ABSTRACT

Information systems administrators face a difficult balance between providing sufficient security to protect the organization's computing resources while not inhibiting the appropriate use of these resources. Striking this balance is particularly difficult in higher education due to the diversity of computer uses and users. This is accentuated by one large, diverse user group, namely students. To facilitate striking such a balance, a better understanding of students' motivations to use security measures is useful. A theoretically sound model linking student and system security characteristics to students' security behaviors is developed and presented in this paper. The model is operationalized using student responses to a web-based questionnaire. The empirical results show that training to use security measures has no impact on students' security behaviors while experience with security does. Furthermore, ease of security use positively impacts students' security behaviors through security self-efficacy. The influence of peers has similar impacts through security outcome expectancy.

DOI: 10.4018/978-1-4666-0026-3.ch013
INTRODUCTION

Information systems administrators in all organizations face a difficult balance between providing sufficient security to protect the organization’s data and computing resources while not inhibiting the appropriate use of these resources and data. While this balance is difficult in any organization, for information systems administrators in higher education it is particularly difficult to accomplish. In higher education, the uses and users of information systems are very diverse, accentuated by a large, diverse user group, students. It is this challenging environment that is used to examine the factors influencing individuals’ use of computer security.

Students not only use university computing resources for classroom-related activities, they also use these resources for a variety of personal activities. These personal activities make use of a wide range of computing resources. Such diversity of uses and activities makes providing a secure yet usable environment for computing resources very difficult. As a result, the information systems administrator in higher education faces a very difficult environment to provide appropriate security measures protecting data and computing resources while allowing reasonable ease of use of these resources and data.

In order to facilitate striking an appropriate balance between security and ease of information systems use, a better understanding of students’ motivations to use these security measures would be useful. Such insights are of interest for at least two reasons. First, information systems of American universities have been subject to a significant number of security attacks since 2001 (Shroff & Vogel, 2009). These attacks most certainly lead to greater information system security measures being implemented on campuses. Increased information system security inherently affects students since students constitute a major user group of these information systems. Hence, a better understanding of students’ security attitudes and behaviors are important to information system administrators in higher education. Secondly, in a more general organizational context students may serve as a reasonable proxy for the attitudes of employees in general toward security.

These concepts motivate the research that follows. A theoretically sound model linking student and system security characteristics to students’ security behaviors is developed and presented. The model is operationalized using student responses to a web-based questionnaire regarding their knowledge and use of security measures. Based on this data, the operationalized model is tested and the results presented. Using these results, discussion and policy implications for information system administrators in higher education as well as conclusions are offered.

THE THEORETICAL MODEL

The research extends the works of Rounds, Pendegraft, and Stone (2008) and Rounds Pendegraft, Pendegraft, and Stone (2008) by examining the attitudes and behaviors of students toward computer security. A formal model of student security attitudes and behaviors is presented and empirically examined. The theoretical model is grounded in social cognitive theory as pioneered by Bandura (1982, 1986). The application of social cognitive theory has been shown to be meaningful in explaining motivation, behavior, and affective reactions in a variety situations and applications. Among these applications are ones applied to computer and technology adoption and use characteristics. For example, social cognitive theory has been used to study the antecedents of knowledge management systems (Lin & Huang, 2008), computer system use (Stone & Henry, 2001), computer users’ organizational commitment (Stone & Henry, 2003), and computer users’ perceptions of job control and stress (Henry & Stone, 1999). Other studies have used key constructs from social cognitive theory (e.g., self-efficacy and outcome expectancy or perceived...