THE TECHNOLOGY ACCEPTANCE MODEL AND THE DECISION TO INVEST IN INFORMATION SECURITY

Alice M. Johnson
North Carolina Agricultural and Technical State University
amjohns1@ncat.edu

Abstract

Security breaches have increasingly become a major threat to organizations. Nevertheless, according to recent reports, many organizations do not plan to increase spending on information security. In fact, little is known about an organization's motivation to invest in information security. This paper uses the Technology Acceptance Model as a basis for studying factors that might motivate organizations to invest (or not to invest) in information security. It proposes that perceived usefulness and ease of use of information security influence such investment decisions. It further proposes that seven other variables influence perceived usefulness and ease of use. They are: external environment, prior information security experiences, perceived risks of not securing information, information security budget, security planning, confidence in information security, and security awareness and training. The research proposes a model of information security investment. A Delphi study and a mail survey will be used to test it.

Keywords: Technology Acceptance Model; Information security; IT decision making

Introduction

Information security refers to any process, activity, or task that protects the confidentiality, integrity, and accessibility of information (NIST 1995). Since the introduction of e-mail and the World Wide Web, information security breaches have increasingly become a major threat to organizations. More than 76,000 such breaches were reported in the first six months of one year. This was only 6,000 less than reported incidences for the entire previous year (Stahl 2003). Nevertheless, many organizations did not plan to increase their spending on information security. Furthermore, firms that suffered the most damages were twice as likely as others to decrease security spending in the future (Berinato 2003).

A paucity amount of empirical research exists to explain an organization's motivation to invest in (or not to invest in) information security. Therefore, the objective of this research is to investigate the factors that influence an organization's information security investment decisions. It thus proposes a model of information security investment.

The current study uses the Technology Acceptance Model (TAM) (Davis 1989) as the theoretical basis for development of an information security investment model. TAM has been used primarily to explain the usage of information technology (Ma and Liu 2004). However, recent research has supported its use for investigating IT decision-making (Benamati and Rajkumar 2002).

Background

Two streams of research can be used to summarize the types of studies that have addressed information security investment. One has used surveys to assess the state of information security in organizations and to indicate the types of security technologies firms tend to use. The other has used empirical studies to provide security professionals and managers with guidance in identifying appropriate information security investments.

Surveys

Most of the studies that have addressed information security investment have been surveys. One such survey, the Computer Crime and Security survey, is the longest running survey in the information security field. Its primary objectives are to demonstrate trends in such areas as the magnitude and types of security breaches, the impact of such breaches on organizations, and the types of technologies organizations invest in to secure their information resources. Recent survey findings reported that 52% of 251 respondents had experienced unauthorized use of their organizations' computing facilities. The total annual losses reported for those respondents was $201,797,340. Theft of proprietary information was the greatest loss of $70,195,900, while the average reported loss was $2.7 million. Virtually all organizations had invested in anti-virus software and firewalls. Approximately 70% used file encryption (CSI/FBI 2003). .

A second survey of 7,600 respondents suggested that society, in general, was just beginning to accept information security as an ongoing discipline. Furthermore, it showed that firms did not readily allocate resources to protect stored data. Although such data is more vulnerable and is thus attacked more frequently (Swartz 2004), only 30% of the organizations encrypted it (Berinato 2003). Instead, organizations allocated more resources to the encryption of data in transit.

A third and final survey of 56 financial institutions found that 59% of the organizations rarely or never calculated return on investment for information security expenditures (Schneider 2003). Failure to perform such calculations could adversely affect an organization's ability to receive proper funding for information security (Piazza 2003; Vijayan 2003).

Empirical Studies

Most of the empirical studies have typically presented models or methods for ultimately determining information security investments. For example, investment in security risk planning (Straub and Welke 1998) and security awareness training/education (Straub and Welke 1998; Whitman 2003) has been identified as areas where organizations could allocate resources to protect or secure corporate information. More specifically, effective information security requires that organizations maintain a security policy that properly identifies threats to information and then apply controls to address such threats (Whitman 2003).

The Policy Framework for Interpreting Risk in E-Business Security, referred to as PFIRES (Rees et al. 2003), has suggested that security strategy and policy could be created and maintained in line with the standard information technology life cycle. The PFIRES life cycle consisted of four major phases: assess, plan, deliver, and operate.

Theoretical Development: TAM

TAM posits that perceived ease of use and perceived usefulness predicts attitude toward use of a technology. Then, attitude toward use predicts the behavioral intention to use. Finally, intention predicts the actual use of that technology (Davis 1989). A variety of applications have been used to validate the model (Ma and Liu 2004). For example, it was employed to study user acceptance of microcomputers (Igbaria et al. 1989), the World Wide Web (Lederer et al. 2000), software, and decision support systems (Morris and Dillon 1997).

