Cyber Security A Challenge for Bangladesh

Bangladesh University of Engineering & Technology

Course No: HUM172

Course Name: Developing English Skills Sessional

A report on

Cyber Security: A Challenge for Bangladesh

Prepared For:

Dr. Mizanur Rahman
Assistant Professor (English)
Department of Humanities
Bangladesh University of Engineering and Technology, Dhaka-1000

Dr. Sharmin Chowdhury
Assistant Professor (English)
Department of Humanities
Bangladesh University of Engineering and Technology, Dhaka-1000

Prepared By:

1705066 - Ataf Fazledin Ahamed
1705067 - Nishat Farhana Purbasha
1705068 - Saadman Ahmed
1705069 - Tanzim Hossain Romel
1705070 - Al Arafat Tanin
1705071 - Prantik Paul

Forwarding Letter

6th January, 2019
Dr. Mizanur Rahman
Assistant Professor (English)
Dr. Sharmin Chowdhury
Assistant Professor (English)
Department of Humanities
Bangladesh University of Engineering and Technology, Dhaka-1000.

Subject: Letter of submission of a report on “Cyber Security: A Challenge for Bangladesh”

Dear Sir and Madam,

With due respect, we would like to express our gratitude for encouraging us to prepare a report on “Cyber Security: A Challenge for Bangladesh”. It is one of the most talked topics in Bangladesh recently. It has been a great privilege to make a report on the above mentioned topic.

The report is based on the recent events about cyber security. Nowadays maintaining cyber security is an alarming issue all over the world and Bangladesh is facing many challenges regarding this. Data has been collected about recent events and we have tried to point out some problems regarding cyber security in various sectors like banking sector, educational sector, social media, business sector etc. Data has been gathered by analyzing articles, newspapers, books, websites etc. After working on these, we have been able to find out some solutions to overcome problems associated with cyber security and we are hoping these solutions will be effective.

We apologize for any undesirable mistakes and thankful to our course teachers for providing us proper guideline while making this report. We are grateful to articles, newspapers, books for enlightening us with so much information. We hope that our respected teacher would consider our report in spite of unwanted mistakes.

With regards,
1705066 - Ataf Fazledin Ahamed
1705067 - Nishat Farhana Purbasha
1705068 - Saadman Ahmed
1705069 - Tanzim Hossain Romel
1705070 - Al Arafat Tanin
1705071 - Prantik Paul
Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology, Dhaka-1000

Table of Contents

Forwarding Letter ii

Table of Contents iii

List of Illustrations iv

Summary 1

1. Introduction 2

1.1 Definition 2

1.2 Cyber Security in the Globalized world 2

2. Cyberspace and its present condition 4

2.1 Penetrating Private Data 4

2.2 Recent Breaches in Websites 5

3. Cyber Security & Financial sector 6

3.1 Overview 6

3.2 Recent Cyber Attacks in Financial Sector 6

3.3 Investigation & statistics 7

3.4 Challenges in the banking sectors 8

3.5 Steps to ensure security in banking-sector 9

4. Cyber security issue from government's perspective 9

4.1 The current scenario of cyber security 10

5. Cyber law and issues in Bangladesh 11

5.1 Cyber Law in Bangladesh 12

5.2 Punishment for Penalty in ICT Act 2006 13

6. Conclusion 14

Recommendations 16

List of References 18

Glossary 19

List of Illustrations

Figure 1: A summary of internet users and mobile users 3

Figure 2: Total no of mobile subscriptions in Bangladesh 11

Figure 3: Bangladesh ranks 83 in Global Cyber Security Index 2018 15

Summary

Internet has become a powerful weapon all over the world and it has spread out significantly in Bangladesh. Recently about 81.66 million people use internet in Bangladesh and close to 30 million people use many types of social media. As the users are increasing day by day, the threat in cyber security is enlarging also. Bangladesh Government has established internet based activities in almost every sector of the country. But because of the lack of proper maintenance we have seen threats associated with cyber security in these sectors. In social media sector, many people's personal information has been compromised because of the attacks of hackers. Even banking sector has faced more cyber-attacks than any other sectors and this problem is rising. About USD 101 million was stolen from Bangladesh Central Bank account at the New York Federal Reserve by hackers, and whole money was transferred to Philippines and to a third party of Sri Lanka. Moreover, a recent research reveals that 52% of the banks are at high risk of cyber-attack. Besides public and private organizations are providing digital facilities without ensuring safety. Even people are using applications without knowing the fact that they are permitting these apps to access their personal information, credit card number, bank account number etc. And when these apps are attacked by the hackers, their information is compromised. To ensure cyber security and safety the government of Bangladesh has taken some steps. The very first cyber law of Bangladesh-The Information and Communication Technology Act (ICT) was introduced and enacted in 2006. But this law is not sufficient for ensuring safety in cyber space. The authorities should prepare their individuals with skills to overcome hacking, cyber-breach etc. and to maintain cyber-security, encryption properly. Overall, the government and the IT companies have to work together to maintain cyber-security to secure this country's future from any kind of cyber-crime.

1. Introduction

1.1 Definition

The term cyber security can be referred to as the security and safe utilization of the cyberspace. According to Singer and Friedman, “Cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared and communicated outline.” In other words, cyber security deals with the protection of data, networks, computers, programs etc. from unauthorized attacks and access from intruders. It is mainly a technology that protects computer, data and information from being stolen, attacked or manipulated by unauthorized access caused by cyber criminals, hackers, malicious code or virus.

