Chapter 3
The Different Aspects of Information Security Education

Suchinthi Fernando
Rutgers University, USA

ABSTRACT

This chapter discusses the importance of information security education for everyone, ranging from organizations to professionals and students, all the way through to individual users of information and communication systems. It discusses the different subject areas in information security and shows how instead of being intimidated by it, different categories of users can obtain varying depths of information security education based on their cyber-activities and need for knowledge. Information security professionals would require an in-depth knowledge in all aspects of information security, and information technology professionals and students would require an overall education in these areas, while most users of information and communication systems would only require a basic education to help protect their information assets in cyberspace.

INTRODUCTION

Information is power. All important decisions, whether personal or corporate decisions, short-term or strategic long-term decisions, are made based on information available at a given time. The importance of acquiring and managing up-to-the-minute and accurate information has become more and more important in this digital era leading up to the fourth industrial revolution, where information technology prevails over all other types of technology. Managing information entails not only maintaining the integrity of the information, but also preserving its confidentiality to gain that much required edge over competitors, or ensuring that the privacy of any groups or individuals is not violated. As important as it is to obtain the latest information in order to gain that competitive advantage, it is even more important to ensure that that information does not fall into the wrong hands, since the damage caused by an information security breach, both financially as well as to the reputation of an organisation or any individual, could be phenomenal. As the race for acquiring information gets heated leading to all out cyber warfare, the difficulty of managing information also increases exponentially.

Cyber-security has become a focal point of most organisations, where they strive to provide information security and assurance by creating more resilient structures and systems to keep the never-ending, ever-increasing threats and attacks at bay. Where they previously used to focus only on other aspects of information technology, such as faster networks with higher bandwidths, higher processing speed and power, timely and cost effective software delivery, etc., information technology now revolves around information security, where secure networks, stronger encryption protocols, stronger and more robust systems, secure software development, etc. have taken the centre stage. The software and information industry has finally come to the realization that information security is not something that can be plugged in at the end, but is, in fact, an integral component of information technology that needs to be considered and planned for from the start, incorporated into the design of systems and software, and where the implementation of software systems should be carried out around the established information security standards and procedures. Thus, information security is now finally acknowledged as a journey and not simply as an end destination. Almost all corporations now incorporate information security at all levels and in all branches of business by setting up the required perimeter, hardware and software security systems in place and laying out information security policies and procedures.

The weakest link in all these security measures, however, is the users of these information systems. No matter how strong the technological security measures are, or how well conceived the security policies, procedures and protocols are, if these policies, procedures and protocols are not properly administered or followed, therein lies the biggest vulnerability of any system. The human aspect of information security is the leading cause of information security breaches, and is the component that is most commonly and easily exploited, whether it is in the form of intrusions from the outside or insider threats. This stands true whether it is a corporation, a government, or an individual – the weakest component in an information system is its users. The only way to guard against this is to ensure that information users are properly educated and made aware in the ways of securing information, and thereby, securing their lives.

Living in this digitized age, using all kinds of communication devices which allow people to access and share information in a multitude of ways, without at least a basic awareness of information security is analogous to being in the driver's seat in a car on a busy highway without knowing how to drive. This does not mean that one must shy away from all technology and not be socially active in this digital world. As extensive as the subject of information security is, the fear of not being able to acquire all that knowledge should not deter people from using the technology available to them. Instead, they should gear themselves up by learning what they need to learn about information security, so they may be ready to function in this digital era without having to face major threats.

Information security covers a vast range of subject areas, but not each user needs to be thoroughly educated in each of these different areas. Based on what their job entails and the level of engagement they have with the information, and the criticality of the information they deal with, their information security education can be catered to suit each user role accordingly. Some users might require in-depth knowledge of certain areas, while needing only a basic understanding in others, whereas other users might need only basic awareness overall, and others need an all-round detailed understanding. Regardless of a user's job within a certain organisation, all individual users of information and communication systems should also be cognizant in information security so they may know how to protect their privacy and not put their lives at risk. The mission of this chapter is to discuss the importance of information security education, the different aspects of such an education, and the varying depths and levels of information security education and awareness required by different types of users based on their user roles within an

Related Content

Closing the Gap Between Students' Career Readiness and Employers' Expectations: An Innovative Competency-Based Approach

Jennifer L. Doherty-Restrepo, Katherine Perez, Michael Creeden, Bridgette Cramand McLudmer Charite (2023). *International Journal of Innovative Teaching and Learning in Higher Education (pp. 1-14).*

www.irma-international.org/article/closing-the-gap-between-students-career-readiness-and-employers-expectations/327348

Teaching Normatively: An Approach for Integrating Mission Values Across the Business Curriculum

Brian K. Steversonand Adriane D. Leithauser (2019). *Mission-Driven Approaches in Modern Business Education (pp. 1-19).*

www.irma-international.org/chapter/teaching-normatively/208246

The Anti-Syllabus as a Culturally Responsive-Sustaining Approach to Online Instruction

Taryrn T. C. Brown, Lindsey Chapman, Tara Mathienand Vivian Gonsalves (2025). *Developing Culturally Responsive Curriculum in Higher Education (pp. 121-138).*

www.irma-international.org/chapter/the-anti-syllabus-as-a-culturally-responsive-sustaining-approach-to-online-instruction/383621

Degree Attainment in Online Learning Programs: A Study Using National Longitudinal Data

Heather Carter, Credence Baker, Kim Rynearsonand Juanita M. Reyes (2020). *International Journal of Innovative Teaching and Learning in Higher Education (pp. 19-43).*

www.irma-international.org/article/degree-attainment-in-online-learning-programs/265505

Metacognition of Organization Members as the Basis of Learning Strategy in Higher School

Irina Sergeyevna Yakimanskaya, Anna Mikhaylovna Molokostovaand Milyausha Yakubovna Ibragimova (2017). *Metacognition and Successful Learning Strategies in Higher Education (pp. 114-131).*

www.irma-international.org/chapter/metacognition-of-organization-members-as-the-basis-of-learning-strategy-in-higher-school/175782