In addition to the relationships proposed by TAM, many researchers have studied the antecedents of perceived usefulness and perceived ease of use (Agarwal and Prasad 1999; Dishaw and Strong 1999; Lederer et al. 2000; Straub et al. 1995). Some have also ignored attitude toward use and/or intention to use (Adams et al. 1992; Gefen and Straub 1997; Igbaria et al. 1995), and instead focused on the direct effect of ease of use and usefulness on system usage. Others have suggested that TAM could be used for areas other than end-user and software acceptance (e.g., Agarwal et al. 2000; Hu et al. 1999). For example, Benamati and Rajkumar (2002) applied TAM to technology-related decision-making. They employed a qualitative methodology to investigate the predictive capability of TAM for studying application development outsourcing decisions. Ten executives from seven companies were interviewed to determine their outsourcing decision-making process. The results suggested that perceived usefulness and ease of use of outsourcing mediated the effects of the external environment, prior outsourcing relationships, and risks on organizations' outsourcing decision-making.

Following Benamati and Rajkumar (2002), the current study applies TAM to information security investment decision-making and acceptance. Figure 1 illustrates the conceptual model, which is based on research about TAM, information security investment, and decision-making. It proposes the study of (1) the influence of a set of external variables on the perceived usefulness of information security and the perceived ease of use of information security and (2) the influence of the perceived usefulness of information security and the perceived ease of use of information security on actual investment in information security.

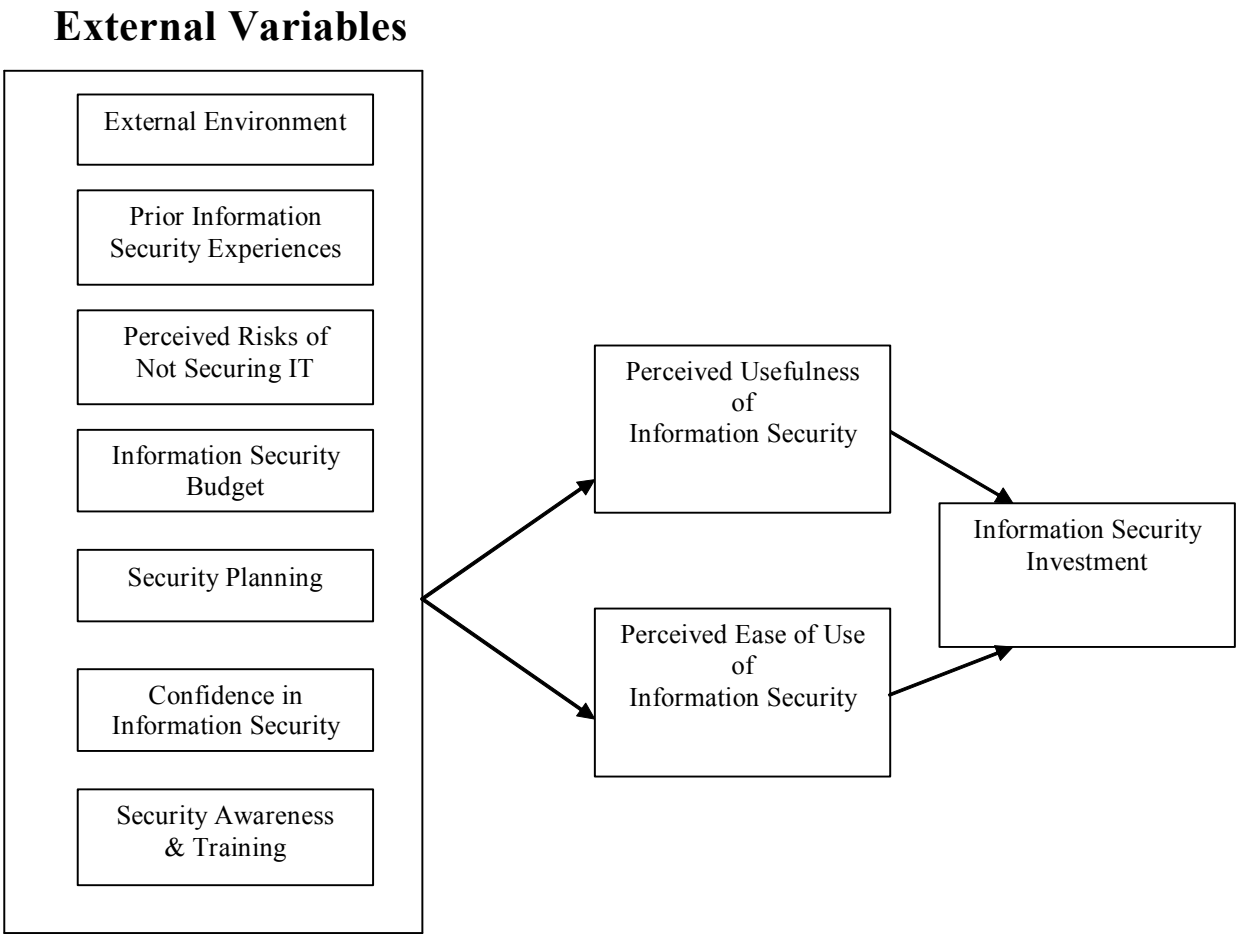

Figure 1. Conceptual Research Model

Similar to previous research, the model shown in Figure 1 omitted the attitude toward use and the intention to use variables (Adams et al. 1992, Gefen and Straub 1997, Lederer et al. 2000). Such omissions will result in a more parsimonious instrument and will permit a more concentrated study of the antecedents of ease of use and usfulness.

