A STUDY OF THE EFFECTS OF CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEMS

Supervised by

AKM Enamul Haque
Associate Professor
MS In MIS Program
Department of CSE
Daffodil International University

Prepared by

Mohammad Soyeb Rana
ID: 163-17-336
MS In MIS Program
Department of Computer Science and Engineering
Faculty of Science and Information Technology
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
Dhaka, Bangladesh

DECEMBER 2018

ACKNOWLEDGEMENTS

This thesis has get the reality with the kind support and coordination of many individuals. I would like to express my gratitude to all of those beloved persons.

Foremost, I want to offer this endeavor to my Almighty ALLAH for my strength, good health, and peace in mind and bestowed upon me in order to finish my academic research.

Also, I would like to express my gratitude towards my parents for help me in completion and encouragement of this research. My supportive and beloved mother, Shahana Islam was always by my side to help in making my study, and my beloved father Shahidul Islam who served as my inspiration to pursue this undertaking.

I am highly indebted to FSIT (Faculty of Science and Information Technology) department for their guidance and constant necessary information regarding this research and also for their support in completing this endeavor.

I would like to express my special gratitude and thanks to my advisor, AKM Enamul Haque for imparting her knowledge and expertise in this study. My thanks and appreciations also go to my colleague and superior Md. Khurshed Alam who have willingly helped me out with his abilities.

DEDICATION

This research paper is dedicated to my honorable teachers and my parents, who honestly helped me to think, understand and express my topic. Without their inspiration, it could be tough to me to make this research.

ABSTRACT

Tough computer technology has made our life so speedy and fast but have come with facilities of some drawbacks. We cannot think our entire activities, government operations and daily business without using computer. This has been made us dependent on it by proliferation of user-friendly, powerful and cheap technology. Besides, it has enabled us to rely on it more importantly in our normal way of life.

Equivalent to more than one third of the total world's population currently directly and indirectly using internet. Developed countries are using more than the developing counties which is approximately 70 percent and 24 percent respectively.

Business firms, private sectors and government organizations which are working with immeasurable valuable secured data and information using internet facilities in both developed and developing countries due to economic and demographic transformations, with rising income disparities, tightened private sector spending, and reduced financial liquidity. This demographic which is also broadly corresponds with a group often at special risk of criminal offending.

The growth of internet can be compared with an infrastructure like the development of roads, electricity, and railways which are dependent on a huge amount of economic investment and proper Management of Information System (MIS). There is no doubt that, Information System (IS) and internet are enhancing capabilities of human interaction in our socio-economic benefits which can be used for criminal activity.

Education and awareness is important to take preventive measures to protect and reduce victimization risk on our Information System (IS) arena and any crime type on it.

Table of Contents

CHAPTER 1

INTRODUCTION

As Information Technology (IT) continues to evolve so also do the opportunities and challenges it provides. I are at a crossroad as I move from an era already entwined with the internet to the coming age of automation, big data and information and various type of Internet of Things (IoT) devices. But Management of Information System (MIS) that runs largely on internet now-a-days, which are also as a result dependent on it. And just as internet brings ever greater benefits, it also brings ever greater threats. Therefore, protecting it is of paramount priority. This paper looks at some of these concerns and provides some background to the nature of digital forensic and fundamentals of cyber-crime which effects on Management Information System (MIS), and focused on-

1.1 OBJECTIVES OF THE STUDY

- To identify the general effects of cyber-crime on Management Information System (MIS) in global perspective.

- To identify the effects and implications of cyber-crime on Management Information System (MIS) in Bangladesh; And

- To find out the preventive measures to protect this crime on Management Information System (MIS) in Bangladesh.

1.2 SCOPE OF THIS STUDY

The study represents a snapshot of an overview of effects, implications and preventive measures of cyber-crime on Management Information System (MIS). As the world is moving round into a hyper-connected community with universal internet access. It is hard to imagine a computer crime and perhaps any crime, that will not involve electronic evidence linked with internet connectivity. But this paper is trying to highlight the effects, implications and preventive measures of cyber-crime on Management of Information System (MIS), focusing the various types of cyberattack, regards to essential infrastructure and governance, developing cyber security for economic growth, education and awareness to create a safe information world from both angle of global and local perspective.

1.3 METHODOLOGY

The methodology for this study tasked the United Nations Office on Drug and Crime with developing the study, including developing a questionnaire for the purpose of information gathering, collecting and analyzing data, and developing a draft test of the study. Information gathering in accordance with the methodology, including the distribution of a questionnaire to member states, Intergovernmental Organizations and representatives from the private Sector and academic institutions, was conducted by UNODC. Information was received from 69 member states with regional distribution, from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations, and various reports from news media, news portals and open sources documents.

