PREVENTION OF CYBER CRIME: BANGLADESH PERSPECTIVE

Dr. Md. Washel Uddin Mollah
Advocate
Supreme Court of Bangladesh

Abstract

Computer crime, also referred to as cyber crime, has increased in severity and frequency in the recent years and because of this it has become a major concern of attention for the companies, universities and organizations. The Governments across the world, police Departments and intelligence units have started to react to cyber crimes. This study provides an overview of cyber crime and examines awareness in different respondents on the issue of cyber crimes in Bangladesh as well as emphasizes the severity of the problem and the urgent need to limit its impact worldwide. It is pertinent to mention that without creating a precise legal framework enabling law enforcement agencies to identify cyber offenders and prosecute them it is almost impossible to prevent cyber-attacks and cyber crimes in Bangladesh. The present technical protection measures in the prevention of cyber-crimes in the country there are many circles and cases wherein such technology is not available or failed or circumvented by a number of barriers. To remove all such obstacles, the existence of a proper legal frame-work is of great importance for recreating and maintaining cyber-security.

Keywords: *Cyber Crime, Law, Internet Crime, Awareness, Prevention.*

INTRODUCTION

Cybercrime is still a low priority in Bangladesh. Though computers are becoming common house hold items and the numbers of internet users have already crossed thirty millions, very few computer related offences are reported to the police. In Bangladesh there is no Computer Emergency Response Team (CERT), no cyber police or virtual police to handle the incidents such as computer abuses, hack attempts and other information security breaches. Bangladesh has enacted the Information and Communication Technology ACT of 2006(Act no 39 of 2006) with a maximum punishment of 14 years of imprisonment or maximum fine of 10 million taka (Bangladeshi currency) or with both for a cyber-crime. Still the legislation seems not to be sufficient to effectively fight cyber-crimes in the country.

The present Government is expected to invest millions of taka to materialize its promise to build a digital Bangladesh. This is why the issue of prevention of cyber-crime must get due priority and a considerable portion of budget should be allocated to ensure the issue. This chapter finds the policy of prevention of cyber-crimes in Bangladesh and also provides some sort of recommendations.

OBJECTIVES OF THE STUDY

It is always emphasized that a problem usually comes with its own seeds of solution. This statement signifies the need of defining the objectives of the research. The main objective of the research is to come up with an important solution that may curb cyber crimes in Bangladesh. In order to achieve this goal, the awareness of the problem of cyber-criminal activities among the people of the country is a must. People must understand how the internet as well as the cyber world operates. The growing danger arising from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. This study investigates whether or not people would use the Internet to report cyber crimes. Main objective, therefore, of the study is to develop an awareness of cyber crimes among the people

as well as to design the way outs and the measures to control and prevent cyber-crimes and address the recommendations to mitigate the loopholes of cyber-laws of Bangladesh.

In this study, some arguments are also intended to be set out in the research-work that can provide links to academic and other material so as to shed light on the examination of the issue of prevention of cyber-crimes in Bangladesh perspective.

METHODOLOGY OF THE STUDY

In this study, I followed the quantitative research in the form of a survey instrument which is used to collect data and descriptive statistics. The decision to follow a quantitative research methodology is based on the fact that the results of the survey should be a representative sample of the total population of the country.

Due to the exploratory nature of the research, research questions are derived from the literature. These questions provide a basis for the research in order to find the awareness of cyber crime among the respondents as well as to find out what type of cyber crimes are occurring these days in Bangladesh and what should be done to prevent cyber crime. The primary target respondents are working professionals who are aware of the various computer crimes and security issues within their organizations. Typically, they are senior managers, IT (The term `information technology' may be meant by IT throughout the study) administrators and IT security consultants. Simple random sampling is the primary sampling method used when selecting the sample for survey.

RESULTS AND FINDINGS

In conducting the research, the researcher uses SPSS (SPSS is a widely used program for statistical analysis in social science) 13.0 software program and takes the hypothesis that there is no association between respondents' occupation and the level of cyber crime awareness.

