A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India

Priti Saxena, Bina Kotiyal, R H Goudar, and Senior *Member*, *IACSIT*

***Abstract*—Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures. Firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security. As our nation rapidly building its Cyber-Infrastructure, it is equally important that we educate our population to work properly with this infrastructure. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. The valuable aspects for cyber-security are technology, operations and awareness, training and education. This paper focuses issues related to cyber-security in India and presents various methods in bringing awareness at founder levels in educational system.**

***Keywords*—Cyber-infrastructure, social-networking, brain –compatible, cyber–safety, cyber-ethics.**

I. Introduction

Cyber security depends on the care that people take and the decisions they make when they set up, maintain, and use computers and the Internet. Cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means.

Albert Einstein was quoted as saying "Problems cannot be solved with the same level of awareness that created them." The problem of End-User mistakes cannot be solved by adding more technology; it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management.

This paper discusses the following topics. The first section contains the introduction, the second section contains the motivation for our research as the need of cyber-security at all levels, third section contains the issues related to cyber-security, the fourth section, which focuses on the awareness program in the education system is the main core of the paper. This is followed by some of the FAQ's. The concluding section contains a brief summary and suggestions for further research.

Manuscript received February 15, 2012; revised April 18, 2012.

The authors are with Department of CSE, Graphic Era University, India (e-mail: asmi.saxena@gmail.com).

II. Background

Before addressing cyber security needs in the current Indian educational system, we are defining the necessity of cyber security in terms of need of cyber-security in the current Indian security system.

A. Necessity of Cyber Security

Information is the most valuable asset with respect to an individual, corporate sector, state and country.

With respect to an individual the concerned areas are:

1) Protecting unauthorized access, disclosure, modification of the resources of the system.
2) Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
3) Security of accounts while using social-networking sites against hijacking.
4) One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses [1].

With respect to the corporate sector the concerned areas are:

1) Securing the details of the employees.
2) Securing confidential reports at managerial level.
3) Permitted access at various level of the organization.
4) Secured flow of information within and outside the organization.
5) Strong administration level strategies against any disclosure of information.
6) Need of separate unit handling security of the organization.
7) Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness [2].
8) In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered [3].

With respect to state and country

1) Securing the information containing various essential surveys and their reports.
2) Securing the data basis maintaining the details of all the rights of the organizations at state level.

III. Issues And Challenges

Organizational View

1) Ethical issues and legal issues

2) The dependence on computers opened the doors to various kinds of threats.
3) The advancement in technologies supported the intruders or hijackers in the better understanding of the current cyber security methods.
4) Most cyber- crimes are "inside jobs" which means the threats to the information system covers almost 50% of the damage to the information due to the negligence, grievances, communication gaps between security professionals and employees, lower acceptance to the current security system etc.
5) Fortunately or not, the techniques that adversaries can use to cause this sophisticated mischief are often complex and arcane [4].
6) Computer and cyber security issues have become more and more important to the continuity or even to the survival of a business. In the public or private, large or small sectors, finding a qualified security professional for an organization is almost impossible [5].

Education System

1) No separate lesson plans for the cyber security awareness.
2) Teachers are not aware of the current threats in the information technology
3) People are not aware of the reason for the educational course and so do not make any effort to understand or learn the course.
4) It is related to the subject matter and non-interactive learning system.
5) People have the tendency to forget what they learnt about information security if there is not practical implementation.
6) The training and education programs don't consider the present knowledge and experience of their target audience and the problem of "One-size-fits-all" appear [6].
7) The course material is usually not presented in a memorable manner and therefore makes no impression.
8) The complete and comprehensive education of the users in cyber security involves a continuum of three levels of education [7], [8].

Personal Level

1) Use of internet by children in the absence of filters or parental control.
2) Firewalls are not appropriately configured and non-updating of anti-virus.
3) Unawareness of the use of computer with security.
4) The protection of the confidentiality, integrity and availability of information as a vital resource is given appropriate recognition and attention before a problem can occur [9].

IV. Some Elements to Create Awareness in Cyber-Security Educational System

The nature of the Internet as a tool for communication and education has been used and misused for personal gain, which resulted in cyber - attacks and unprecedented rise in cyber - crime rates.