1.4 LIMITATIONS

In spite of best of efforts to minimize all limitations that might creep in course of the research, there Ire certain constraints within which the research was completed. HoIver, the objectives of this research is to find out the effects, implications and preventive measures of cyber-crime on Management Information System (MIS), which are continue introducing a new era and new term of cyber world, which may not covering in this research at all. Cyber-crime on Information System (IS) is a vast and is not an optional topic in our technology world. It is a part of the design of every product, of every Information System (IS), of every electronic communication. And although education, awareness, and proactive change of Information System (IS) database – I can all play a part in securing our Information arena. But this vast amount of such terminologies are really hard to showing up and explore within this short curriculum schedule, which is made for our educational purpose only.

1.5 SOURCES OF DATA

This research was based on secondary as Ill as primary data. The primary data required for research was collected from United Nations Office on Drugs and Crime. Although UN is an authentic international information hub, it cannot be considered as a proper representation of cyber-crime on Management Information System (MIS) in recent world.

Various reports from news media, news portals and open sources documents are also been used to make a complete and comprehensive research report on cyber-crime effects on Management Information System (MIS) of our current world.

CHAPTER 2

AN OVERVIEW OF CYBER-CRIMES

2.1 INTRODUCTION

The world of internet today has become a parallel form of life and living. Public are now capable of doing things which Ire not imaginable few years ago. The internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others, which are becoming exclusively dependent on automation and I can see its influence on all spheres of our life. The history of automation began when Babbage invented computer and especially a new horizon I opened before us with the invention of network particularly the Internet and World Wide Ib (WWW). Internet has become the backbone of all kinds of communication systems and it is also one of the most important sources of knowledge in the present digitalized world.

It is a network of network, that consist of millions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The World Wide Ib (WWW) is a huge set of interlinked documents, images and other resources, linked by hyperlinks and URLs.

HoIver, the means that internet allows computer users to connect to other computers and networks to share and store information easily across the world. This free flow of information across borders also give rise to worryingly high incidence of irresponsible behavior. They may also offer to do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This free access to network creates privileges to illegal deeds in the cyber world. Any technology is capable of beneficial uses as Ill as misuse.

The most common evil doings are crashing a computer system, theft of valuable and secured information contained in electronic form; email bombing, data diddling, financial fraud like unlawful transfer of money by breaking the security code of credit cards, denial of services and virus attacks. In where, the intruders directly attracts against Information System (IS), and the Management of this Information System (MIS) is going to be more challenging job after day by day, where the negative effect is much more alarming for the technology arena of Information System (IS).

2.2 DEFINING CYBER-CRIME

Definition of cyber-crime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cyber-crime. Now-a-days it is the latest and perhaps the most complicated problem in the cyber world. "Cyber-crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime" "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime”

A generalized definition of cyber-crime may be “unlawful acts wherein the computer is either a tool or target or both”. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, cyber stalking. The computer may hoIver be target for unlawful acts in the following cases- unauthorized access to computer/computer system/computer networks, theft of Information System (IS) contained in the electronic form, email bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, Ib jacking, theft of computer system, physically damaging the computer system.

There is apparently no distinction betIen cyber and conventional crime. HoIver on a deep introspection I may say that there exists a fine line of demarcation betIen the conventional and cyber-crime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber-crime.

2.3 CLASSIFICATION OF CYBER-CRIME

Cyber-crime mostly a property related crime. It has no direct contact with the victims and involves less visible and intangible kinds of property such as information, data and computer networks. Victims come to know about their losses long after the actual communication of crimes. Profits from high-tech crimes are vast. Hackers are able to steal greater amount with greater comfort; a single act can victimize many people in many places at once. It may be divided into two types-

1. Crimes that target computer networks or resources directly.
2. Crimes facilitated by computer networks or devices.

Examples of crimes that primarily target computer networks or devices would include malware and malicious code, denial-of-service attacks and computing viruses. Examples of crimes that merely use computer networks or devices would include, among others, cyber stalking, fraud and identity theft and information warfare. It is further subdivided into the following four categories.

- ➢ Cyber-crime against individuals.
- ➢ Cyber-crime against property.
- ➢ Cyber-crime against organization.
- ➢ Cyber-crime against society at large.

This crime can be broadly defined as criminal activities using information and communication technology including the followings, which can be committed against the above mentioned groups. Above mentioned offences may discuss in brief as follows:

2.3.1 HARASSMENT VIA EMAILS

Harassment through emails is not a new concept. It is very similar to harassment through letters. Recently, I had received a mail from one of my fried wherein she complained about the same. Her former boyfriend was sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is very common type of harassment via emails.

2.3.2 CYBER-STALKING

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

2.3.3 PORNOGRAPHY

Pornography on the net may take various forms. It may include the hosting of Ibsite containing these prohibited materials. Use of computers for producing these obscene materials. Downloading through the internet, obscene materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal-Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

2.3.4 DEFAMATION

It is an act of imputing any person with intent to loIr the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium e.g. the mail account of Mr. X was hacked and some mails Ire sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.

