Information Security Awareness at Saudi Arabians’ Organizations: An Information Technology Employee’s Perspective

Zakarya A. Alzamil, King Saud University, Saudi Arabia

ABSTRACT

Information security awareness is human and organizational attitudes which can be described as a behavior or an attitude of an organization and/or its members towards protecting the organization’s information assets. The goal of this paper is to understand the state of the information security awareness at some of the Saudi Arabians’ organizations, i.e., governments and privates by investigating the perception of their information technology’s employees. The author believes that understanding the state of information security awareness of IT employees can give a better understanding of the level of awareness at the entire organization. The results of this study show that most of the IT employees at the surveyed organizations have some misconceptions about information security practices. In addition, many responses indicated that many IT employees are not aware of the internal information security threats. Such results required very urgent actions from the top management of these organizations to consider the information security awareness programs within their public relations and training programs.

INTRODUCTION

Human behaviors and attitudes come as a central factor in security, whether for computer, or a broader for information. When an attack is launched, the computer is used as an object or subject for such attack which is carried by a human. Personal computers and handheld devices are used almost by every person and hacking tools are available on the Internet to everyone whether as a computer expert or novice computer’s user which expands the information security threats. Information System is a set of software, hardware, data, people, and procedures that enable us to use information as a resource in the organization. Protecting information requires integrating four basic components into the process of building an information security model, which consists

DOI: 10.4018/jisp.2012070102
of policy, awareness, training/education, and technology (Wilson & Hash, 2003).

According to the 2010 annual report of the Saudi Communication and Information Technology Commission -CITC-, the 2010 has witnessed a significant growth of broadband penetration in the Kingdom with an average cumulative annual growth rate of about 123% per year during the past five years. In addition, the number of Internet users grew from around 1 million in 2001 to an estimated 11.4 million at the end of 2010; which corresponds to an average cumulative annual growth rate of around 31% over the ten year period 2001-2010. Internet penetration increased to 41% of the population by the end of 2010 (CITC, 2010). Such growth impacts the information security of the public and private organizations in Saudi Arabia.

Due to the importance of training for increasing the information security awareness, the National Institute of Standards and Technology -NIST, a USA based agency- has developed a security education, training and awareness program -SETA-, which is a control measure designed to reduce the internal incidences of accidental security breaches by employees. SETA aims to enhance security by improving awareness of the need to protect system resources, developing skills and knowledge so computer users can perform their jobs more securely, and building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. The most important part of the SETA structure is security awareness program because it concerns all the employees of any organization; however, it is the least frequently implemented program. Figure 1 shows the structure of the SETA programs (Wilson & Hash, 2003). This structure is also, supported by a security assessment model proposed by Ang and others (Ang et al., 2007) in which eight constructs are presented, i.e., technology, finance, strategy, policy, culture, accessibility, confidentiality, vulnerability. As indicated in Figure 1, security awareness program is point of entry for all employees into the progression of IT security knowledge levels, and is aimed to keep information security at the forefront of the users’ minds at their work day-to-day to care about security. Keeping the goal of the information security awareness programs, such programs may be simple like promotional trinkets with motivational slogans, videotapes, emails, lectures, and posters or flyers etc.; however, these programs should be implemented efficiently to reduce the possible internal security accidents or failures.

Figure 1. The IT security learning continuum (adapted from Wilson & Hash, 2003)
Privacy and Security in the Age of Electronic Customer Relationship Management
www.igi-global.com/article/privacy-security-age-electronic-customer/2457?camid=4v1a

A Self-Supervised Approach to Comment Spam Detection Based on Content Analysis
A. Bhattarai and D. Dasgupta (2013). *Privacy Solutions and Security Frameworks in Information Protection* (pp. 15-34).
www.igi-global.com/chapter/self-supervised-approach-comment-spam/72735?camid=4v1a