There are some major areas covered in cyber security from basic point of view -

- Application Security
- Information Security
- Disaster recovery
- Network Security

Application security covers the security of apps at the time of design, development, upgrade or maintenance. It helps the apps from any kind of threat in its process.

Information security protects data from unauthorized access and offers privacy for data. Some techniques like Identification, Cryptography etc. are used for maintaining privacy.

Disaster recovery planning includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. It helps any company to act accordingly when any disaster occurs.

Network security introduces various activities like protecting usability, reliability, integrity and safety of any network. Proper and effective security measures ensure the safety of the network. Some network security tools are Firewall, antivirus, IPS, VPNs etc. and these tools help to block unauthorized access to distinguish fast-spreading threats and to provide secure remote access.

1.2 Cyber Security in the Globalized world

In the era of modern technology, people around the world are connected with each other through internet which makes them a citizen of the global village. With the revolution of such technology, cyber vulnerability and crimes have been increasing proportionately. It has become a national security issue in technological advanced countries. Cybercrimes usually occur in four ways as described below:

First, occurrences for commercial purposes. In April 2013, U.S. stock market encountered a fall of amount of $130 billion within minutes due to a hacked tweeter post that generated a false news of White House explosion.

Second, security breaches by the hackers for intellectual purposes. In this case, classified information of intellectual property is the target of the criminals.

Third, posing threats to individuals from terrorist websites for creating chaos in international area.

Fourth, state boosted cyber-attack on another state's national security websites to lessen their strength for gaining political or economic advantage over that particular state.

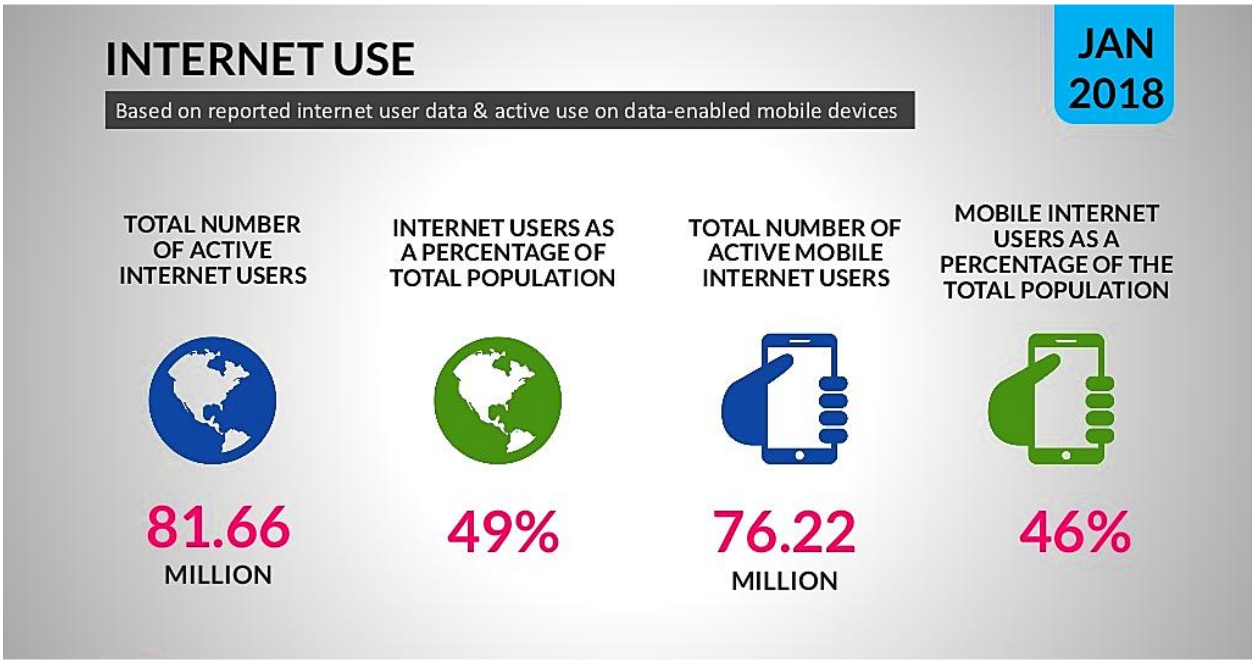

INTERNET USE
Based on reported internet user data & active use on data-enabled mobile devices
JAN 2018
TOTAL NUMBER OF ACTIVE INTERNET USERS
81.66 MILLION
INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION
49%
TOTAL NUMBER OF ACTIVE MOBILE INTERNET USERS
76.22 MILLION
MOBILE INTERNET USERS AS A PERCENTAGE OF THE TOTAL POPULATION
46%

Figure 1: A summary of internet users and mobile users

Source: https://jmustafa.com/digital-in-bangladesh-2018-report/

2. Cyberspace and its present condition

In this digital era, the main component for advancement is connection and correspondence. Now-a-days, social media has become synonymous for contact, whether it be between acquaintances or business associates. Because of user-friendliness and inherent capabilities, every social media, let it be casual ones like Facebook, Messenger, Instagram or the ones that have more of a professional attitude like Google+ or LinkedIn, have gained edge over diversity, wisdom and the overall understanding of the concept of globalization. However, every social media requires personal data and information of the user to function properly. Though these data and related personal and monetary information are confidential and promised to be used under certain protocol, constraint, model, mechanism and algorithm, the leakage of these information has raised a serious threat towards cyber safety which needs to be addressed immediately.