Methodology

The model shown in Figure 1 is based on prior research about TAM, information security investment, and decision-making. A Delphi study is currently being conducted with IT and business executives. The purpose of it is to identify all factors that could potentially influence information security investment (i.e., factors that are not included in the current research model).

Subsequent to the Delphi study, an instrument will be developed to test the model. A survey will be mailed to a random sample of 1000 IT and business executives. The survey instrument will be validated in accordance with the methods prescribed by Churchill (1979) and Gefen et al. (2000). Structural equation modeling will be used to test the proposed relationships.

Expected Benefits

A number of benefits and contributions are expected. Support for the research model would confirm that TAM is a useful framework for studying IT decision-making. Previous research had supported this type of application. However, it used a qualitative methodology. The current study proposes to use a large sample. Moreover, the research would support the applicability of TAM for making decisions specifically about information security investment. Such contributions might provide a basis for further research.

The results of the study would also help practitioners to understand the complexities involved in allocating resources to information security. It might also provide guidance to managers in their efforts to justify and receive funding for information security.

References

Adams, D. A., Nelson, R. R., and Todd, P. A. (1992) Perceived usefulness, ease of use, and usage of information technology: a replication. *MIS Quarterly*, 16(2), 227-247.

Agarwal, R., and Prasad, J. (1999) Are individual differences germane to the acceptance of new information technologies? *Decision Sciences*, 30(2), 361-392.

Agarwal, R., De, P, Sinha, A., and Tanniru, M. (2000) On the usability of OO representations. *Communications of the ACM*, 42(10), 83-89.

Benamati, J. and Rajkumar, T. M. (2002) The application development outsourcing decision: an application of the technology acceptation model. *Journal of Computer Information Systems*, 42(4), 35-43.

Berinato, S. (2003) The state of information security 2003. *CIO*, 17, 2, 1-3.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 16, 64-73.

CSI/FBI. (2003) *Computer Crime and Security Survey*, Retrieved February 2, 2004, from http://ww.gocsi.com.

Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13, 319-339.

Dishaw, M. T. and Strong, D. M. (1999) Extending the technology acceptance model with task-technology fit constructs. *Information & Management*, 36(1), 9-21.

Gefen, D, and Straub, D. W. (1997) Gender differences in the perception and use of e-mail: an extension to the technology acceptance model. *MIS Quarterly*, 21(4), 389-400.

Gefen, D, Straub, D. W., and Boudreau, M. (2000) Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information Systems*, 4(7), 1-78.

Hu, P. J., Chau, P, Y, K., Liu Sheng, O. R., Yan Tam, K. (1999) Examining the technology acceptance model using physician acceptance of telemedicine technology. Journal of Management Information Systems, 16(2), 91-112.

Igbaria, M., Guimaraes, T., and Davis, G. B. (1995) Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems*, 11(4), 87-14.

Lederer, A. L., Maupin, D. J., Sens, M. P., and Zhuang, Y. (2000) The technology acceptance model and the World Wide Web. *Decision Support Systems*, 29, 269-282.

Ma, Q and Liu, L. (2004) The technology acceptance model: a meta-analysis of empirical findings. Journal of Organizational and End User Computing, 16(1), 59-74.

Morris, M. G., and Dillon, A. (1997) How user perceptions influence software use, decision support systems. *IEEE Software*, July-August, 58-65.

NIST (National Institute of Technical Standards). (1995) *An introduction to computer security: the NIST handbook*, Special Publication 800-12.

Piazza, P. (2003) Budget suffers without ROI calculations. *Security Management*, 47(11), 34.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. (2003) PFIRES: A policy framework for information security. *Communications of the ACM*, 46(7), 101-106.

Schneider, I. (2003) Information Security: Room for Improvement. Bank Systems and Technology, November, 16.

Stahl, S. (2003) Security needs to become IT basic. *InformationWeek*, July 28, 949, 6.

Straub, D. W., Limayem, M., and Karahanna-Evaristo, E. (1995) Measuring system usage: implications for IS theory testing. *Management Science*, 41(8), 186-204.

Straub, D. W., and Welke, R. J. (1998) Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Swartz, N. (2004) Survey assesses the state of information security worldwide. *Information Management Journal*, 38(1), 16.

Vijayan, J. (2003) IT security short on funding. *Computerworld*, 37(29), 1.

Whitman, M. E. (2003) Enemy at the gate: threats to information security. *Communications of the ACM*, 46(8), 91-95.