CYBER SECURITY AWARENESS THROUGH EDUCATION: PROBLEMS AND PROSPECTS

Arpita Banerjee[1] and C. Banerjee[2]

Abstract

The internet has become a critical framework for both public and private sectors and has brought new levels of productivity, convenience, and efficiency. The increasing threats to internet attacks represent how vulnerable the information systems of any organization are. The threats can be intentional or unintentional, targeted or non-targeted, and can originate from a variety of sources, such as intervention of foreign nations in espionage and information warfare, delinquents, hackers, virus content writers, discontented employees and stakeholders working within an organization. Moreover, these groups and individuals have a variety of attacking skills at their disposal, and misuse of cyber security activity has grown more sophisticated, more targeted and more serious. Adopting a secure and enhanced software development process will reduce the number of exploitable faults and weakness in any organization. Further, the governance and management of these security policies and practices are more effective when they are systemic, that is, woven into the culture and fabric of organizational behaviours and actions. The aim of our research paper is to discuss the problems associated with cyber security awareness and further generalize the prospects of cyber security. Our paper will do a comparative study of available problems faced in establishing the awareness of cyber security. Further, it will also analyze the policies made and undertaken by the government.

Introduction

Over the past decade, organizations have sought to become more efficient and productive by adopting information and communication technologies. Many organizations relied heavily on technological innovations for the security of their information system. They deployed new security policies to lock down network resources, by creating a safe boundary for efficient working of business. Besides this, an organization also has a goal of educating end users on the importance of security awareness as it is indeed somewhat like the "holy grail" of security.

When used correctly, these techniques drastically reduce security incidents within the enterprise. Along with the organizations, the educational institutions worldwide also struggled to secure their computers and networks (Saluja). While technology plays a pivotal role in doing so, end user education is vital to secure the system communications. However, as successful and sophisticated these technologies have become, technical methodologies alone are not sufficient to solve security problems for the simple reason that information security isn't merely a technical problem but it is also a social and organizational responsibility.

1. Asst. Prof., Department of Computer Science, St. Xavier's College, Jaipur
2. Sr. Lect. AIIT, Amity University, Jaipur

It is also highly difficult to detect and prevent Internet crimes in widely scattered networking environment. For example, cyber-attacks on the Federal Government alone increased 680% from 2006 to 2011. Also, the breach of the Sony PlayStation network in 2011 resulted in a leak of the private information of over 70 million customers. Incidents like these reinforce the risks that exist in cyberspace and their potential impact in the real world. In this regard Indian government strives towards preventing the cybercrimes by enacting Information Technology Act, 2000.

Education will make ready the cyber security workforce of tomorrow; and can keep today's cyber security professionals at the leading edge of the latest technology and mitigation strategies. The number of cyber security-related educational programs around the world has increased significantly over the past decade. One reason for this progress is the very strong demand from industry and government for trained professionals as both groups are facing a significant skills gap. In fact, over half of industry respondents in a current survey said that they had very few information security workers on staff.

Many universities are recognizing the need to produce graduates well-versed in information technology and security. There is a rapid growth of degree-granting programs in information technology as the need for security professionals grows in the workplace. Not only this, the National Security Agency promotes the degree-granting certification programs through their National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program. The focus of our paper is mainly identifying the problem which are faced by the IT industry in handling cyber security issues due to lack of proper education about the importance and awareness of cyber security.

Limitation of Previous Work

The defense of cyberspace necessarily involves the forging of effective partnerships between the public organizations and government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The defense of cyberspace has a special feature, i.e., the national territory or space that is being defended by the land, sea and air forces. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

This report argues that government and the private sector give cyber security some priority in their security and risk management plans, and do this jointly. Being a report that is addressed to the security community in the widest sense and intended to stimulate public discussion, it relies on publicly available information.

One of the first decisions that will need to be made before any organization or institution is the actual deployment of any security awareness project and who will undertake this task of developing and delivering the training. Specifically, will it be developed and delivered by internal company personnel (and if so, will it be done by the IT department, the HR department, or someone else?) or will the organization contact with any educational institution that impart such training. If it is developed by the organization itself then time to develop and cost are the basic two factors to be considered. Instructors often expend as many or more hours outside the classroom. What is the hourly value of the time at the pay grade of the employees who will be doing this extra work?

Going with any educational institution may allow the organization to benefit from economies of scale; the curriculum will likely already be developed and in place and the development costs are spread among many

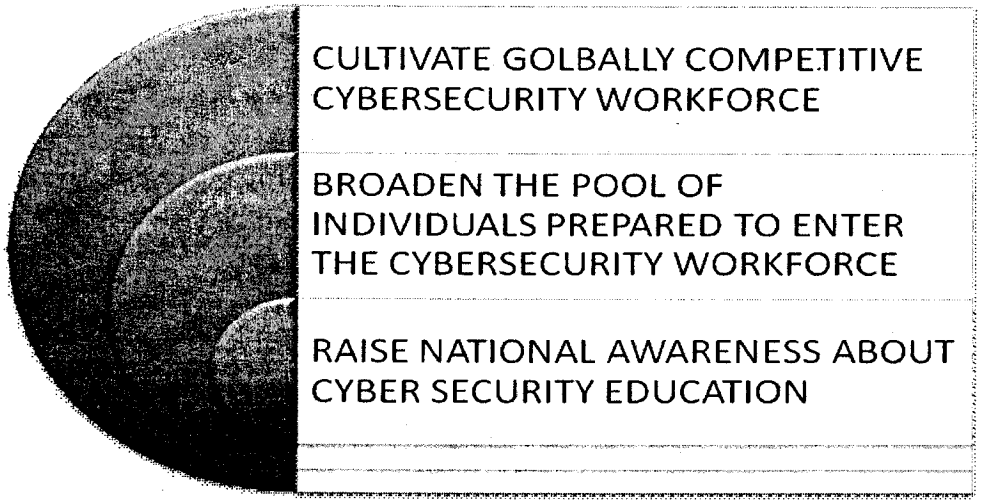
employees. This also means that the organization will probably be able to put the training program in place much more quickly. However, it may also mean that the training is more of a "canned" package that's not specifically tailored to the organization and the individuals who work there.