Fig. 1: Lack of Awareness

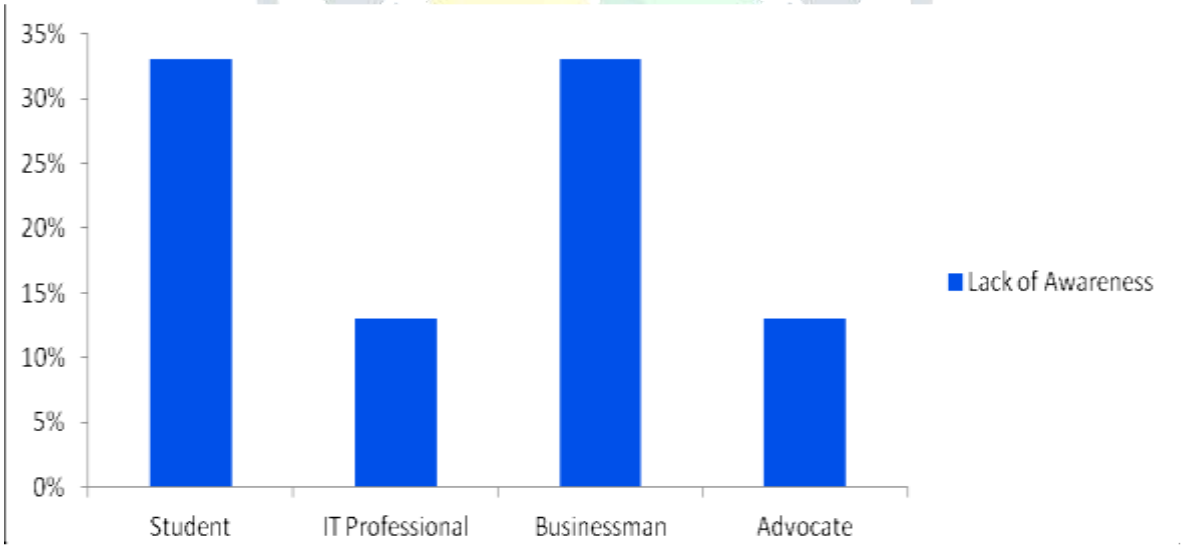

Table 1 shows that among the respondents 33% students, 13% IT professionals, 33% businessman and 13% advocates think that major drawbacks, which prevent cyber crimes from being solved in Bangladesh, is lack of awareness among the people.

Fig. 2: Law Enforcement Agencies not equipped

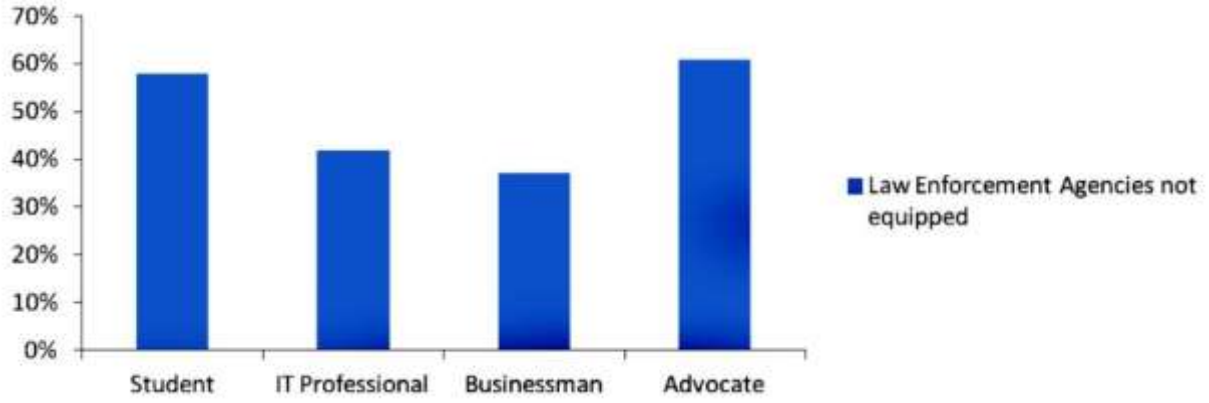

Fig. 2 shows that among the respondents 58% students, 42% IT professionals, 37% businessman and 61% advocates are of the view that law enforcement agencies are not fully equipped with handling cyber-criminal activities.

