Chapter 4

Establishing a Personalized Information Security Culture

Shuhaili Talib
University of Plymouth, UK & International Islamic University, Malaysia

Nathan L. Clarke
University of Plymouth, UK & Edith Cowan University, Australia

Steven M. Furnell
University of Plymouth, UK & Edith Cowan University, Australia

ABSTRACT

Good security cannot be achieved through technical means alone and a solid understanding of the issues and how to protect one’s self is required from users. Whilst many initiatives, programs and strategies have been proposed to improve the level of information security awareness, most have been directed at organizations. Given people’s use of technology is primarily focused between the workplace and home; this paper seeks to understand the knowledge and practice relationship between these environments. Through a developed survey, it was identified that the majority of the learning about information security occurred in the workplace, where clear motivations, such as legislation and regulation, existed. Results found that users were more than willing to engage with such awareness raising initiatives. From a comparison of practice between work and home environments, it was found that this knowledge and practice obtained at the workplace was transferred to the home environment. Given this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organizational awareness programs and to move towards awareness raising strategies that will develop an all-round individual security culture for users independent of the environment they are operating in.

DOI: 10.4018/978-1-4666-2163-3.ch004
INTRODUCTION

The volume and nature of information security threats has evolved, moving away from technical savvy hackers demonstrating their skill, to organized and well established crackers that aim to receive substantial financial rewards for their efforts (Hinde, 2004). This has resulted in an increase in cybercrime activities and subsequent threats end-users find themselves the target of. For example, in the Computer Security Institute (CSI) survey report stated that 52% of organizations had encountered threats in 2007 (Richardson, 2007). Another survey conducted by Harris on behalf of Microsoft and the National Cyber Security Alliance (NCSA) found that 64% of respondents had encountered a Phishing email – a threat rarely encountered 5 years ago (Harris Interactive, 2009).

To safeguard users a range of security countermeasures exist. These tools continually evolve in sophistication and increase in number to counter the changing nature of the threats. However, in order for these to operate successfully they inherently rely upon the end-user to be able to deploy, configure and operate them. Unfortunately, it is also a well recognized fact that security is only as strong as the weakest link; and the weakest link is frequently the end-user (Schneier, 2000).

To counter the threat caused by end-users an increased focus has been given towards information security awareness and the need to educate and inform end-users. Within an organizational context, efforts towards improving awareness amongst employees have increased with CSI survey indicating 82% of Enterprise organizations having training programs (Richardson, 2008). Unfortunately, however, this is not necessarily the case for all, with Business Enterprise Regulatory Reform (BERR) Information Security Breach Survey, which largely comprises of small-to-medium sized companies (SMEs), indicating only 40% of their respondents conduct training (Business Enterprise Regulatory Reform, 2008). Whilst many organizations arguably have the resources to provide such training, should they deem it important to do so, they only represent a (95%) proportion of people who use the Internet. The remaining users are typically home-users or the general public. Worryingly, evidence demonstrate that it is this group of users that are most at risk, with 95% of all attacks being focused upon them (Symantec, 2007). Home users have a variety of resources at their disposal in order to improve their awareness of online threats. All the major Anti-Virus providers, Operating System vendors and government initiatives provide supporting information to the home user (GetSafeOnline, 2009; StaySafeOnline, 2009; WebWise, 2009).

Whilst training programs and initiatives exist within both the workplace and home, little research has been conducted to understand what is being taught and where, the effectiveness of such strategies and to what degree learning styles play a role in achieving good information security practice. Information security awareness can be tackled from a variety of different directions, such as within school, government-sponsored initiatives and security providers; however, this paper will specifically focus upon and investigate behavior, practices and interactions within and between organizations and home environments. The paper is organized as follows: the next section discusses the current state-of-the-art information security awareness and the development of security culture. Next, the methodology of the study is described followed by the presentation of results. Then, main findings of the study are presented along with the conclusion and possible future areas of exploration.

PRIOR WORK IN INFORMATION SECURITY AWARENESS TRAINING

Information security awareness has been given an increasingly important focus within both academic and commercial communities. Organizations are gradually understanding the importance of their