It is important to think not only as to which department but also as to who in that department will undergo the training. Some people are very knowledgeable about a topic but are not good at conveying that knowledge to others, so ensure you have staff members who are experienced and competent teachers. This can be a stumbling block for any organization with limited personnel resources to draw on. Even if qualified instructors are assigned the job, do they have the time to devote to this effort along with whatever other duties they may have? An instructor who is overloaded and/or just doesn't want to be there is almost worse than inexperienced and untrained one. Several other issues are also there which are not yet clarified, like the inability to map cyber security issues learnt online to actual issues in the real-life job. Managing people is part of good cyber security; but handling them correctly is difficult.

Proposed Architechture

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cybercrime being in billions of dollars worldwide. This paper proposes an architecture that will function with the help and coordination of government and educational institutions. Education plays a very important and vital role in preparing today's workforce to face upcoming challenges, but at the same time cybercrime is becoming an upcoming and important challenge faced by the internet users.

This architecture, if properly implemented by the organization and the educational institution, can help in minimizing the cyber-criminal activities to a wide extent.



Figure–1. Architecture of Cyber Security Awareness through Education

Awareness about the internet is extending through the education sector though there is still illiteracy of cyber education related to security. A large number of youth are getting exposed to the latest technology. The exposure is making the youth to become technology savvy and as such they are using the internet for a variety of tasks, though this also puts them at risk. Among the youths in the range of 13-14 years old many are frequent online surfers and most often these children have very little education at schools pertaining to

the right conduct in cyberspace. The students are not given the crucial guidelines of the internet and how to stay safe while surfing it. The same age group is constantly exposed to increasing dangers on the net. 15% of online surfers reported online harassment, 33% reported interaction with unknown people and 18% reported cyber maltreatment but none of these children knew where to go for help or what to do. Currently, none of the education boards in India have any form of cyber safety education until the 11th grade while the majority of youth internet users comprises 9th graders unknowingly putting themselves at risk.

A change is needed in the global scenario to cultivate well-secured educational society which will curtail the cyber security crimes on private and public sector in their earlier stages of development.

The central and state governments need to take a stand regarding the cyber security awareness through institutions, colleges, schools, etc. Educational sectors act as the pillars to cultivate globally competitive cyber security workforce among the virtual world.

Conclusion

Internet access is gaining pace in the information society. It also allows the criminals to commit crimes in the virtual environment. Cybercrime is emerging as a serious threat. The governments, police departments and intelligence units have started to react to prevent this crime. Initiatives have been taken by the government departments to prevent the cybercrime and raise awareness. For this, various cyber cells in the metropolitan cities of India have been established. They are actively involved in educating the people. Present day academic libraries along with the public libraries need to be conscious in this regard. Sources of the cybercrimes should be known and this information should be transferred to the public especially the students and teachers who spent huge amount of time over the Internet.

Works Cited

Bamrara, Atul. "The Challenge of Cyber Crime in India : The Role of Government." *Pakistan Journal of Criminology.* 3.3 (2013): 127-134.

Connolly, Chris. "An Overview of International Cyber-security Awareness Raising and Educational Initiatives." *Research Report : Australian Communications and Media Authority* 2011.

"Cyber Laws in India and Technology Laws and Regulations in India" 2014.

Cyber Threats <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>

Dark et al., "Integrating Information Assurance and Security into IT Education : A Look at the Model Curriculum and Emerging Practice." *Journal of Information Technology Education.* 5 (2006): 389-403.

Kumar, Vinay D. "Cyber Crime Prevention and Role of Libraries." *International Journal of Information Dissemination and Technology.* 3.3 (2013): 222-224.

Rowe, Dale C. "The Role of Cyber-Security in Information Technology Education." D.O.W., D.O.R. 2011. <dl.acm.org/citation.cfm?id=2047628l>

Saluja, Samridh "Cyber Safety Education in High Schools." *International Proceedings of Computer Science and Information Technology.* 47 (2012): 107-112.

Sony, Tallies "$171M in Data Breach Losses... and Counting." 2011. <http://www.ecommercetimes .com/story/72520.html#sthash.4mbhi7ki.dpuf.>

Tengku, Mohd T. Sembok, "Ethics of Information Communication Technology." (ICT) University Kebangsaan Malaysia for the Regional Meeting on Ethics of Science and Technology. (2003): 5-7, Bangkok.

"The Comprehensive National Cyber Security Initiative" 2014.