Fig. 3: All factors

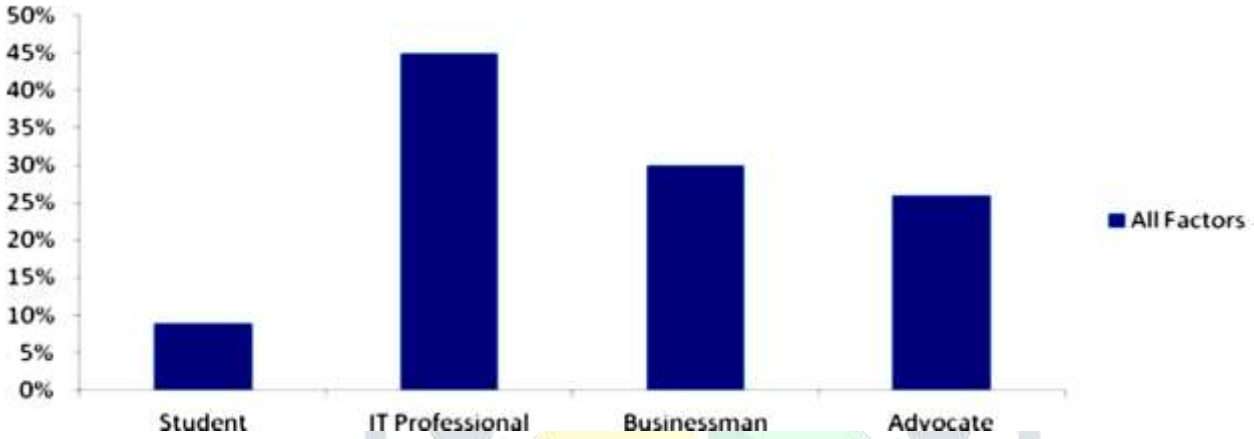

Fig. 3 shows that among the respondents 9% students, 45% IT professionals, 30% businessman and 26% advocates feel that all the factors are responsible for preventing cyber crimes to be solved in Bangladesh.

Fig. 4: Spreading Cyber Crime

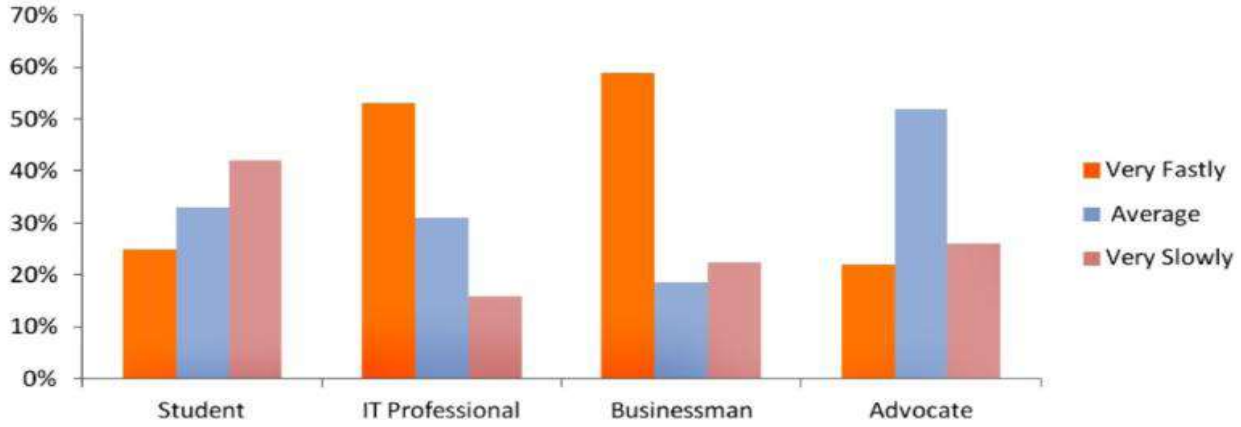

Fig. 4 shows that out of the respondents, on the issue of spreading the disease of cyber crime these days, 25% students, 53% IT professionals, 59% businessman and 22% advocates feel that it is spreading very fast; and 33% students, 31% IT professionals, 18.5% businessman and 52% advocates are of the opinion that it is spreading at an average; whereas 42% students,16% IT professionals, 22.5% businessman and 26% advocates believe that it is spreading very slow.

