Decision Support Systems 46 (2009) 815–825

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Studying users' computer security behavior: A health belief perspective

Boon-Yuen Ng *, Atreyi Kankanhalli, Yunjie (Calvin) Xu

Department of Information Systems, National University of Singapore, Singapore

ARTICLE INFO

Available online 21 November 2008

Keywords:
Computer security
Security awareness
Health belief model
Email attachment
Virus

ABSTRACT

The damage due to computer security incidents is motivating organizations to adopt protective mechanisms. While technological controls are necessary, computer security also depends on individual's security behavior. It is thus important to investigate what influences a user to practice computer security. This study uses the Health Belief Model, adapted from the healthcare literature, to study users' computer security behavior. The model was validated using survey data from 134 employees. Results show that perceived susceptibility, perceived benefits, and self-efficacy are determinants of email related security behavior. Perceived severity moderates the effects of perceived benefits, general security orientation, cues to action, and self-efficacy on security behavior.

1. Introduction

Organizations increasingly rely on information systems for the transmission, processing, and storage of information. Hence, it is essential to protect the information within these systems and the availability of the computer systems. However, the increase in organizational dependence on information systems as well as the ease of mounting attacks has led to a corresponding increase in the number of security incidents and damage caused [26]. A computer security incident is defined as a security-related adverse event in which there is a loss of information confidentiality, disruption of information or system integrity, disruption or denial of system availability, or violation of any computer security policies [19]. According to the 2007 annual survey conducted by the Computer Security Institute [36], 46% of respondents indicated that their organization experienced a security incident within the last 12 months. Of these, a significant number (52%) of the attacks are virus-related. It is therefore important for organizations and employees to be aware of and protect themselves against security threats and cybercrime.

Chung et al. [8] described three approaches at a national level to fight against cybercrime, i.e., legal, organizational, and technological. Countries around the world have created laws (e.g., Computer Misuse Act in Britain and Singapore) and set up national agencies (e.g., the Computer Analysis Response Team in the US) to combat computer security threats. Various technologies are applied at the national level for this purpose, such as a computer surveillance system developed by the FBI. Further, organizational measures are important in this fight. Organizations need to develop and implement a multi-dimensional approach to safeguard their information assets [52].

Among the approaches, technological measures such as firewalls for perimeter defense are common in organizations. Such solutions are necessary but not sufficient for protection [35]. This is because success of computer security depends on the effective behavior of users [43]. Employees in an organization play an essential role in the prevention and detection of security incidents. While system administrators are responsible for configuring firewalls and servers in a secure manner, users are responsible for practicing security countermeasures such as choosing and protecting appropriate passwords.

Thus, for effective security, users have to make a conscious decision to comply with the organization's security policies and adopt computer security behavior. To this end, organizations have been implementing security training and awareness programs to educate users [35]. While many practitioner guidelines are available, there is a lack of empirical studies concerning the design and effectiveness of security awareness programs. An effective awareness program should influence a user's attitude and behavior to be more security-conscious [47]. Thus, it is critical to understand what will influence a user's security behavior so that appropriate awareness programs can be designed. However, there is little theoretically grounded empirical information systems research on the behavior of individuals in practicing secure computing.

Motivated by such theoretical and practical concerns, our research question is, "What are the salient influences for a user to practice computer security in an organization?" Through this study, we aim to contribute to the better understanding of security behavior of computer users in organizations, so that the security climate of an organization can be improved. By identifying and understanding the determinants of computer security behaviour, interventions can be designed to change behaviour by directing at one or more of the determinants.

* Corresponding author.
E-mail addresses: ngby@comp.nus.edu.sg (B.-Y. Ng), atreyi@comp.nus.edu.sg (A. Kankanhalli), xuyj@comp.nus.edu.sg (Y.(C.) Xu).

0167-9236/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2008.11.010

With the paucity of theoretical perspectives in this area, this study draws upon relevant literature from other fields. Specifically, it makes use of the well-known health belief model [40] traditionally employed to explain preventive healthcare behavior. This perspective is applicable because security practices can be seen as preventive behavior to avert security incidents. The model suggests that an individual's behavior is determined by the threat perception and evaluation of the behaviour to resolve the threat. This model offers a new perspective to better understand the phenomenon using constructs that have not been previously explored in IS research, such as cues to action and general security orientation. Our research model is tested by surveying 134 employees from multiple organizations. The findings are expected to inform theory and practice in this area.