2.3.5 UNAUTHORIZED ACCESS / HACKING

Hacking is a simple term which means illegal intrusion into a computer system without the permission of owner/user.

2.3.6 EMAIL SPOOFING

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it’s origin to be different from which actually it originates. Recently spoofed mails Ire sent on the name of Mr. Na.Vijayashankar (naavi.org), which contained virus. Rajesh Manyar, a graduate student at Purdue University in Indiana, was arrested for threatening to detonate a nuclear device in the college campus. The alleged email was sent from the account of another student to the vice president for student services. HoIver the mail was traced to be sent from the account of Rajesh.

2.3.7 COMPUTER VANDALISM

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

2.3.8 INTELLECTUAL PROPERTY CRIME

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc. The Hyderabad Court has in a land mark judgement has convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software.

2.3.9 CYBER TERRORISM AGAINST GOVERNMENT

At this juncture a necessity may be felt that what is the need to distinguish betIen cyber terrorism and cyber-crime. Both are criminal acts. HoIver there is a compelling need to distinguish betIen both these crimes. A cyber-crime is generally a domestic issue, which may have international consequences; hoIver cyber terrorism is a global concern, which has domestic as Ill as international consequences. The common form of these terrorist attacks on the internet is by distributed denial of service attacks, hate Ibsites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of – Osama Bin Laden, the LTTE, and attack on America's army deployment system during Iraq war.

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives" Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to –

- Putting the public or any section of the public in fear; or
- Affecting adversely the harmony betIen different religious, racial, language or regional groups or castes or communities; or
- Coercing or overawing the government established by law; or
- Endangering the sovereignty and integrity of the nation.

And a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

2.3.10 TRAFFICKING

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms Iapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs Ire being sold under the pseudonym of honey.

2.3.11 FRAUD & CHEATING

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. Recently the Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer working in a call centre, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony Ibsite. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating under IPC, but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs 20,000, and was released on a year's probation.

2.4 REASONS BEHIND CYBER-CRIME

“The Concept of Law” has said ‘human beings are vulnerable so rule of law is required to protect them’. Applying this to the cyberspace I may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber-crime. The reasons for the vulnerability of computers may be said to be:

2.4.1 CAPACITY TO STORE DATA IN COMPARATIVELY SMALL SPACE

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

2.4.2 EASY TO ACCESS

The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

2.4.3 COMPLEX

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber-criminals take advantage of these lacunas and penetrate into the computer system.

2.4.4 NEGLIGENCE

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber-criminal to gain access and control over the computer system.

2.4.5 LOSS OF EVIDENCE

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

2.5 CATEGORIES OF CYBER-CRIMINALS

The cyber-criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber-criminals.

2.5.1 CHILDREN AND ADOLESCENTS BETWEEN THE AGE GROUP OF 6 – 18 YEARS

The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal-Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

2.5.2 ORGANIZED HACKER

These kinds of hackers are mostly organized together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as Ill as the Microsoft sites is always under attack by the hackers.

2.5.3 PROFESSIONAL HACKER/CRACKER

Their work is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are vend employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

2.5.4 DISCONTENTED EMPLOYEES

This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

2.6 MODE AND MANNER OF COMMITTING CYBER-CRIME

2.6.1 UNAUTHORIZED ACCESS TO COMPUTER AND NETWORK

This kind of offence is normally referred as hacking in the generic sense. HoIver the framers of the information technology act 2006 have nowhere used this term so to avoid any confusion I would not interchangeably use the word hacking for 'unauthorized access' as the latter has wide connotation.

2.6.2 THEFT OF INFORMATION CONTAINED IN ELECTRONIC FORM

This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

2.6.3 EMAIL BOMBING

This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

2.6.4 DATA DIDDLING

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerized.

2.6.5 SALAMI ATTACKS

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

2.6.6 DENIAL OF SERVICE ATTACK

The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

2.6.7 VIRUS / WORM ATTACKS

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses Ire accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert

Morris sometime in 1988. Almost brought development of Internet to a complete halt.

2.6.8 LOGIC BOMBS

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

2.6.9 TROJAN ATTACKS

This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized program, which passively gains control over another's system by representing itself as an authorized program. The most common form of installing a Trojan is through e- mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber-criminal through the Ib cam installed in the computer obtained her nude photographs. He further harassed this lady.

2.6.10 INTERNET TIME THEFTS

Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa's case- the Internet hours Ire used up by any other person. This was perhaps one of the first reported cases related to cyber-crime in India. HoIver this case made the police infamous as to their lack of understanding of the nature of cyber-crime.

2.6.11 IB JACKING

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the Ib site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also Ib jacked. Another case of Ib jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded as ransom. Thus Ib jacking is a process whereby control over the site of another is made backed by some consideration for it.