Critical Analysis

It is rightly said that prevention is better than cure. It is always better to take certain precautions while operating the internet. As Bangladesh is a part of the world community and the country is emerging as an economic as well as political power in the South-Asian region with its GDP of no less than 6.5% over a couple of years, including 7.05% of the year 2016, and a cyber-revolution with the slogan of Digital Bangladesh, which is evident in her providing computer or Internet facilities across the country, including even the remote villages, there is every possibility of cyber-attacks on its cyber system involving financial sectors at any time. It may destroy not only the Internet environment but also the economic condition and development of the country as is evident from the recent Reserve Hacking of 80 billion US dollar of the Bangladesh Bank, the central bank of the country. All the economic, social and political atmosphere of the country, as addressed above, may turn vulnerable by means of such cyber criminal activities that may happen in the country or outside the country. It is, therefore, high time the people of the country have been not only aware of the issue but also sincere in dealing with the Internet or computer arena. In this view one may keep in mind the followings:

1. Children should not give their identifying information such as their names, home addresses, school names, and phone numbers in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive. They should remember that people online might not be who they seem.

2. Parents should use content filtering software on their computers so that their child is protected from pornography, gambling, drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.

3. People should keep back-up volumes so that one may not suffer data loss in case of virus contamination.

4. People should always use latest and update anti-virus software to guard against virus attacks.

5. People should never send credit card number to any site which is not secured.

6. People should not do panic if find something harmful. If there arises any immediate physical danger they should contact local police. Moreover, they should avoid getting into huge arguments online during chat and discussions with other users, and be careful about personal information about themselves online.

7. People should be cautious on meeting online introduced person. They should try to keep record of all communication for evidence and not edit it any way.

8. Big organizations should implement access control system using firewalls, which allow only authorized communications between internal and external network.
9. The use of password is most common for security of network system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.

10. System managers should track down the holes, bugs and weaknesses in the network before the intruders do.

Practices Recommended for Cyber Crime Prevention in Bangladesh

Cyber-attacks could emerge as a major threat to the digital transformation of Bangladesh given the poor knowledge and lack of government initiatives to counter the growing problem, according to the study. Therefore, it is always better to take certain precaution while operating the net.

Firewalls (network security system)

These are programs that protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people whom the user permits.

Frequent password changing

With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.

Safe surfing

Safe surfing involves keeping one's e-mail address private, not chatting on open systems, which do not have adequate protection methods, and visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimize the risk.

Frequent virus checks

One should frequently check ones computer for viruses and worms. Also any external medium such as floppy disks and CD (compact disc) ROMS (read-only memory) should always be virus checked before running.

Email filters

These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.

Online photography

Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

Undergo

Always keep back up volumes so that one may not suffer data loss in case of virus contamination.

Credit Card security

To guard against frauds one should never send credit card number to any site that is not secured.

Depravation in children

Always keep a watch on the sites that children are accessing for the purpose of preventing any kind of harassment or depravation in children.

Secure the Program

It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

Watching Traffic

Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

Protecting internal network

Web servers running public sites must be physically separate and protected from internal corporate network.

Backup

Make Backups of Important Files and Folders to protect important files and records on computer if one's computer malfunctions or is destroyed by a successful attacker.

Off internet

Disconnect from internet when not in use some other advises to be addressed while using the Internet or computers:

1. Habitually download security protection update patches & keep your browser and operating system up to date.

2. Change administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.

3. Disable file sharing on computers.

4. Turn off the network during extended periods of non-use, etc.

5. Check online account frequently and make sure all listed transactions are valid. Use a variety of passwords, not the same for all the accounts.