Bangladesh is no longer a third nation country, rather it is galloping towards development and already has achieved the status of being a middle-income country. The Bangladeshi citizens are now quite familiar with the concept of internet and its usage. There are close to 81.66 million internet users in this country among whom about 30 million people use various social media actively. 28 million of these users access these sites or application through their cell phones. The total number of mobile internet users in Bangladesh today are approximately 76.22 million. 48% of the users in social media are actively using Facebook which has proved to be the most popular platform for inter-connection between themselves. Moreover, 93% of the total users are on Twitter, 66% of the users are on Pinterest, 17% of the users are on Google+ and 13%of the users are on LinkedIn. . 80 million users remain active on monthly basis on Instagram also.

2.1 Penetrating Private Data

Like any other medium of cyber-attack, security in social media can be breached in many ways such as,

- Cyber-crime against individuals
- Cyber-crime against property
- Cyber-crime against organization

Social media sites contain sensitive information of their users in their server. These information include:

- Contact information
- Email-address
- Credit card information

Often during installation, the social-media sites or applications on cell-phone require permission to access personal contacts, overwriting data on other applications and so on. We often provide these permissions without foreseeing the results of leakage. As a result, these confidential data get exposed for exploitation in the following scenarios:

- Hacking or cracking the websites or servers
- Crash-down of servers
- Illegal/Unauthorized access
- Illegal interception of data in servers
- E-mail spoofing

The result of this type of leakage is quite severe and can lead to some serious mishaps like:

- Data interference
- Cheating and fraud
- Identity theft
- Indecent exposure
- Harassments and cyber stalking
- Computer and network resource vandalism
- Forgery
- Indecent exposure
- Defamation
- Internet time and information thefts
- Dissemination of obscene materials
- Virus attack
- E-mail bombing
- Blocking access to resources
- Dissemination of propagandas
- Conning the contacts of money

2.2 Recent Breaches in Websites

- In the recent years, there have been a lot of breaches in Govt. Educational Websites. The last one dates back to April 5, 2018. It was the Dhaka education board website which was hacked.
- In April 10, 2018, there was also an attack on government websites where the ministry of education’s website was also breached. After some days, in the same month of April, the website was attacked once again.
- Recently a government organization in Bangladesh was barraged with 4,600 attacks in a single day.
- The payment transaction system of Bangladesh Bank was also breached which led to the theft of 101 million US Dollar.

- ICT Division’s websites faced damage due to cyber-attacks led by Indian hackers recently.

3. Cyber Security & Financial sector

Nowadays cyber security is an alarming issue for all over the world and cyber-attacks in financial institutions is rising rapidly because of hackers can successfully break down the security system due to low stability of the security system of banks and global cyber security practice leaders are recently brought together for a discussion about the matter of “Cyber Security in Financial Sector” all over the world.

3.1 Overview

With increasing cyber threats banks are facing so much challenges from being the victims of data theft by hackers and for maintaining the security of their complex system. Now the noticeable trends in banking industry are given below:

1. Banking sectors face almost 3 times of cyber-attack more than other industries and their cost from being data theft victims is rising exponentially with globalization.

2. It is estimated that the cost of maintaining cyber security infrastructure will increase over 40% by 2025.

3. As a security purpose banks have been recognized that biometrics can be the solution of payments control and sensitive data theft.

3.2 Recent Cyber Attacks in Financial Sector

Financial industries are considered most developed industry in the era of globalization. It is not only for that, globalization allowed us to connect across greater distance but is also for our ability to make our system more complex and also for our expanded database system and processing power. But for making our system more complex, vulnerability of our security system increases with order of exponential complexity.

This is why our main focus is on the security system of financial sectors and it is widely practiced after claiming than about USD 101 million was stolen from Bangladesh Central Bank account at the New York Federal Reserve by hackers, and whole money was transferred to Philippines and to a third party of Sri Lanka.

After that the story gradually surfaced. Subsequently, the Bangladeshi media revealed that the false transfer orders to Philippines included fraudulent payment orders of US$ 25 million for the Kanchpur, Meghna and Gumti 2nd Bridge Construction Project, US$ 30 million for the Dhaka Mass Rapid Transport Development Project, US$ 6 million for the IPFF project cell and US$ 19 million for the Bheramara Combined Cycle Power Plant Development Project. A ranking official of Pagcor, which is in charge of regulating gaming activities in Philippines has said that the funds were split into a $26-million tranche that was channeled into the account of Solaire Resort and Casino and a $20-million tranche that was directed to the accounts of Easter Hawaii Casino and Resort at the Cagayan Economic Zone Authority in Santa Ana, Cagayan province. The two tranches, totaling $46 million represented 56 percent of the stolen money that entered the Philippine financial system between Feb. 5 and Feb 9, 2016.

3.3 Investigation & statistics

An investigation comes with more concerning matter that hackers were able to exploit weakness in the "supposedly secure global money transfer system known as SWIFT", which banks use for major money transfers between themselves, according to Al Jazeera. But the specifics of what weaknesses were exploited in the SWIFT system are yet to be made clear.