CHAPTER 3

GENERAL EFFECTS OF CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEM (MIS)

3.1 PERCEPTION OF THE IMPACT ON MANAGEMENT INFORMATION SYSTEM

The impact of cyber-crime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap betIen lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. HoIver, it is especially true in cryptography, used for securing transactions and data interchange as Ill as to secure communications covering illegal activities and the establishment of evidence. History shows that new technologies, rarely regulated and not fully complete, are both used for good and bad. The nest ten years will be marked by mobility, with the need for availability, real-time communication, connectivity, and a dependence on digital identity equipment and risk. This decade will also include monitoring automata systems and increasingly new risks.

Over the past decade management of information systems security has emerged to be a challenging task. Given the increased dependence of businesses on computer-based systems and networks, vulnerabilities of systems abound. Clearly, exclusive reliance on either the technical or the managerial controls is inadequate. Rather, a multifaceted approach is needed. Historically, management of information security has mostly relied on technical control measures; hoIver, research has shown that the majority of information security failures occur because of violations of controls by trusted personnel. This suggests that management of information security can only be adequately assured if the emphasis goes beyond technical controls and incorporates business process and organizational issues. Management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program. Some of the most salient issues include asset valuation, auditing, business continuity planning, disaster recovery planning, ethics, organizational communication, policy development, project planning, risk management, security awareness education/training, and various legal issues such as liability and regulatory compliance.

3.2 NEGATIVE EFFECTS ON MANAGEMENT INFORMATION SYSTEM (MIS)

Expected developments, which may have a negative impact on Information System (IS) for cyber-crime, render little distinction between work life and private life, using for example the difficulty of locating information for a company and Ib applications with cloud computing, targeted stealth malware, and more generally, the massive use of new technologies, including mobile and wireless technologies, and a careless exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past. I must emphasize the volatile nature of finding data as evidence and the difficulty of reporting offences to the sources, with no legal means, because cybercriminals are adapting alongside new technologies.

3.3 POSITIVE EFFECTS ON MANAGEMENT INFORMATION SYSTEM (MIS)

Security measures based on these same technologies could have a positive impact. Information Security is central to the problem and must be based on policies and be strictly enforces. It will be a major challenge with cloud computing, due to the complexity of where data is stored and the numerous jurisdictions involved, major risks associated with governance and territoriality. The effective level of quality security will be a key factor in the acceptance of these new services.

3.4 THE MANAGEMENT OF INFORMATION SECURITY REGARDING CYBER-CRIME

Information security management is the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission. Ideally, information security management activities should be driven by organizational objectives so that no resources are expended on security without an explicit documented understanding of how it supports the organizational mission. Historically, information security management has been dealt with solely by establishing technical and physical controls. However, the increasing use, value, and dependence on computerized systems to support real world operations have increased the importance of incorporating process and organizational issues in security risk management. Information security risk management, the process used to identify the optimal protection strategy when constrained by a limited security budget, has evolved as a required function within organizations which are concerned with their ability to mitigate the effects of a breach of information security. Such breaches are referred to as "incidents." Risk analysis, the first step of the risk management process, requires the identification and documentation of critical organizational resources (e.g., information, people, processes, and technologies) among a huge number of total information resources that are used to support the organizational mission. Determining criticality is not trivial. It requires an estimation of the value the resource provides to the organization based upon how it supports the organization's strategic objectives. The scale and complexity of the organization, interdependencies between resources, and the dynamic nature of resource utilization greatly complicate value determination. However, an accurate resource valuation is essential as it directly impacts the quality of the decisions made during risk management. The valuation, in conjunction with an estimation of threats, vulnerabilities, and the likelihood (per unit time) of their intersection, is used to determine the potential damage to a resource, given the state of the organizational security capability. Collectively, this information provides the ability to rank order and address risks by risk avoidance (e.g., change processes), transference (e.g., outsource), mitigation (e.g., apply control measures), or acceptance (e.g., accept possible losses), commensurate with the value of the resource.

Proper day-to-day and strategic management of information security operations are among critical success factors in achieving organizational goals. Pipkin [2000] identifies a cyclic, five- phase process to conceptualize the information security management process: inspection, protection, detection, reaction, and reflection. The inspection phase requires the identification, valuation, and assignment of ownership of information assets critical to the organization; the protection phase requires the assignment of the control measures to protect critical information assets commensurate with their value; the detection phase requires the development of robust detection capabilities to insure that any breach of the organization is detected in a timely manner; the reaction phase requires that the organization has developed the resources and capabilities to quickly respond, contain, investigate, and remediate breaches; and the reflection phase requires effective post-incident documentation, reporting, and accountability to assure institutional learning. Pipkin asserts that assuring organizational security requires consideration of all the five phases. Neglecting any one of the five phases can expose the organization to excessive losses when they inevitably experience an information incident. Unfortunately, as will be shown in the next section, organizations are not aware of, choose not to, or are not capable of implementing these phases in an effective and efficient manner

3.5 CHALLENGES / ISSUES IN MANAGEMENT OF INFORMATION SECURITY FOR CYBER-CRIME

The management of information security faces three major challenges. First, even after decades of research in the theory and practice of IS security, its management is usually considered as an afterthought. Second, largely because security is considered as an afterthought, the problem of development duality creeps in. Third, conceptualizations of information security have largely been a theoretical. I believe that a focus on these three challenges will help in defining and addressing many of the problems in managing information security.