2. Conceptual background

2.1. Computer security behavior

There are relatively few research studies of security behavior of computer users and how behavior can be modified to practice security countermeasures. Previous studies in this area can be categorized according to their context, i.e., organizational or non-work use of computers. An example of a study in the organizational context is the investigation of end-user security behaviors and their antecedents by Stanton et al. [43]. It reveals relationships between end-user security behavior (such as password management, non-work-related computing behavior, and obtaining security training) and a combination of situational factors (such as organizational type) and personal factors (such as income level and job role). The study provides empirical insights but without theoretical bases. Yet another study in the organizational context by Aytes and Connolly [4] proposes a conceptual model of user security behavior based on risk perception. Of the rare theoretically-grounded empirical studies in this context is the study by Chan et al. [7], which explores the influence of security climate and self-efficacy on user compliance to security policies. Thus there is a lack of studies that comprehensively model and test the individual beliefs that influence computer security behavior in organizations, which is broader than compliance to organizational security policies.

Other related studies pertain to computer users in a non-work environment, which differ from organizational settings by the absence of managerial interventions and controls. For example, the factors that influence a home user's intention to practice computer security have been investigated by applying the decomposed theory of planned behavior [33]. Findings indicate that family, peer, and mass media influence, perceived usefulness, and self-efficacy are important factors that influence a home user's intention to practice computer security. Another empirical study in the non-work context surveyed students to investigate determinants of safe online behavior [29]. It finds significant influences from online safety involvement, self-efficacy, and personal responsibility but without a theoretical explanation. In another study of college students, application of protection motivation theory borrowed from healthcare showed that self-efficacy predicts online consumers' intention to practice safe online behavior, such as updating virus protection [28]. With the lack of theoretically-grounded empirical studies of determinants of computer security behavior in organizations, we now review theories that may be applicable for our study.

2.2. Applicability of IS adoption theories

Information systems (IS) research is rich in theories pertaining to technology adoption. Computer security behavior includes the adoption and use of security technologies such as anti-virus software and firewalls. Theories such as Technology Acceptance Model [14] and Theory of Planned Behavior [3] can be applied to study users' intention to use security technologies (e.g., [33]). However, recent research in security behavior has revealed that there are significant differences between positive technologies (used for designed utilities) and protective technologies (used to prevent negative consequences) [15]. Security technologies generally belong to the category of protective technologies as they are used to avert undesirable incidents, such as virus attacks. This recent discussion gives the impetus to look for theories that are more suitable to study the use of such protective technologies.

In addition, computer security behavior involves more than just the adoption of technology. While the use of protective technologies is critical, computer security behavior also includes other behaviors such as the choice of strong passwords, regular backing up of data, and exercising caution with suspicious email attachments. Such behaviors do not involve the adoption of any specific technology but require the computer user to consciously decide to perform additional steps for the sake of preventing unwanted situations such as loss of data. For

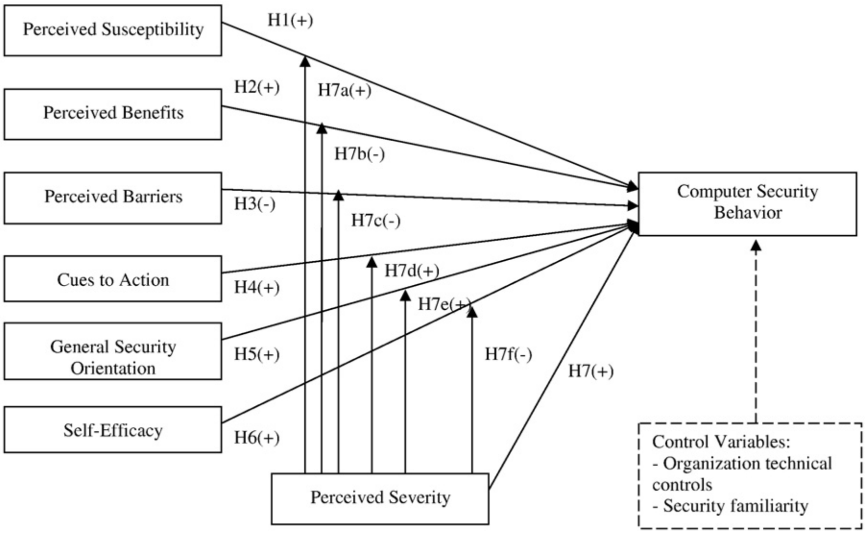

Fig. 1. Research model.