6. Never respond to text messages from someone unknown.

7. Avoid posting cell phone number online.

8. Open email attachment carefully.

Policies Recommended for Prevention of Cyber Crime in Bangladesh

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bringing into practical part so that the practices become easier to implement. Policies recommended are as follows:

a. Integrated policies are required to ensure the effective benefits from the information system. The basic challenge and issue in the development of a cyber-society is the lack of financial and trained human resources.

b. A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secured and free from cyber crime and within the reach of a common man.

c. Promotion of research & development in ICT (information and communications technology) area and also in Human Resource is to be a core part of the system.

d. Up-to-date, common, and mutually supporting cyber laws should be there to fight with cyber crimes and protection of intellectual property rights towards the creation of cyber-crime free information society.

e. Adoption of ICT standards, regulation, and quality assurance is a necessity to foster high quality of services and productions that keep competition in place for the benefits of the communities within each country.

f. High levels of awareness in each part of the society should be there in regard to information security and cyber crimes and increased exchange of information on information security and cyber crime at the regional and national levels should be there.

g. Effective mechanisms should be there for the detection and prevention of cyber crimes and for improving protection against, detection of, and responses to, cyber crimes, at the lower level itself.

h. Conducting national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and private sector using different media is also a must.

i. The government should educate and involve the media professionals, and then encourage them to increase public awareness.

j. People should engage large private sector corporations and industry associations in the sponsorship of awareness programs.

k. Stress should be laid on less developed countries on effective systems for protection against, detection of and responses to, cyber crime.

l. People should promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.

m. Law enforcement personnel must be trained and equipped in addressing high-tech crimes. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

n. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

o. People should use established network of knowledgeable personnel to ensure a timely and effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis.

p. 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. These cyber crime fighters should be given specialized training home and abroad.

q. Awareness rising, education, and technical support to prevent e-crime (anti-social behaviour over the internet or via electronic devices) is essential, but without discouraging the development of e-commerce.

Minimizing the Risk of Becoming a Cyber Crime Victim

As widespread as cybercrime appears to be, it would be easy to conclude there is little anyone can do to avoid becoming a victim. However, the prevalence of cybercrime does not mean that victimization is inevitable or that people should avoid using the Internet. Users can make themselves aware of the vulnerabilities its use creates and can take steps to reduce their risks.

Use strong passwords

Use separate ID (Own password for access different digital account)/password combinations for different accounts, and avoid writing them down. Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis (Angel Cruz, 2012).

To secure computer

Firewalls are the first line of cyber defence; they block connections from suspicious traffic and keep out some types of viruses and hackers.

Use anti-virus/malware software Prevent viruses from infecting computer by installing and regularly updating anti-virus software.

Block spyware attacks

Prevent spyware from infiltrating computer by installing and updating anti-spyware software.

Secure the mobile device

Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources only. Do not store unnecessary or sensitive information on mobile device. Most importantly, keep the device physically secured; millions of mobile devices are lost each year. In case of loss of device, report it immediately to carrier and/or organization. Some devices allow remote data erasing. Always protect mobile device password.

Install the latest operating system updates

Keep applications and operating system, e.g., Windows, Mac, Linux,(applications of computer operating system) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

Protect the data

Use encryption for most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of important data.

Secure the wireless network

Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid conducting sensitive transactions on these networks. I. *Protect e-identity*: Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secured, especially when making online purchases, or ensure that enabled privacy settings, e.g., when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc. Once something is posted on the Internet it may be there forever.

Avoid being scammed

Never reply to emails that ask to verify your information or confirm your user ID or password. Don't click on a link or file of an unknown origin. Check the source of the message; when in doubt verify the source.

Recommendations

The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their "attack surface" and mitigate the risks. For this purpose the following recommendations may be proposed.

Education on Cyber Crimes

Education is the most important strategy that can be used in combating crimes in the cyberspace. People can be educated in workshops and seminars specially planned by organizations taking into account cyber safety. It is recommended that this should be done on a regular basis as new employees are always recruited. In doing so employees or system users may learn how to keep personal and organization information safe, then the cyber-criminals will flee. The study shows that most of the cyber-criminals of Bangladesh are youths, students of tertiary institutions, or they have graduated from tertiary institutions. It is recommended that tertiary institutes should introduce studies on cyber crimes, and cyber management and its prevention as part of their course curriculum. In doing so the present social changes happening in the country are to be addressed.