CHAPTER 4

EFFECTS AND IMPLICATIONS OF CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH

4.1 BANGLADESH: INTERNET HISTORY

In late 1995, the government of Bangladesh invited applications to subscribe the VSAT (Very Small Aperture Terminal) data circuits and on June 4, 1996 the VSAT connection was commissioned and the internet was launched in Bangladesh for the first time and the first usage of internet was the publication of the National Polls Result in 1996.2 But this introduction could not create a good market at the very initial stage. After the year 1996, there were only two ISPs (Internet Service Providers) and about one thousands of users in the country. But the year 1997 is a landmark in this field as it recorded a tremendous advancement in internet using. The number of ISPs increased into twelve and users into ten thousand.

Afterwards some new ISPs started their service which fuels the proportional advancement of this sector. However, the government adopted more liberal national policies for a sustainable and rapid growth of this industry and as a result we had 180 ISPs by 2005. In 2006 Bangladesh got connected with Submarine Cable (SEA-ME-WE 4 Submarine Cable) which afforded big bandwidth and low cost than ever before. After this, over the years Bangladesh Telecommunications Company Ltd., BTCL (Now BTRC, ‘Bangladesh Telecommunication Regulatory Commission’) reduced the bandwidth price at regular intervals which attracted more and more users towards the internet world. As of now BTRC has about three hundreds and forty five (ISP Natiowide-94, ISP Central Zone-79, ISP Zonal-53, ISP Category A-99, ISP Category B-16, ISP Category C-04) registered ISP license holders3 and there are approximately 4.5 million users connected to them which is about 0.32% of our total population.

4.2 PRESENT SCENARIO OF MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH

Bangladesh does not have enough natural resources and has been trying to achieve the economic development through the utilization of ICT industry. Over the last few years, many nations have taken advantage of the opportunities afforded by ICT within a policy framework, laid down guidelines and proceeded with the formulation of a national ICT strategy as a part of the overall national development plan. Bangladesh intends to use ICT as the key-driving element for socio-economic development.

The present government has also declared the vision-2021 i.e. within 2021 this country will become Digital Country and the per capita income will be equal to a middle income country. But the government as well as other concerns should consider crimes that may be committed in this world with the expansion of internet and other networks to convert this country into a digital country.

The first recorded cyber-crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been in India, Japan and China around since 3500 B.C. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber-crime in the world history. A recent survey showed that a new cyber-crime is being registered every 10 seconds in Britain. The situation of other countries in the world is almost the same and in some cases it is more critical and miserable. On July 4, 2009 two dozens of websites of South Korea and United States of America's were under cyber-attack and the attack was remarkably successful in limiting public access to victim web sites such as government web sites, treasury department, federal trade commission and secret service.8 They were continuously reporting problems days after the attack started during the July 4 holiday. IT experts believe that about 90 percent of cyber-crimes stay unreported. In case of Bangladesh, the situation is getting worsening day by day. The most common cyber-attacks and crimes are listed below in Bangladesh:

- Blackmailing girl by capturing their nude photographs and video on the sly and threatening to expose publicly. Such incidents are caused frequently by their boyfriends and others.
- A number of community websites have been introduced, which the young girls and boys are using to exchange phone numbers for Posting hidden videos or even pictures with nudity etc.

- Hacking in the website of Bangladesh Computer Society, which took place after a few days of a 3 day-long 'Regional Seminar on Cyber-crime' in Dhaka.

- E-mail threatening the current Prime Minister Sheikh Hasina from a cyber cafe.

- Hacking into the Internet account of Barisal DC office in 2003 AD, the incident was revealed after the DC office received a heavily bloated Internet bill and lodged a complaint with the Bangladesh Tar and Telephone Board (BTTB).

- Hacking took place in the website of Bangladesh Rapid Action Battalion (RAB) in 2008, during the access to www.rab.gov.bd, the website read: "Hacked by Shahee Mirza.

- Hacking the mail of BRAC Bangladesh.

- Stealing the transaction report of Dhaka Stock Exchange through hacking.

- Inserting naked pictures to the website of Bangladesh National Parliament.

- Inserting naked pictures to the website of Jamate Islami Bangladesh.

- Inserting naked pictures to the website of The Daily Jugantor.

- E-mail threatening to World Bank Dhaka Office.

4.3 ICT POLICIES AND CHALLENGES FOR MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH.

In order to improve the living standard of the common mass through expansion of development activities in science and technology and its application, the Government of Bangladesh has formed National Council for Science and Technology (NCST). The Executive Committee for NCST has also been formed to implement policies formulated by the Council.