During this attack, hackers had used very simple malware to target Bangladesh Bank computer system to control money transfer to their target account but giving the conformations that the transfer was as normal as other transfer and having control on secondary controls system.

After the attacks in BB's account at New York, Bangladesh Institute of Bank Management (BIBM) conducted many researches on the cyber security of banks in Bangladesh, with one of its research revealing that 52% of the banks are at a high risk of cyber-attack.

Another BIBM research found that 80% of banks in the country do not have relevant staff skilled and efficient enough to face any such attack, or even as much as a firewall in their data center. Only 4% of banks have employees with excellent knowledge about IT and cyber security systems, found another BIBM study which also revealed that half the banks officials in Bangladesh are unaware of cyber security.

The research found that 28% of the officials in the banking industry are "very ignorant" about cyber security and 22% are "ignorant" about IT security, while 20% of officials have a minor knowledge about the matter.

From another study of Daily Sun, it was found that, one of the main reasons behind the vulnerability is that the country has been suffering seriously from the skilled ICT manpower. And this is worrying to note that, as per academicians, more than two hundred thousand fresh ICT graduates enter job market a year, but most universities do not bother matching their curricula with those of other universities on the globe and improving it to help overcome the cyber security challenges.

Another study of Bangladesh Institute of Bank Management found that Sixty-two per cent of the country's scheduled banks are vulnerable to cyber-attack while 28 per cent of the banks have no preparation for tackling such attack.

Fifty-seven scheduled banks are operating in the country.

The study report was presented at a seminar on 'IT Security of Banks in Bangladesh: Threats and Preparedness' organized by BIBM at its auditorium in Dhaka on Sunday.

The report also showed that another 34 per cent of the banks lacked preparation for tackling cyber-attack as they had taken partial measures in this regard.

Only 38 per cent of the scheduled banks have preparation for tackling any cyber-attack, it stated.

The study that analyzed 50 fraudulent activities in the banking sector found that 43 per cent of the incidents took place by means of automated teller machines.

Another study of the Bangladesh Institute of Bank Management (BIBM) reveals that the country's 38 percent banks are ready to tackle any king of cyber-attack while 34 percent do not have full-pledged preparations and 28 percent do not have preparations at all to resist big cyber-attacks.

3.4 Challenges in the banking sectors

As cyber-attacks are rising more rapidly in banking system so now the main challenges for the banking industry are given below:

1. Secure Transferring Data and Customers Data:

After attacks, different banks of North Korea, India, Bangladesh, Taiwan it was a great challenge for the banking sector to secure their data from third party attacks. It was mostly found that, in different attacks the hackers had stolen data from the bank server and tracked their activities of transferring money, storing customers' information, their security and so on.

After the investigation by Bangladesh Bank, it was found that, a malware was pushed within the banking system in 2016 and was sitting there for a month gathering the information on the bank's operational procedure for international payments and fund transfer so that they can perform a perfect attack. And it was so common in case of other bank attacks.

And so, according to the report of The Daily Star, "Bangladesh Bank has taken a major remediation plan involving around Tk. 200 crore to strengthen its security system."

2. Evolving cyber threat landscape:

The development in technologies is leading to the latest cyber threats like next generation ransom-wares, web attacks, Social Engineering and Phishing, Man in the Middle etc.

3. Third party risk:

Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank.

4. Transaction frauds:

Fraud detection technologies should be in place with proper consideration of risks based on the business factors.

5. Secure SDLC:

Banks need to incorporate SDLC security for banking products and applications.

3.5 Steps to ensure security in banking-sector

To ensure security in banking industries, some steps can be taken. Some of the key steps can be:

- Cyber Security Policy has to be distinct from the broader IT policy/ IS Security Policy of a bank
- Arrangement for continuous surveillance
- Comprehensive network and database security
- Protection of customer information
- Cyber security preparedness indicators
- Cyber Crisis Management Plan
- IT architecture should be conducive to security
- An immediate assessment of gaps in preparedness to be reported to Bangladesh Bank
- Creating cyber security awareness among stakeholders/management Board

4. Cyber security issue from government's perspective

The rapid spread of information and communication technology worldwide has led cyber security to be one of most important parameters to determine the success of a government in this modern era. Even the most technologically advanced countries like United States fall victim to cyber-crime, being not able to meet cyber security demands of 21st century. A much less developed country, Bangladesh, falls under the risk of cyber-crimes that threatens the national security of the country. As a part of agenda to transform Bangladesh to 'Digital Bangladesh', the government has worked consistently to digitalize the whole country by introducing modern technologies, which has been a remarkable success so far. However, this has given rise to few new challenges, cyber security being one of them.