Creating Cyber Employment

The Government should act swiftly on domestic cyber crime legislations and enact a comprehensive law on cyber crimes. In order for the law to be effective and efficient the Government should empower graduates by providing employment or funds to be able to employee themselves with their ideas on cyber-crimes (Schjolberg, 2008).

Providing Training

The Bangladesh Government should also make provisions for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals, whatever intelligent and cunning they may be.

Cooperation to Government

For the government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb cyber crimes, it is recommended that there is a need for them to understand the technology and the individuals who engage in such criminal acts. The findings show that cyber criminals are part and parcel of the society, as such, prevention of cyber crimes requires the cooperation of all the citizens and not of the law enforcement agencies alone.

Identification of Cyber Criminals

Everyone should watch and report to law enforcement agencies quickly when they feel someone is being involved in the commission of cyber crimes. This enables the government to bring the cyber criminals to the books of law.

Ensuring Punishment

The assets of the cyber criminals should be confiscated by the government and the imposition of longer prison terms should be enacted for cyber criminals in domestic legislation. This may serve as deterrent to those youths who want to indulge in heinous cyber crimes.

Circulating Current Trends

Innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICT; through this they can not only be well informed about the current trends in cyber crimes but also gather knowledge on different forms of the said crimes, and the methods how the cyber criminals carry out their bad activities. Thereby they can devise means of protecting their information from cyber criminals.

Drawing Consciousness

Internet users should be conscious of security. In simple words, they must learn how not to provide personal or financial information to others unless there is a legitimate and assumed reason. They should not, for instance, throw out cheques, old credit cards, driving licenses, passports, receipts and other numerous documents containing personal data. i. *Awareness of Internet Service Provider*: The internet service providers should not just provide broadband connection to their subscribers, but they should also monitor effectively what the subscribers are doing on the internet. They should provide their customers, especially financial institutions and cyber cafes with well guided security codes and packages in order to protect their information and software from hackers and publishers.

CONCLUSION

In Bangladesh people are at increasing risk of being affected by cyber crimes. Everything of modern life is by any means affected by computers. Cyber crime is everyone's problem. There is no doubt that the Internet offers criminals unparalleled opportunities. There is much that can do to ensure a safe and trustworthy computing environment. It is crucial not only in the personal sense of well-being, but also in the national security of Bangladesh. It is not easy and possible to up root cyber crimes from the society once for all in view of the latest scientific development, but quite possible to combat and check. To achieve the object the first and foremost requirement is the awareness among the people of the cyber crimes and the precautions to prevent the same.

REFERENCES

[1]. Matthews, B. (2008) *Computer Crimes: Cybercrime Information, Facts and Resources. Available at http://www.thefreeresource.com/computer-crimes-cyber information (accessed* on*7 June 2015).*

[2]. Thomas, D., & *Loader,* B. (2000).*Cybercrime: law enforcement, security and surveillance in the information age, Routledge, London*.

[3]. Svensson, P. N. *'hackers target service for corporate boards,' retrieved* available at *http://news.yahoo.com/s/ap/ (accessed 3 February 2016).*

[4]. Nadia Khadam, Insight to Cybercrime, available at http:// www. hanyang.ac.kr/ home_news/H5EAFA/0002/101/2012/29-3.pdf,(accessed 4 February 2016).

[5]. 'International Journal of Engineering Sciences and Emerging Technologies,'vol.6, no.2, 2013, pp. 142-153 available at *https://www.privacyrights.org/content/childrens-safetyinternet (accessed on 1 July, 2017).*

[6]. The Office of Angel Cruz, Chief Information Security Officer, State of Texas September 2012, Volume 6, Issue 8.

[7]. Schjolberg, S. J. (2008). *An International Criminal Tribunal for Cyberspace: Cybercrime Legal Work Group, Geneva, (2007-2008).*

BIOGRAPHY

Dr. Md. Washel Uddin Mollah is an Advocate of the Supreme Court of Bangladesh. He has been practicing for Criminal Sectors in Bangladesh since 2002. He is actively engaged in research activities through his academic career more than ten years and published many research papers. He has participated many international seminars & conferences.