Recently formulated National Information and Communication Technology Policy (2002) has also given enormous importance to the development of ICT for capturing our share in the multi-billion dollar software export market, for ensuring good governance, for enacting ICT related policies, special allocation of funds for software projects, development of world class ICT professionals and creation of a world class ICT institution for promoting excellence in the field.

The Vision of this Policy aims to building an ICT-driven nation comprising knowledge-based society by the year 2006. To achieve this objective, a country-wide ICT-infrastructure will be developed to ensure access to information by every citizen to facilitate empowerment of people and enhance democratic values and norms for sustainable economic development by using the infrastructure of human resources development, good governance, e-commerce, banking, public utility services and all sorts of on-line ICT-enabled services.

National ICT Policy includes issues of human resource development, creation of ICT infrastructure, facilitating research and development on ICT, development of ICT industries on a priority basis. It has also highlighted importance of hardware industries, e-Commerce, e-Governance, legal issues related to ICT, application of ICT in health care, application of ICT in agriculture to exploit the potential for development of rural economy and agro-business. Application of ICT in other areas like social welfare, transportation and the judiciary system is also highlighted.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) has adopted a Model Law on Electronic Commerce. This is known as UNCITRAL Model Law of e-commerce. In conformity with UNCITRAL Model Law, Bangladesh has drafted an ICT Law, which has been approved by the highest authority in February 2005 to facilitate electronic commerce and to encourage growth and development of information technology.

The ICT Law establishes rules and norms that validate and recognize contracts, forms through electronic means, sets default rules for contract formation and governance of electronic contract performances, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes and supports the admission of computer evidence in courts and arbitration proceedings. In addition, the Copy Right Law 2000 has been amended to include computer software.

The Government is committed to mounting a direct and sustainable effort on the reduction of poverty, enhancing livelihood security, removal of hunger and malnutrition and generation of employment. This will call for generation and screening of all relevant technologies, their widespread dissemination through networking and support for the vast unorganized sectors of our economy.

Realizing the importance of ICT and the enormous impact it can create in our everyday life, the name of the Ministry has been changed from Ministry of Science and Technology to the Ministry of Science and Information & Communication Technology. The Ministry of Science and ICT have been entrusted with the responsibility of harmonious growth of this sector in Bangladesh. Bangladesh Computer Council (BCC), the apex body having the responsibility for promotion of all sorts of ICT activities in the country, is also governed by the Ministry of Science and ICT.

Development of Science and ICT depends on the expansion of telecommunication sector. This sector is still under developed due to lack of deregulation and open competition. In 2002, independent telecom regulatory authority, Bangladesh Telecommunication Regulatory Commission (BTRC) has been created.

4.4 CYBER SECURITY REALIZATION FOR MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH

Most of the developing countries like Bangladesh have limitations in access to information and the available access is not affordable because of the inadequacy of the existing infrastructure as well as the non-availability of appropriate education. The challenges are posed by the lack of an integrated computer security system and education about computer security. Therefore, there is a need for co- operation; collaboration and investment for security, which also develop the culture of security needs for assuring the security issue. As in business or any dealings, trust is important and trust can be achieved when the practitioners feel that the transaction is secured. Security from a business perspective must therefore be seen as a business enabler not as cost.

Our challenges are posed by the lack of an integrated computer security system and education about computer security is therefore one of the most important issues. Bangladesh is planning, as important next steps for awareness raising and the provision of appropriate knowledge, as well as the development of security guidelines. Further exploration activities are needed on standards for the security of information systems. In order to realize these objectives, global partnership is indispensable.

We also realize that Research and Development is more important for Information Security Framework Program at the same time for successful program we need to have advisory functions, that contribute to awareness rising and co-operation, promote risk assessment methods and best practices and follow standardization efforts, thus contributing to the development of a global approach to information security.

Bangladesh become conscious that Information security is an important business enabler and for further co-operation between countries and across sectors is essential and there is a need to find ways to ensure effective public-private partnerships. There is an urgent need to develop a cyber-crime legislation that will protect cyber security. There is also a need to have more projects on cyber-crime legislation and enforcement capacity building and training courses throughout the country. Policies of the country should also include privacy policies, trust marks and other self-regulatory measures for the development of products and provision of services and the implementation of the necessary measures for establishing consumer confidence.

CHAPTER 5

PREVENTIVE MEASURES TO PROTECT CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH

5.1 SCENARIO OF PREVENTIVE MEASURES OF CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEMS (MIS)

When internet was developed, the founding fathers of internet hardly had any Idea that internet could also be misused for criminal activities. But the fact is that it is happening roughly and largely all over the world. Now the question is how these offences can be treated-whether through conventional or something extraordinary methods. If we have a deep introspection it will be proved that apparently there is no great difference between conventional crime and cyber-crime.19 the first demarcated difference line is the medium of committing the offence. Conventional crimes are prima facie territorial and occurred in physical world, but cyber-crime is territorially unlimited and occurred in the world which is an electronic or virtual one. Some other major questions are raised regarding the nature of the cyber-crime that whether it is a criminal offence or a civil wrong or tort. The answer would depend on the nature of the occurrence. After the ICT (Information and Communication Technology) Act, 2006 being passed all the aforesaid computer crimes are now treated as criminal offence.