Secure cyberspace is a key element of protecting national security, which plays a significant role in achieving economic prosperity and credible defense of a country. These are important to build a strong, modern, powerful and industrial nation. With the rapid advancement of technology, and people's growing dependency on technology, cyber-crime has globally become a considerable security concern. The current state of cyber security in Bangladesh is nowhere near it needs to be. Consequently, this has given birth to cyber-crimes which abysmally impact the growth of the nation and create diplomatic conflict in world order. In the words of Estonian President, T.H. Ilves, "In a modern digitalized world, it is possible to paralyze a country without attacking its defense forces. The country can be ruined by simply bringing its Supervisory Control and Data Acquisition (SCADA) systems to a halt. To impoverish a country one can erase its banking records. The most sophisticated military technology can be rendered irrelevant. In cyberspace, no country is an island. One of the best examples of how cyber-attacks can paralyze a country is that "In May 2007, during a dispute between Estonia and Russia, hackers launched massive attacks on Estonian government agencies including parliament, ministries, banks, television stations, newspapers and other organization, using networks of computers to shut down Estonian systems online." Therefore, cyber-attack can be the biggest threat to the security and survival of modern states. And hence, Bendrath (2001) argues that "Tomorrow's terrorists may be able to do more with a keyboard than with a bomb."

Public and private organizations are providing digital facilities to people without giving emphasis on ensuring cyber security. As a result, a large portion of country's cyberspace is left vulnerable to any kinds of cyber-crime. Also, the existing Information and Telecommunication Act of the country remains ineffective to secure the cyberspace. There is no denying that most people affiliated with ICT ministry also lack resources as well as awareness that is required to ensure proper cyber security. The country has already faced severe consequences for such inadequacy and is inevitably on verge of facing more severe disasters.

4.1 The current scenario of cyber security

Bangladesh is an active participant in the technological revolution that has changed the lives of humankind. Bangladesh intends to use ICT sector as boosting element for socio-economic development. The Awami League-led government has already introduced people with digitalization in educational institutes, law-enforcement agencies, service sectors, etc. Private sectors, inspired by the government, has also brought online services to consumers, facilitating online shopping, e-commerce, e-banking, mobile banking etc. While this has positively changed people's lives, this has brought many adverse effects too. Most of the effects relate to cyber security.

No country is in isolation in cyber space, then Bangladesh is not out of possible cyber-attacks. The recent cases strongly support this argument that Bangladesh is also vulnerable to this threat. According to media reports, the official website of the Ministry of Foreign Affairs, Bangladesh, was hacked two times, on December 9 and 12, 2012. Furthermore, on September 5, 2008, the official website of RAB was reportedly hacked. Very recently, the websites of two newspapers also came under cyber-attack. Several government websites including those of the prime minister's office and the home ministry have been hacked on April 4, 2018. The Bangla version of the Bangladesh Election Commission was hacked around January 13, 2018. The website of Bangladesh Association of Software and Information Services or BASIS has reportedly come under a cyber-attack by a group of Myanmar hackers on May 26, 2018.These incidents clearly shows that how poorly secured Bangladeshi websites are. Bangladesh should, therefore, give proper attention to cyber security, since it is an issue that can impact us at the personal level as users of the Internet, and at the national level it has the potential to become a persistent threat.

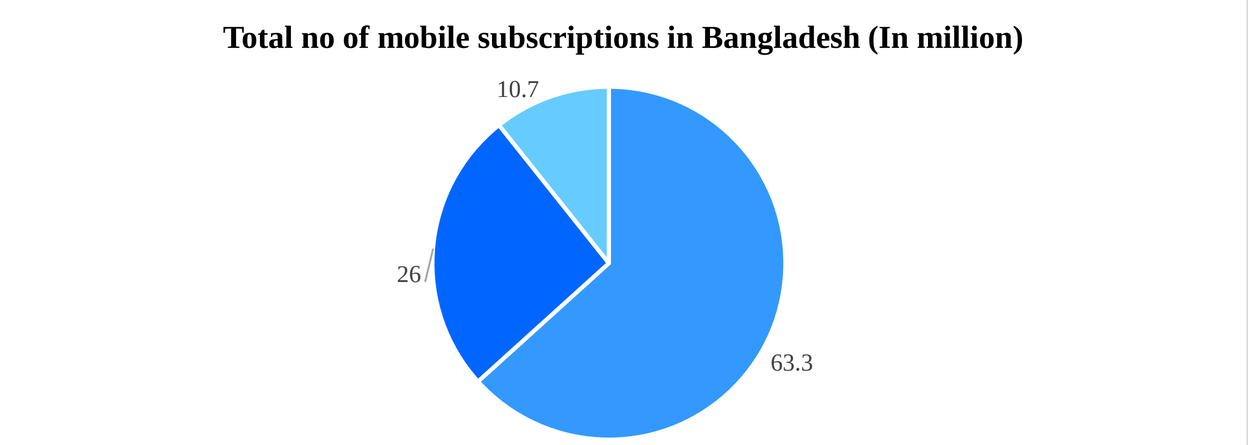


Figure 2 : Total no of mobile subscriptions in Bangladesh

5. Cyber law and issues in Bangladesh

Considering the present trend, it has become almost obligatory for everyone to understand the jurisprudence that countries worldwide have framed to regulate and control the use of computers. (Zulfiquar Ahmed, A Text Book on Cyber Law in Bangladesh, 1st ed., (Dhaka: National Law Book Company, 2009), page 39 – 52.) For the past few years, many countries have been concentrating on the awareness on questions of about the governance of cyberspace. From the moment internet was made public, different groups all over the world wanted to dominate, such as user, communication companies, ISPs, and the government. So, government intervention was necessary to sustain control over the internet to ensure its proper usage and safety. As internet has grown in our country, the need for appropriate cyber laws have become more and more evident.

