IGI PUBLISHING **ITJ3679**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **International Journal of Information Security and Privacy**, Volume 1, Issue 2
edited by **Hamid Nemati © 2007, IGI Global**

Information Security Effectiveness: Conceptualization and Validation of a Theory*

Kenneth J. Knapp, US Air Force Academy, USA

Thomas E. Marshall, Auburn University,USA

R. Kelly Rainer, Jr., Auburn University, USA

F. Nelson Ford, Auburn University, USA

ABSTRACT

Taking a sequential qualitative-quantitative methodological approach, we propose and test a theoretical model that includes four variables through which top management can positively influence security effectiveness: user training, security culture, policy relevance, and policy enforcement. During the qualitative phase of the study, we generated the model based on textual responses to a series of questions given to a sample of 220 information security practitioners. During the quantitative phase, we analyzed survey data collected from a sample of 740 information security practitioners. After data collection, we analyzed the survey responses using structural equation modeling and found evidence to support the hypothesized model. We also tested an alternative, higher-order factor version of the original model that demonstrated an improved overall fit and general applicability across the various demographics of the sampled data. We then linked the finding of this study to existing top management support literature, general deterrence theory research, and the theoretical notion of the dilemma of the supervisor.

Keywords: *information security; organizational effectiveness, organizational IS; structural equation modeling; survey development; top management support*

INTRODUCTION

With modern national economies dependent upon information technology for survival, the need to protect information and mitigate risk has become paramount. One can find evidence of poor information security in the frequency of media reports about security breaches and from published survey data. As of this writing, media headlines about security incidents have become a regular occurrence, with one of the more embarrassing breaches occurring when a laptop went missing that contained sensitive information of millions of U.S. veterans and military personnel (Files, 2006). Multiple national surveys confirm a high number of attacks against organizational information resources (Bagchi & Udo, 2003; Computer Emergency Response Team (CERT), 2004; Gordon, Loeb, Lucyshyn, & Richardson, 2005). Between 1998 and 2003, the number of reported incidents to the U.S. Computer Emergency Response Team (CERT) has nearly doubled each year with

137,529 reported incidents in 2003 alone.[1] An Ernst and Young analysis found that security incidents can cost companies between $17 and $28 million each occurrence (Garg, Curtis, & Halper, 2003). Because incidents are frequent and costly, management must take security seriously to protect organizational information.

Noting the disappointing state of information systems (IS) security in organizations, Dhillon & Backhouse (2001) called for more empirical research to develop key principles that will help in the management of IS security. Despite the call, few studies have developed and empirically tested theoretical models of IS security (Kotulic & Clark, 2004). In some studies, the sensitive nature of the security topic (Straub & Welke, 1998) impeded the collection of a sufficient sample willing to participate in the research (Kotulic & Clark, 2004). The few empirical studies that contained information security effectiveness as a dependent variable used general deterrence theory as a research foundation (Kankanhalli, Hock-Hai, Bernard, & Kwok-Kee, 2003; Straub, 1990). Sensing that other variables in addition to those related to deterrence theory might significantly predict information security effectiveness, we engaged in a study to develop and empirically test a model of effectiveness that is not based on predetermined independent variables.

Using a sequential quantitative-qualitative methodological approach, we developed and tested a theoretical model that illustrates four practices through which top management can positively influence security effectiveness. The role of management support has been identified as a critical success factor in a wide area of information system implementations and IT projects (Jasperson et al., 2002; Sharma & Yetton, 2003). Management support has been called the variable most frequently hypothesized as contributing to IS success, but empirical analysis has limited modeling "success" as a simple linear function of management support (Sharma & Yetton, 2003, p. 535). Our model offers a more comprehensive view by including four critical mediator variables through which management can improve security effectiveness: user training, security culture, policy relevance, and policy enforcement. By doing so, the theoretical model proposed in this study provides practical help to professionals and researchers who seek to advance the managerial effectiveness of information security programs.

The following methodology section describes our qualitative approach used to conceptualize the theoretical model and the survey instrument to test the model. Using survey data, we then quantitatively test the model using structural equation modeling (SEM). We also proposed and analyzed an alternate structural model. To add credibility to the results of this study, the discussion section links our findings to related theory including previous IS studies based on general deterrence theory. We close our paper with limitations, implications and a conclusion.

RESEARCH METHODOLOGY

Rather than developing a theoretical model based on existing theory in the literature, we used a qualitative strategy that closely followed grounded theory to develop a theoretical model. For this reason, we are going straight into the methodology section. Later in the discussion section, we will appropriately link our findings to theory in the literature. This format is consistent with the grounded theory approach, which aims to discover theory directly from a corpus of data rather than from theory generated by logical deduction based on *a priori* assumptions (Glaser & Strauss, 1967). Using a coding process consistent with developing grounded theory, question responses provided by a sample of information security practitioners are analyzed to identify key issues in IS security. A theoretical model emerges based on the categorical relationships among the key managerial issues identified in the responses. After developing and giving the survey to a sample of information security practitioners, we test the model using structural equation modeling. We then explore an alternative model where the four mediator variables are represented by a higher order factor.