In education system, the children must be made aware of the possible attacks and types of intruders. They should have knowledge about the frauds and scams like phishing, cyber theft and their historic records. They must know about the types of malicious software, their preventive measures etc. Curriculum must also include the advance concepts like the safe use of social networking n mobile devices using GPRS. They must also be aware of the terms like:

1) Hardware/Desktop Security
2) Wi-Fi security, wired security
3) Password Protection/(File/Folder)level security
4) Malicious software:
   - Phishing, Hoaxes
   - Scare ware, Malware, Virus, Worm,
   - Trojans, Zombie and Botnet, Spyware, Adware,
5) Social networking attacks security

Students are acquiring information technology skills marks question on the educators' abilities to ensure that positive habits of on-line behavior are being formed. Whereas, the teacher giving information about security lacks the knowledge and up-to date information related to Cyber awareness issues, particularly with respect to security. Teacher technology training must be provided for skills development and awareness.

A new kind of emerging cybercrime are the Hacktivists. The current record shows least awareness of cyber-crimes at all levels in India. There is an urgent need for introducing courses in various fields. Department of National Security defines cyber security as, "preventing, detecting, and responding to attacks." Indian Education system needs cyber security awareness programs with the increasing use of Indian users in social networking and mobile devices.

A. Additional Class Room Improvement Measures

Class XII, Graduate and Post graduate level students as well as the employees of an organization must be given: Mock test, Case-studies, Virtual environment creation giving the feel of a problematic situation, must be set in order to create more awareness about the current technologies and relevant threat, General awareness websites creation, Power-point slides, FAQ can be implemented in class room teaching.

B. Class Room Conducted FAQ'S Showing the Need of the Awareness

There are some expected questions that the educational security professionals must be aware of:

1) Stealing information through internet is known as: cyber- crime, cyber- theft, phishing?
2) A person reading the confidential content is known as: intruder, hacker, and impersonator?
3) A cyber- crime, which deceives people into giving their banking details, is: phishing, spyware, hacking.
4) Accessing accounting details of an individual and using it for information is known as: impersonation, snooping, spoofing?
5) A computer program automatically installed on your computer, spyware tracks personal information you entered and sends it to its creator. Unlike computer

viruses, this leaves the computer owners totally unaware of its presence: worm, spyware, Trojan horse.

6) What is Adware?
7) Information security is the protection of information and information system. True or False
8) Cyber security deals with the preventive measures for securing information and information system. True or False
9) Virus hit Microsoft and other big companies in 1999, which led them to temporarily terminate their e-mail systems: Melissa
10) Who is Hacktivists?

There is growing evidence of politically motivated attacks over the internet, targeting various organization and companies, from so-called 'Hacktivists'. Hacktivists usually use techniques involving relatively unsophisticated malware but which use the sheer weight of numbers.

11) What is Cyber-safety?

Cyber-safety are steps that one can take to avoid revealing information by "social" means, cyber-safety focuses on acting safely and responsibly.

12) What is "Software loopholes"?

These are the weak links which provides entry points to the intruders into the system.

13) What is the difference between a Virus and a Hacker?
14) What is the difference between a Hacker and a Cracker?

A hacker is a person who is proficient with computers and/or programming to an elite level where they know all of the inn's and out's of a system. There is no illegality involved with being a hacker. A cracker is a hacker who uses their proficiency for personal gains outside of the law. Ex: stealing data, changing bank accounts, distributing viruses etc.

15) What are Malware, Worms, and Trojan Horses?

These spread by email, instant messaging, malicious websites, and infected non-malicious websites. Some websites will automatically download the malware without the user's knowledge or intervention. This is known as a drive-by download. Other methods require the users to click on a link or button.

16) How an Intruder differs from a Hacker?
17) What are Botnets and Zombies?

A botnet, short for robot network, is an aggregation of compromised computers connected to a central controller. The compromised computers are often referred to as zombies.

18) What is a Scare ware?

Fake security software warnings: this type of scam can be particularly profitable for cyber criminals, many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to protect their system.

19) What should be the fundamental countermeasures for the general public?

The three fundamental countermeasures for defending information and data are technology, operations and awareness, training and education.

20) What is a Hoax?

A deceptive alert disseminated via forwarded email warning users of a computer virus, internet worm, or other security threat which in reality does not exist.

Students with different background are not aware of this basic awareness about cyber security. Hence there is a need for awareness in educational system.

V. Additional Measures to Be Taken at Personal, Organizational, Government Levels

At Organizational Level

1) Technical security controls are strong but must be correctly specified, designed, developed, configured used and maintained. All of which involves human participation.
2) Proper co-ordination of senior management, information security, human resources etc. plays a vital role in ensuring data security of the customers.
3) Advance courses must be planned up in order to create good security professionals.
4) Technology itself cannot ensure the security in the absence of proper processes implemented by permitted users.
5) Informing people about information security risk and controls in a general sense and providing guidance whenever necessary.
6) People must be motivated to implement security policies and behave in a more security conscious manner.
7) Speeding – up the identification and notification of security breaches.
8) "Employees can and should be the last line of defense." Security awareness training can pay off by training users on what they can do to prevent malicious activity and what to do in the event of such activity. Of course security awareness training is not the be-all-end-all, it is a significant layer of security to add to existing security measures (Rothman, 2007) [10].
9) Tools are necessary for organizations to analyze their information systems' security, reliability, and resilience against cyber-attack [11].