The government of Bangladesh came up with the first cyber law of Bangladesh – The Information and Communication Technology Act (ICT), in 2006. The Cabinet of Minister of Bangladesh has approved the Information and Communication Technology bill (ICT), 2006 on February 2005 and it has been enacted on 8th October, 2006. The ICT Act defines various terms, which are innovative in the legal lexicon in Bangladesh. The law consists of a preamble, 97 sections and four schedules. Cyber Laws are contained in the ICT Act, 2006. This Act aims to provide the legal infrastructure for e-commerce in Bangladesh and the cyber laws have a major impact for e-businesses and the new economy in Bangladesh.

The Cyber Law in our country is not sufficient to ensure a safe cyber space. In fact, there has been a lot of criticism of the Cyber Law of Bangladesh. The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time? For example, it was not possible to track down the Emil Indian Hacker who hacked 17 of district web portals back in 2010. The Act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse of the law. Also, power have been given to police officer not below the rank of an Inspector of Police (IP), or any other officer of the Government authorized by the Government in this behalf for purpose of investigating and preventing the commission of a cyber-crime under section of the ICT Act, 2006. The unrestricted power given by the ICT Act is highly likely to be cause misuse and abuse of power by police officers. Also, The ICT Act does not provide extra-territorial jurisdiction or multi-territorial jurisdiction to law enforcement agencies, but such powers are basically ineffective.

There are plenty of laws on the books, however, enforcing them is very difficult. Often it is the case that perpetrators are never brought to justice, which is indeed very frustrating for the victims. Also, the local police departments often shy away from investigation of the crime. Surely, enforcing laws governing online behavior is intrinsically more difficult, but negligence has made the situation even worse. Also, because of existence of various ways to stay anonymous in internet, it is very hard to track down perpetrator let alone bring them to justice. The fact that any digital evidence is just collection of bits represented by signals, magnetization makes any digital evidence fragile and susceptible to damage. Hence, integrity of such evidence is often questioned.

At present we are a developing country and trying our best to be a developed one. In order to digitalize Bangladesh there is no alternative to secured technological advancement among which tenable internet using should prevail in priority. The first step towards ensuring a secure cyberspace must be taken by the government. Only then it is possible to make the vision of ‘Digital Bangladesh’ a reality.

5.1 Cyber Law in Bangladesh

In order to promote e-commerce and enhance information and technology, the Information and Communication Technology Act. 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or both. Although the ICT Act.2006, amended in 2013, is a notable achievement for Bangladesh in cyber law, critics say that there are still some limitations in this Act. Some of the limitations are stated below:

1. Though Domain name is an integral and major issue regarding internet as well as cyber world throughout the world, this Act does not even define "Domain Name" and remains unclear about the rights and liabilities of it.
2. This Act defines e-mails as evidence, that conflicts country's Evidence Act which does not recognize e-mails as evidence.
3. The law is remains silent about various intellectual property like copy rights, trade mark, patent right of e-information and data.
4. This Act does not introduce any crime committed through mobile phones.
5. Spamming has become a hazard in the West as they have made anti-spamming provisions in their cyber law. On the other hand, our act says nothing about it.

5.2 Punishment for Penalty in ICT Act 2006

ICT Act. 2006 declared different punishment for different levels of crimes as listed below:

Punishment for Hacking in Computer Systems: Whoever commits hacking offences, he/she will be punished with imprisonment with a term which can be extended to ten years or fine up to 10 million taka or both.

Punishment for Publishing Fake, Obscene or Defaming News in Electronic Form: Criminals regarding this kind of crime will be punished with imprisonment with a term which can be extended to 10 years or fine with up to 10 million taka.

Punishment for Failure to Surrender License: Will be punishable with imprisonment up to 6 months or fine with maximum amount of taka 10 thousand, or both.

Punishment for Failure to Comply with Order: Punishable with imprisonment up to one year or with fine with maximum amount of one lakh taka, or with both.