Changes is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changes their method and have started relying of the advanced technology, and in order to deal with them the society the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber-criminals. Thus necessary facilities must be established in various parts of the country so that crime in the virtual world can be contained. Another aspect which needs to be highlighted is that a culture of continuous education and learning needs to be included amongst the legal and the law enforcement authorities because the Information Technology field is a very dynamic field as the knowledge of today becomes obsolete in very short time.

5.2 REMEDIES AVAILABLE AND THEIR DRAWBACKS FOR CYBER-CRIME ON MANAGEMENT INFORMATION SYSTEMS (MIS) IN BANGLADESH

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. This advancement demands ICT experts of which we have great lacking. The state should move forward for creating such experts with indispensable national ventures. Besides this statutory shields should be made most effective by executing the aforesaid course of actions. Finally, we have to remember that technology is such a thing which is changing its nature and direction every moment and we have to achieve the maximum capability to fight its change in every moment change both in physical and virtual world for a perpetual existence.

A proverb goes 'Prevention is better than cure'. For prevention of numerous cyber-crimes it is better to initiate advanced technological actions. These are technological precautionary affairs for prior prevention. We will rather try to find out the legal and other remedies and their lacking available in Bangladesh for curing the alleged cyber-crimes. A cyber victim in Bangladesh has a better opportunity to get the proper remedy under the ICT Act, 2006. This statute is the first and the only door open for the lawful remedy of numerous cyber-crimes in Bangladesh. Through this statute it is being tried to locate all the probable grounds of cyber-crime frequently occurring at present and which might occur in future as well like damaging any computer or computer system, hacking, spreading viruses and false information, causing defamation through the internet, changing the source code, stealing or damaging any text, audio, video documents etc. Provisions for special Cyber Tribunals20 (both Original and Appellate) and punishments of lighter/severe form have been fixed.

In addition to the above mentioned remedies it is also noted that even after three years of passing this Act not a single case is filed under this law. Mass people are not so aware about such types of new crimes and the procedure of their remedy. One of the causes of this may be that no Cyber Tribunal and Cyber Appellate Tribunal have been formed by the government yet. Moreover as per the provisions of the ICT Act a good number of other procedural and structural hurdles also exist which are as follows:

Firstly, a session judge or an additional session judge will preside over the Cyber Tribunal21 and a bench of three members including a chairman who will be an ex or acting judge or a competent person to be a judge of Supreme Court and an ex or acting Dist. Judge and an ICT expert, two other members of the bench, will preside over the Cyber Appellate Tribunal22 and like the other criminal cases Public Prosecutors will prosecute on behalf of the state in this regard. The problem is that judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the opportunity to be assisted by the ICT expert. But is it possible to give the verdict on the basis of another's knowledge? The reality in our country is that so far no initiative is taken by the government to train up the judges for acquiring the minimum technological knowledge required for ensuring justice.

Secondly, a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer) 23 regarding the cyber-crimes. Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. So, is it possible for such a police officer to make a proper investigation into such matters? Moreover, it may result in a snag to justice.

Thirdly, the government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of those proposed tribunals.24 Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state.

Proper execution of statutes ensures the rule of law. Circumstances say that inadequate execution of the ICT Act, 2006 is one of the root causes for the increasing cyber-crimes in Bangladesh. The solution of those aforementioned problems demands that the state must take nippy steps along with logistic and financial assistance.

5.3 SOME NEW DIMENSIONS AS REMEDY FOR MANAGEMENT INFORMATION SYSTEMS (MIS) AGAINST CYBER-CRIME IN BANGLADESH

No doubt technological defense is better than legal remedy in preventing hi- tech crimes, but there is always a chance of destruction of such defenses as these are not of perpetual nature. People who are more advance in technology than us can smash the security wall anytime. So, legal and other related remedies are obligatory to fight the war against the said circumstances. In addition to the present remedies the state can commence some new course of actions which are being trailed by some developed hi-tech state of the world. Let us have a glance at their features:

5.3.1 CONSTITUTIONAL SAFEGUARD

Bangladesh is a country of constitutional supremacy. Constitution plays the mother role in preserving and ensuring the rights and duties of both the state as well as the mass people. Constitutional provisions against cyber-crimes may escort the cyber warfare to a national temperament which may result in a better form than any other organizational and legal remedy. Constitutional amendment may be the introducing procedure of such provisions.

5.3.2 SPECIAL WING OF POLICE

For a digital Bangladesh, we need to equip our law enforcement agencies with training and technology to ensure peaceful cyber cloud. Cyber-criminals are not the rivals of any specific country or of a region; rather they are the common enemies of the world. Citizens of the 21st century need to fight together against their common enemies. The rise of cyber-crime insists the law enforcers to work as global police rather than regional or national police only. The Police Force through global partnership need to be able to meet the challenges of the technology to curb all crimes including Cyber-crime. U.K., U.S.A, India, Malaysia and some other developed countries have established special wings of police to combat the cyber war. Bangladesh can initiate such special police wings as a new armament against hi-tech threats along with other deterrent actions.

5.3.3 CYBER-CRIME AGENCY BY GOVERNMENT

On the last 23rd July of 2009 North Korea twisted 'Korea Internet and Security agency'25, a government agency uniting three of its preceding internet technology organizations. Now, this agency will endeavor to make North Korea a stronger and a safe advanced country in using internet. India and some other countries have also created such agencies. Considering the present situation of using internet and increasing cyber-crime in Bangladesh, Government can also commence such types of agencies. The worth of such agencies is that these will be able to perform multidimensional actions like advancing the internet infrastructure, maintaining the ISPs, fixing the internet using charges, preventing the cyber threats etc.

5.3.4 WATCH DOG GROUP

These groups are enormously internet like the security oriented intelligence. They include capturing and receiving malicious software, disassembling, sandboxing, and analyzing viruses and Trojans, monitoring and reporting on malicious attackers, disseminating cyber threat information etc. This doggy concept is not a new one. 'Shadow Server Foundation' can be an example of Watch Dog Groups which was established in 2004. These may be individual as well as governmental. At present there is no such organization in Bangladesh, but in consideration with the escalating cyber threats, these doggy groups can be one of the vital constituents for developing Bangladesh as an advanced country especially in internet technology.

5.3.5 PUBLIC AWARENESS

This course is no less important than technological precautionary actions, because most of the time common people become the victims of cyber threats and millions of computers are crashed away. So if it is possible to aware the populace about the nature, possible impairment and the antidote of the threats, it would be more convenient to defeat cyber-criminals as well as save the virtual world and government can play the crucial role here. Like other vital issues, the government should create awareness among the mass people all over the country through different media. Besides, NGOs and other organizations can commence campaign in this regard.

CHAPTER 6

CONCLUSION

CONCLUSION

Modern organizations are heavily dependent on computerized information systems for everyday operations, strategic decision making, and all the administrative activities. Dependencies are increasing at every second alone with emerging the usages of Information Technology, organizations have become increasingly vulnerable to attacks through their networks and their information systems. Proper management of information security has become a very important consideration. Cyber-crime and protective measures to avoid this, is not only a technical issue but a risk management and business process issue which must be viewed through multiple lenses.

RECOMMENDATIONS

In order to properly address this issue, we have identified three relevant management problems. These are: 1) addressing security after the system has been developed, resulting in an overall less secure system; 2) parallel design of security and information systems; and 3) lack of theories in the development of solutions to these crimes. This identification provides a fertile ground for development and testing of new theories. The most important consideration in developing the security tools and hands that will protect these crimes at all. This requires deep understanding of real world cyber-security management problems followed by their classification, categorization, and attribution.

REFERENCES

Cyber Crime Today &Tomorrow, Thiru DayanithiMaran

Cyber crime Up Police found wanting, Chandigarh Tribune Monday May 28, 2001.

Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30, 2006.

Duggal Pawan - Is this Treaty a Treat?

Duggal Pawan – The Internet: Legal Dimensions

Duggal Pawan – Cybercrime

Kapoor G.V. - Byte by Byte

Kolkata man threatens to blow up Stock exchanges arrested. Express India.com

Kumar Vinod – Winning the Battle against Cyber Crime Mehta Dewang- Role of Police in Tackling Internet Crimes Nagpal R- Defining Cyber Terrorism
Nagpal R. – What is Cyber Crime?

Kamini Dashora, P.P. Patel College of Social Sciences, Gujarat, India

Nasik Police play big boss for internet voyeurs, Hindustan Times, Sunday, Oct 28, 2007.
Nowa Pune base for net's cyber cops The Hindu Sunday Nov 26 2006.

Police make headway, The Hindu, Sunday October 29.2006.
Suhas Shetty Cyber Crime Case, First conviction in India under ITA-2000. Tamil Nadu to come out with IT security policy soon, The Hindu,
Saturday, Oct 27, 2007.

Youth in jail for sending email threat, The Hindu Friday August 10, 2007.

Korea Internet and Security Agency, at
http://www.nida.or.kr/kisa/eng/english_ver.html, Last visited: 10/11/2009

The Information and Communication Technology Act-2006, Sec: 68, 82.
21 Ibid, Sec:68(2)
22 Ibid Sec:82(2)(3)
23 Ibid Sec: 69(1)