General public are considered as a weakest link in securing systems. It can be improved by:-

1) Improving awareness of the need to protect system resources
2) Developing skills and knowledge related to security
3) Building in-depth knowledge as needed to design, implement or operate security programs for organizations and systems.

Awareness techniques should be created and frequently changed knowing the experience and the knowledge of the learners.

At Individual Level

1) Protecting our private identity information in cyber space
2) Disconnect a computer from the internet when not in use
3) Learned to recognized on-line spams and marketing schemes which are often disguised as contests
4) Getting aware of the laws pertaining to the use of network
5) Learning safe chatting and messaging skills
6) Securing data by using hard-to-guess password
7) Installing and updating anti-virus software and regularly downloading security protection updates
8) Backing-up data on computer on regular basis and

Understanding the risk associated with file sharing.

9) Humans must have a correct balance of decision making and delegation to maximize their effectiveness and to acknowledge their legal responsibility for the actions of their automated systems [12].
10) Preventing stranger access to private computer files
11) Individual awareness about all the laws and rights before using any new software

At Government Level

1) Government must participate in funding cyber education and create strong partnerships with local state and regional governments industry and educational institution
2) Government should provide proper laws for cyber-crime and prosecute people who steal digital property or harm others on-line.
3) It must train its citizenry to watch for suspicious events on-line.

VI. Conclusion And Future Work

Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work. The IT industry has been playing catch-up with hackers and cybercriminals for decades. Thus there is a need of cyber –security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals not only in the security sector but also in the every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers. Effective cyber-security policies, best practices must be planned and most-important must be implemented at all levels. In the future the Government role and education systems participation in the cyber security awareness approach will lead to a strongly secured nation.

References

[1] M. R. Stytz and S. B. Banks, "Issues and requirements for cyber-security in network centric warfare," Jun 2004.

[2] Cisco, *Cisco 2009 Annual Security Report: Highlighting Global Security Threats and Trends*, December 4, 2009.

[3] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, "Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels," September 9, 2010.

[4] J. Stamp, V. Urias, and B. Richardson, "Cyber Security Analysis for the Power Grid Using the Virtual Control Systems Environment," Oct 10, 2011.

[5] W. Chookittikul and P. E. Maher, "Effective Real-World Project Collaboration: Strategies from a Cyber Security Degree Program," Jun 16, 2011.

[6] L. J. Hoffman, D. Burley, and C. Toregas "Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce," Nov 1, 2011.

[7] J. D. Tressler and J. B. Ippolito, "P-Based Model Information Technology Security Training Requirements: A Role- and Performance-Based Model," Jan 5, 2011

[8] S. K. Katsikas, "Health care management and information systems security: awareness, training or education?" *International Journal of Medical Informatics*, vol. 60, 2000, pp. 129 - 135.

[9] R. Reid, J. V. Niekerk, and R. V. Solms, "Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0," May 18, 2011.

[10] C. Brodie "SANS Institute Reading Room site," 2009.

[11] B. V. Leeuwen, V. Urias, J. Eldridge, C. Villamarin, and R. Olsberg, "Cyber Security Analysis Testbed: Combining Real, Emulation, And Simulation," Dec 30, 2010.

[12] J. N. Haack, G. A. Fink, W. M. Maiden, A. D. McKinnon, S. J. Templeton, "Ant-Based Cyber Security," *2011 Eighth International Conference on Information Technology: New Generations*

Priti Saxena is currently pursuing M.Tech from Graphic Era University,Dehradun.The area of interests include Network Secturity and cloud computing. She has worked as a lecturer in Graphic Era University for One and half year.

Bina Kotiyal is currently pursuing M.Tech from Graphic Era University,Dehradun.The area of interests include Network Secturity.

Dr. R H Goudar, currently working as an Associate Professor, Dept. of CSE, Graphic Era University, Dehradun. He also worked as Faculty at International Institute of Information Technology, Pune for 4 years and Indian National Satellite Master Control Facility, Hassan, India. His Subjects of Interest include Semantic Web, Network Security and Wireless Sensor Networks.