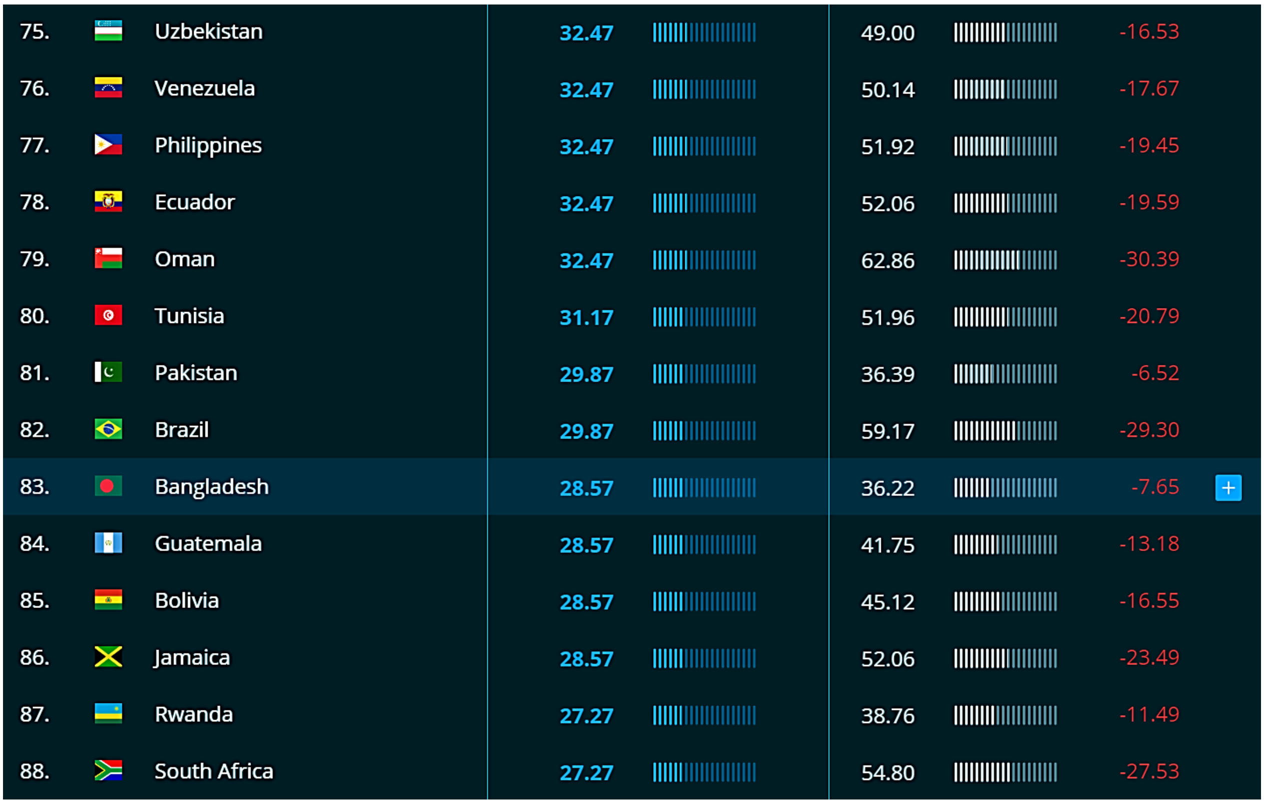
Punishment for Misrepresentation and Obscuring Information: Punishable with imprisonment of two years, or fine up to two lakh taka, or with both.

6. Conclusion

With the technological advancement of the rest of the world, Bangladesh also is becoming digitalized in various sectors such as educational institutes, financial institutes, law-enforcement agencies, hospitals, service sectors etc. Government has declared Vision 2021 to create digitalized platforms in all aspects of living. Besides, private sectors are evolving rapidly to facilitate online shopping, e-commerce, mobile banking, e-banking to the mass people. But due to poor infrastructure and lack of adequate technological knowledge among our people, phishing, hacking and stealing of personal information is a common phenomenon in Bangladesh. Almost 90% software used throughout the country is pirated which makes our system vulnerable to cyber criminals.

The nature of cybercrimes in Bangladesh is almost similar to that of global context. Such occurrences include malicious and intriguing e-mails to foreign diplomatic and VIP personnel, using internet to spread fake news, breaching national crucial websites, using internet for trafficking women and children etc. These incidents are paving the way to conventional social crimes such as kidnapping, committing murders, robbing banks and demanding money by blackmailing using online platforms .Besides, virus attack, exposing obscene materials on webpages, unauthorized access over networks, terrorism against the government, using online social networks to spread militancy among young generation are common incidents nowadays in Bangladesh. Recent conflict between Bangladeshi and Indian hackers affected the diplomatic relation between two countries. For these regards, cyber security has become a major concern for Bangladesh.

Both government and the public should work hand in hand to ensure cyber security of Bangladesh. Various events, symposiums and competition could be arranged to extend the knowledge, skills of the people. And it’ll also help them to become aware of their own cyber security. The private companies and farms can recruit young talents to make a better workforce for the cyber space of Bangladesh. If proper guidance and training is given to this workforce, it’ll come out as a fruitful result. No matter what, only we can protect ourselves and our information. As it seems that public awareness is a must to ensure the security of this country’s cyberspace. Soon time will come when we will stand with the developed nations when it comes to the matter of cyber-security.



75.	Uzbekistan	32.47	49.00	-16.53	
76.	Venezuela	32.47	50.14	-17.67	
77.	Philippines	32.47	51.92	-19.45	
78.	Ecuador	32.47	52.06	-19.59	
79.	Oman	32.47	62.86	-30.39	
80.	Tunisia	31.17	51.96	-20.79	
81.	Pakistan	29.87	36.39	-6.52	
82.	Brazil	29.87	59.17	-29.30	
83.	Bangladesh	28.57	36.22	-7.65	+
84.	Guatemala	28.57	41.75	-13.18	
85.	Bolivia	28.57	45.12	-16.55	
86.	Jamaica	28.57	52.06	-23.49	
87.	Rwanda	27.27	38.76	-11.49	
88.	South Africa	27.27	54.80	-27.53	

Figure 3: Bangladesh ranks 83 in Global Cyber Security Index 2018

Source: https://ncsi.ega.ee/ncsi-index/

Recommendations

Although there are various laws regarding cybercrime worldwide, technological awareness is the best way to prevent this. Here are some basic steps that the tech users of our country should be aware of:

1. **Using Strong Passwords:**

One should not use the same password for different sites. Besides, passwords should be changed regularly. Making complex passwords at least 10 characters long with letters, numbers and symbols is a must. Moreover, anyone can use password management applications that are available on the internet.

