social ethics and users' code of conduct for the future IT fellows not to use the technology in a morally reprehensible manner. Law enforcement authority must monitor cafes' and users' activities imposing restriction on some websites and users (under18) requiring bar code/password for use and make the users aware of the possible consequences of using certain sites. A "citizen" should always rethink whether his activities render him vulnerable and keep in mind the following things:

- To prevent ID theft one should avoid disclosing personal information (DoB, bank details) on any web site to strangers.
- Avoid sending any photograph online and providing email address to unknown person or chat friends as there may be misused of it.
- Unexpected financial gain offered by any person without any consideration should be avoided unless the person is close relative, one may be asked to provide some intrinsic information (address, DoB, bank details), transaction/service charges.
- Always uses latest and update antivirus software to guard against virus attacks and keep back up volumes so that one may not suffer data loss in case of virus attack.
- Parents should keep an eye on children that are accessing internet to protect them any abusive or immoral illusion and imminent danger. Finally, it may be submitted that the collective effort of state and nations is only a possible way to see the peoples' dream of a Digital Bangladesh in existence and could protect individuals and national security of the state from the aggression of cyber criminals.

8.0 Conclusion

To fight cyber-crime we must not impose all liabilities to the government. Computer and internet system facilitated the non-government organizations a lot. They have the largest interest in cyber security. At several of US national institute of Justice revealed that the business and financial institutions comprises 46 percent of computer crime targets while the government comprise only 8 percent of the targets. So, non-government organizations must come forward to augmenting the governmental initiatives with money. Logistics and specialized manpower. The Mumbai cyber lab is a unique initiative of police public collaboration for training police officers in the investigation of cybercrime. Similar initiates have also been taken by other states of India. Bangladesh should follow their suit. The government should welcome outsourcing initiatives to prepare a galaxy of virtual police officers and establish few cyber police stations across the country as soon as possible. Those cyber-crime fighters should be given specialized training home and abroad. The non-government organizations utilizing computers and internet system, as their means of business operation should sponsor to send the virtual police officers abroad for advanced training on cybercrime prevention and investigation.

References

1. Sheikh, A. (2019), Prevention of Cyber Crime in Bangladesh. International Journal For Empirical Education and Research, 3(21), 33-47

2. https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/what-is-cyber-crime.html
3. www.bdlawdigest.org/cyber-crimes-and-cyber-laws-in-bangladesh.html
4. https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/#Whale-Phishing-Attacks
5. http://www.dhakatribune.com/business/banks/2017/05/05/banks-high-cyber-risks
6. S. Kundu, K. A. Islam, T. T. Jui, S. Rafi, M. A. Hossain and I. H. Chowdhury, "Cyber crime trend in Bangladesh, an analysis and ways out to combat the threat," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea (South), 2018, pp. 474-480, doi: 10.23919/ICACT.2018.8323800.
7. https://www.csoonline.com/article/3060727/bangladesh-bank-attackers-used-custom-malware-that-hijacked-swift-software.html
8. https://www.tbsnews.net/economy/banking/banks-need-enhance-cyber-security-138367
9. Bangladesh Digital Security Act, 2018, available at https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf.
10. https://www.thedailystar.net/frontpage/new-law-curb-cybercrime-1274128
11. https://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf