An Approach of National Cyber Security: Its Awareness and Education

Mrs. Vishakha Mahendrakar
Assistant Professor, Department Of Computer Science and Technology, Navodaya Institute of Technology, Visvesvaraya Technological University –Belagavi
India

Abstract

Cyber-crime is nothing but the crime that is done using computer and internet. Cyber-crime is the fast growing area of crime. Both the computer and the person can be the victim of cyber-crime. Criminals are taking advantage of the fast internet speed and convenience provided by the internet to perform large and different criminal activities. Cyber-crime can be categorized as the crime against individual, property or the government. Cyber-crime can be any crime related to information theft, hacking, virus, Trojan attack, stealing money while transactions etc. As the internet users have increased considerably, so does the cyber-crime. So, it's the duty of one and all that uses internet to be aware of the cyber-crime and the cyber law made to deal with cyber-crimes.In order to reduce the effect of such cyber threats to minimum at the national level, there are necessary critical initiative and special security precautions to be taken. The establishment of the initiative and personal information security which form the stages of launching national information security at highest level and growth of a national security policy are among the first things that need to be done. In this paper, the principles of ensuring cyber security are identified, then public consultation, active cyber defense that are important stages in providing security for national information systems are described. The necessary security tests and the importance of education and awareness are discussed in the following section.

Keyword: *Cyber Crime, Cyber Security, Awareness, Education, Threats, Active Cyber Defense*

I. INTRODUCTION

It is necessary to protect the national information systems at highest level that include personally and organizationally critical information against foreign intelligence or terrorist cyber-attacks. The threats against the national information security are not only on electronic platforms. As a result of natural or undesired events such as human errors, fire, flood, earthquakes, terrorist attacks or sabotage, information and information systems can be partially or completely damaged. Besides unprotecting, the incorrect identification of protection level as well as not taking necessary security precautions brings along other significant problems such as additional cost, low performance or unproductivity.

Nowadays, almost every day, we talk about the security breaches and violations in electronic environments. As a result of one of those security breaches, being a significant example for national information security, "Distributed service denial attacks against the national information systems of Estonia", the public, bank and media internet sites in Estonia having 1.3 million population, have been down and everyday activities were greatly reduced, nearly stopped, due to large scale, coordinated and continuous attacks originated through Russia from hundreds of thousands of computers. This attack has been noted in history as the first cold cyber war between governments.

Any crime that is done using computer and internet is known as cyber-crime or computer crime. Dr. DebaratiHalder and Dr. K Jaishankar defines cyber-crimes as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Both the computer and the person can be the victim of cyber-crime. It just depends on who is the main target. Cyber-crime is done by the persons who are expert in computers and know the technique of hacking. Cyber-crime does not only mean to steal money from someone's account using online transactions, but it can also be information theft, Trojan attacks, e-mail bombing, DOS attack, hacking someone's system, downloading illegal files. Virus is a small program that is sent to different computers using internet which may harm the other systems is also a cyber-crime. The growing problem of cyber-crime is an important issue. The number of internet users has grown tremendously and so does cyber-crimes. The purpose of this paper is to make awareness regarding cyber-crime and cyber law made to avoid the misuse of internet.

The expansion of the Internet beyond computers and mobile phones into other cyber-physical or 'smart' systems is extending the threat of remote exploitation to a whole host of new technologies. Systems and technologies that underpin our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are connected to the Internet and, therefore, potentially vulnerable to interference.

In order to reduce the impact of such cyber threats to minimum at the national level, there are necessary critical enterprise and personal security precautions to be taken. The establishment of the enterprise and personal information security which form the stages of establishing national information security at highest level and development of a national security policy are among the first things that need to be done.

In this paper, national information systems which include strategic national information are explained, personal and enterprise information security that are important stages in providing security for national information systems are described and security tests and the importance of education is discussed in the following sections. Finally, evaluations have been performed on national information security and proposals have been put forward.

II. SCOPE OF THE STUDY

This strategy is intended to shape the Government's policy, while also offering a coherent and compelling vision to share with the public and private sector, civil society, academia and the wider population. In this strategy, 'cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused purposely by the operator of the system, or accidentally, as a result of inadequate to follow security measures. The strategy sets out planned or recommended actions aimed at all sectors of the society and economy, from central government departments, to leaders across industry and the individual citizen. The strategy aims to increase cyber security at all levels for our collective benefit. This includes ongoing and future efforts to protect Government systems, to extend our network of partnerships to help protect critical infrastructure, and to help Canadians to be safe online. In a more varied and dynamic global cyber security landscape, however, new approach will be more wide-ranging and comprehensive.

III. PRINCIPLES OF ENSURING CYBER SECURITY

1. Cyber security is an essential part of national security, it supports the operational of the state and society, the effectiveness of the economy and modernism.

2. Cyber security is definite by respecting fundamental rights and freedoms as well as by protecting individual authorities, personal information, and uniqueness.

3. Cyber security is guaranteed on the basis of the principle of proportionality while taking into account prevailing and impending risks and resources.

4. Cyber security is guaranteed in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing arrangement and facilities in cyberspace.

5. Cyber security starts with individual responsibility for safe use of ICT tools.

6. A top priority in certifying cyber security is anticipating as well as avoiding potential threats and responding effectively to threats that materialize.

7. Cyber security is supported by intensive competitive research and development.

8. Cyber security is certified via international cooperation with associates and partners. Through cooperation, global cyber securityis promoted and enhances its own competence.

IV. PUBLIC CONSULTATION ON CYBER SECURITY

Despite all the technological security precautions taken, the abuse of weaknesses resulting from human factor will lead to information security violations. These violations will cause problems that are critical for national information security. The errors due to human factor that threaten personal information security as well as necessary precautions to be taken are summarized below in subheadings.

A. Violation of Security Policies

Every user who has access rights to the information in information systems need to abide by information security policies. Security policies are violated by end users most of the time intentionally or unintentionally. It is identified that the major reasons for the violation of security policies are user habits, inapplicable sanctions and lack of awareness. In order to avoid security violations, the users need to be trained in information security topics and security policies need to consist of statements that are applicable.

B. Information Exchange

People exchange important information usually unacquainted with unfamiliar persons. No user shall

exchange information with people whose identity is unknown regardless of the means (e-mail, telephone, telefax, face-to-face, etc.). It must never be forgotten that it is possible to breach security controls with the information acquired from an enterprise personnel without any use of technology at all. There are more and more examples each day that little pieces of information that seemed to be insignificant at the beginning, when combined together can turn into a serious security whole. In order to avoid information exchange with unknown persons, it is necessary to train the end users especially in the area of social engineering.

C. Writing passwords on papers

Encryption policies enforce the utilization of passwords that are hard to be broken and the change of these passwords regularly by the users. The encryption power is directly proportional to the complexity of characters that are used in a password. With the application of powerful encryption policies, the problem of remembering those passwords by the users arises. Under this circumstance, in order to be able to remember their passwords, users write their passwords on a paper at their disposal. This situation leads to a security violation of discovery and abuse of the password by another person with malicious intentions. In order to avoid such situations, users need to get trained in selection and recollection of passwords.

D. The utilization of unreliable software

Unreliable software is software that is illegally copied or downloaded from unreliable internet sites without appropriate licenses and can contain viruses, Trojans, key recording and all other kinds of malicious software. Unreliable software keeps the recordings of visited web sites and send this information to others, opens up undesired advertisement popups, can send personal files in computer system to others, reduces the computer performance and exploits internet connectivity. Many security violations take place as a result of utilization of unreliable software. In order to avoid such violations, the users need to get trained in what unreliable software is and how to evade such software.

Establishment of the physical security of computers: When the users leave their computers without taking any protection measure, people with malicious intentions making use of this situation utilize the computer for maleficent purposes and security violations take place. Taking advantage of physical security vulnerability, the person with malicious intentions can email files containing confidential information to other parties, delete or change the information on the computer system and can perform other actions within the user rights of that user. For the establishment of the physical security of computers, it is necessary to raise the awareness of users in this topic; at least the utilization of password protected screen savers must be considered to minimize the risk of such physical attacks to computers.

E. E-mail utilization without awareness

E-mail is one of the most common means of communication among employees. As malicious software spreads usually through e-mails, the utilization of e-mails with awareness has become more important. Inadvertent uses of email cause security violations. It is necessary to raise the awareness of and educate the users about the important precautions that can be taken during the use of e-mails, such as not opening up e-mails from unknown senders, scanning e-mail attachments for viruses, not sharing personal confidential information (internet bank accounts, identity card data, user account information, etc.) via e-mail. As a result of these, the weaknesses due to use of emails will be minimized.

Generally speaking, education has an important role in eliminating the vulnerabilities originating from human factor which is the weakest link in the establishment of information security. The importance of education is examined in detail in the following section.

V. ACTIVE CYBER DEFENCE AND PREVENTING TERRORISM

Active Cyber Defence (ACD) is the principle of executing security measures to brace a network or system to make it stronger against attack. Active Cyber Defence normally refers to cyber security analysts emerging an empatheticway of the threats to their networks, and then developing and implementing measures to proactively secure against those threats. In the context of this strategy, the Government has chosen to apply the same principle on a larger scale: the Government will use its unique expertise, capabilities and influence to bring about a step-change in national cyber security to retort to cyber threats. The activities proposed represent a defensive action plan, drawing on the proficiency of NCSC as the National Technical Authority to respond to cyber threats at a macro level.

In undertaking ACD, the Government aims to:

- Defeat the vast mainstream of high-volume/low-sophistication malware activity on networks by blocking malware communications between hackers and their victims;
- Evolve and increase the scope and scale of Government's capabilities to disrupt serious state sponsored and cyber-criminal threats;
- Secure our internet and telecommunications traffic from hijacking by malicious actors;

- Harden the infrastructure and citizen-facing services against cyber threats; and
- Disrupt the business model of attackers of every type, to demoralize them and to diminish the harm that their attacks can cause.

Preventing Terrorism

The technical capability of terrorists currently remains restricted but they continue to seek to conduct destructive computer network operations, with publicity and interference as the chief objective of their cyber activity. The Government will recognize and disrupt terrorists using and aiming to use cyber for this purpose. In doing so, we will reduce their impact and prevent araise in terrorist cyber competency that would further threaten networks and national security.

To guarantee the threat posed by cyber terrorism remains low, we will:

- Detect cyber terrorism threats, recognizing actors who are seeking to conduct harmful network operations against our allies;
- Scrutinize and interrupt these cyber terrorism actors to prevent them from using cyber competency against the allies; and
- Work closely with international partners to facilitate us to better tackle the threat from cyber terrorism.

VI. AWARENESS AGAINST CYBER CRIME

In order to establish national information security, different methods need to be used to raise awareness of and provide education for different users who can utilize national information systems at different levels. These methods can include creating awareness by holding meetings, organizing trainings over the web and sending notifications, announcements, seminars, newsletters or security related posters via email.

Although the security risk due to human factor cannot be completely eliminated, information security trainings that are well planned can reduce risk to an acceptable level. It is critical in order to minimize security vulnerabilities due to human factor that groups of people with different backgrounds understand their responsibility and fulfill their obligations of protecting information and information resources.

The major objective of information security trainings is to educate people about their obligations and responsibilities necessary for establishing confidentiality, integrity and accessibility of information resources. With these trainings, it is essential to train people not only on how information is protected but also why it is necessary to protect information. Employees must clearly understand the impact of their errors on national information security. Raising the awareness of users will help to reduce the cost impact of security violations and provide a well-balanced control over the complete information resources of the enterprise.

All the persons who use internet today must be aware of the criminal activities taking place on the cyber space. Online transactions have made a large impact on the internet as it has totally changed the old and conventional methods of doing business. The identity of the customer with which you are dealing must be verified to prevent identity theft. Data and information must be protected on your website to protect it from illegal and unauthorized access. For strong relationship between the owner and the customer, the legal issues of online transactions must be addressed from the beginning. Clear information must be provided for doing online transaction. A person should know have the following knowledge to be aware about the cybercrimes-

1. The basics of internet security.
2. The basic information of cyber law.
3. Impact of technology on crime.
4. Minimum hardware and software required to protect data from theft.
5. Internet policies required for working of organization.

VII. EDUCATION TOWARDS CYBER SECURITY

According to users, the enterprise has worked very well up to date without security enforcements and did not encounter any problems. New security enforcements seem to be inconvenient and unnecessary changes. The trainings for creating awareness must be fluent and enjoyable and be prepared to address elimination of old habits along with providing security related information.

The research undertaken within the scope of this paper indicated that there were no security awareness programs in most of the enterprises or the trainings failed to educate users on why information security is important in those enterprises which had these programs. Successful trainings must address the question “why” convincingly for users. A successful training must result in that users own and are willing to apply the security policy. Most of the users are ignorant of the significance of protecting information and information resources. A well designed and performed awareness and education activity will help strengthening the human factor which is the weakest link of the security chain.

After the enterprise and personal information security stages for the establishment of national information security, the education aspect has been emphasized that minimizes the vulnerabilities due to

human factor. In the following section, security tests have been explained as they are necessary to control the applicability of national information security processes.

Finally, within the analyzed cyber-security awareness and education initiatives, there are definite role-players. It is clear that cyber-security awareness is a shared responsibility; and everyone enjoying the cyberspace has a role to play. This is evident, since in all the countries studied, the governments were core in leading and resourcing cyber-security awareness and education. As such, when planning cyber-security awareness and education campaigns and programmers, the role-players should be identified, and their respective responsibilities should be clearly defined. Moreover, partnerships with relevant stakeholders should ideally be formed.

VIII. RESULTS

Losses caused by the attacks against confidentiality, integrity and accessibility of information are serious and cannot be compensated. It is impossible to eliminate all the losses completely. However, it is possible to minimize them by carrying out security tests. It is necessary that the security tests of national information systems are performed according to contemporary national security policy developed by a national authority. State funded centers to perform security tests free of charge must be formed and national software applications for security tests must be developed and used.

When "Your security is as much as your weakest link" principle is considered, in order to eliminate the vulnerabilities due to human factor which is the weakest link in national information security chain, information security education and awareness should be provided at each level of education from the elementary schools to the universities. In order to realize this, a great part of the mission falls especially to non-governmental organizations, Ministry of National Education and universities.

Identification of the cyber-attacks that threaten national security has an important role in development of national strategies in order to establish information security. When the organized attacks against the information systems are examined, it has been identified that the attacks are carried out using advanced techniques and are widespread from personal to national level. In order to establish national information security, the types of attacks need to be monitored, the advanced techniques used by the attackers must be identified, and the security holes described in related research, reports and activities in our country and in the world must be handled and eliminated in time.

Finally, when it is considered that the activities and precautions necessary for establishment of national information security are not sufficient, personal and enterprise level information security awareness and education has not taken place adequately in our society and that the establishment of national information security in our country is not performed at highest level, it is necessary to take the key aspects presented in this paper into account and carry out the proposals.

IX. CONCLUSION

The rapid evolution of the cyber landscape will constantly throw up new challenges as technology evolves and our adversaries act to exploit it. However, this strategy aims to provide a range of policies, tools and capabilities that will ensure we can respond quickly and flexibly to each new challenge as it arises.

Should we fail to act effectively, the threat will continue to outpace our ability to protect ourselves against it. We can expect an explosion of threat capability at all levels.

With the increase in the users of internet, the increase in cybercrimes can also be seen. Hacking is the method in which the criminals get access to the victim's system without their knowledge. Cybercrime can be done mainly by using the technique of hacking. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today's world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc.

Government is also making efforts to have a control on these cybercrimes. Government has made cyber laws to help people learn about the cybercrimesand cyber security. IT Act 2000 is made to deal with the cybercrimes. Both the government and people should work hand in hand to catch the criminals. People who have been the victim of cybercrime should come forward and file a complaint against the crime in special anti-cybercrime cells. Government should also employee officers with very high intelligent quotient and the knowledge about all the cybercrimes. This will help to catch the criminals very easily and all the criminals must be given hard punishments which can a lesson for millions of other cyber criminals. Awareness of the persons using internet will definitely help to curb the cybercrimes and once, all the people are aware of the cybercrime, no criminal would ever think to commit the cybercrime.

REFRENCES

[1] Er.Harpreet Singh, Cyber crime- a threat to persons, property, government and societies,IJARCSSE,997-1002, volume 3, issue 5 May2013, **ISSN: 2277 128X**

[2] Information regarding cyber laws, IT Act 2000 from http://www.cyberlawsindia.net/cyber-india.html

[3] İnternet: "Information Security Awareness" http://www.massachusetts.edu/SecurityAwareness/securityawareness.html (15.05.2009)

[4] Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", FBI Computer Security Institute, 1- 26, (2005).

[5] Mitnick, K. D., Simon, L. W., Wozniak, S., "The Art of Deception: Controlling the Human Element of Security", Wiley Publishing, New York, 17-18 (2003)

[6] Morales, L.; Dark, M., "Information Security Education and Foundational Research", System Sciences, HICSS 2007. 40th Annual Hawaii International Conference, Hawaii, 269 (2007).

[7] Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html

[8] Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" Synthesis Journal, 2(2):5, 8 (2001).