2. **Keeping Software Updated and clean:**

This is especially important for operating systems and internet security software. Because cybercriminals usually use known exploits, flaws to get access to another one's systems. So, patching those exploits makes a system less vulnerable. Though it might affect the performance of a device, it's a good idea to frequently delete the saved caches.

3. **Managing Social Media Settings:**

Keeping personal and private information on social media locked down is a must. Social engineering cybercriminals often get one's personal information with just a few data points. So, the less information is publicly shared, the better.

4. **Keeping up to date on Major Security Breaches:**

If somebody is doing business or has an account on a website that has been affected by a security breach, he/she should find the information that hackers have accessed and change the password immediately.

5. **Taking Measures to Help Protect Yourself against Identity Theft:**

Identity theft happens if somebody wrongfully accessed your personal data in a way that involves fraud or deception, typically for economic gain. In this regard, a VPN- short for Virtual Private Network can help you to protect the data you send and receive online, especially while accessing the internet o public Wi-Fi.

6. **Knowing What to Do in Case of Being a Victim:**

If somebody believes that he has become a victim of cybercrime, he should immediately inform the local authority concerned no matter how minor the case is. It will surely help them to investigate and prevent criminals from taking advantages on other people in future.

7. **Remember to log out:**

If a public place network is used to access the internet, it's always best to log out from the public device/network after using the internet. Otherwise, people might get hold of your social media accounts or emails and can steal/manipulate your data.

8. **Be protective of your own data:**

Sensitive information such as, e-mail address, contact number or credit card information should not be shared on these platforms not even through personal or direct message. Anti-virus systems could also be installed to keep the devices free of any type of virus, Trojans and malicious or harmful files. Instead of storing sensitive information on electronic devices, it's always a better idea to go analogue and storing these records in a personal diary.

9. **Checking the terms and conditions:**

During installing social media applications, it should be carefully checked access to what information has been given and why. Moreover, it's wise not to share one platform's security info on another, not even in time of signing up.

10. **Keeping the service updated:**

Government and tech companies can hire White Hat Hackers to keep their system out of harm from unethical hackers. They test the security of a website or a service through their vast knowledge and skills. In this way, they can easily identify the threats or weaknesses of the service. Thus, the service stays updated.

List of References

T. H. Ilves, "Cyber Security: A View from the Front", The New York Times, April 11, 2013

The Prothom Alo, 21 March 2010, Page 24

The Washington Post, June 3, 2012

The New York Times, April 11, 2013

https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics

https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

http://bdlaws.minlaw.gov.bd/

https://www.dhakatribune.com/bangladesh/2018/04/11/several-government-websites-hacked-quota-reform-message

https://www.dhakatribune.com/uncategorized/2013/09/04/foreign-affairs-ministry-website-hacked

https://www.thedailystar.net/country/bangladesh-government-websites-hacked-demanding-quota-system-reform-1561267

https://bdnews24.com/technology/2018/05/26/bangladesh-software-entrepreneur-associations-website-hacked-by-myanmar-group

http://www.newagebd.net/article/51981/62pc-of-banks-in-bangladesh-vulnerable-to-cyber-attack-bibm-study

http://www.theindependentbd.com/arcprint/details/39561/2016-04-05

http://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf

https://pagely.com/blog/cyber-attacks-in-2018/

http://businessnews24bd.com/38-per-cent-banks-ready-to-tackle-cyber-attacks/

https://www.thedailystar.net/star-weekend/cyber-security/news/addressing-cyber-security-risks-the-financial-sector-1636582

https://www.dhakatribune.com/opinion/special/2018/02/05/majority-banks-still-vulnerable-cyber-attacks

https://www.daily-sun.com/printversion/details/268222/2017/11/13/Cyber-security-offinancial-institutions

https://www.soravjain.com/digital-marketing-and-social-media-marketing-stats-and-facts-of-bangladesh

https://en.wikipedia.org/wiki/List_of_data_breaches

http://www.academia.edu/13920817/Cyber_security_in_Bangladesh

Glossary

- **SDLC:** The systems development life cycle (SDLC), also referred to as the application development life-cycle, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.

- **Domain:** A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address.

- **White Hat Hackers:** A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers can detect and exploit them.

- **Data Interference:** When committed intentionally, the damaging, deleting, deterioration, alteration, or suppression of computer data without right; includes inputting of malicious codes (for example, viruses) that can threaten the integrity or use of data or programs.

- **Cache**: A cache, pronounced as cash, is hardware or software that is used to store something, usually data, temporarily in a computing environment.

- **Cookies**: A small text file (up to 4KB) created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

Appendix

Please answer these questions. Put a tick beside your answer.

Question 1: Do you use 2 step verification for your email and other social media accounts?

□ Yes □ No

Question 2: Is your password longer than 10 character?

□ Yes □ No

Question 3: Have you ever been a victim of cybercrime?

□ Yes □ No

Question 4: Do you use your credit card for online payments?

□ Yes □ No

Question 5: Have you ever used same password for different website/ social network?

□ Yes □ No

Question 6: What device do you mainly use to access internet?

□ Phone □ Computer

Question 7: Do you use any antivirus program?

□ Yes □ No

Question 8: Do you feel safe on the internet?

□ Yes □ No