December 2007

The IT Security Adoption Conundrum: An Initial Step Toward Validation of Applicable Measures

Merrill Warkentin
Mississippi State University

Jordan Shropshire
Mississippi State University

Allen Johnston
University of Alabama Birmingham

THE IT SECURITY ADOPTION CONUNDRUM: AN INITIAL STEP TOWARD VALIDATION OF APPLICABLE MEASURES

Merrill Warkentin, Mississippi State University, mwarkentin@acm.org

Jordan Shropshire, Mississippi State University, jds372@msstate.edu

Allen C. Johnston, Univ. of Alabama Birmingham, allencjohnston@gmail.com

Abstract

Within information systems research, technology adoption is one of the most widely investigated and accepted research streams. Since its inception nearly two decades ago, conceptual models of the individual adoption decision, such as the Technology Acceptance Model (Davis 1989) and the Unified Theory of Acceptance and Use of Technology (Venkatesh et al. 2003), have been used in a variety of circumstances with sustained success. However, recent findings suggest constructs borrowed from technology adoption literature are less applicable in the case of security adoption (Warkentin et al. 2004). Unfortunately, there has been little empirical evidence available to substantiate or refute this claim. In an attempt to address this void, the authors have undertaken a multi-phase research approach in which a representative sample of current IT adoption constructs are assessed as to their applicability within the IT security context. Consistent with the recent distinction between formative and reflective constructs, the authors followed a prescribed protocol and determined that perceived ease of use (PEOU) and perceived usefulness (PU) are formative in nature – in contrast to previous studies. These findings have implications for the continued development of applicable measures of IT adoption in the security context as well as in other adoption studies.

Keywords: *Technology adoption, individual, TAM, UTAUT, security, assurance, behavior, scale, construct, formative, reflective, validation, validity*

Introduction

What leads someone to start backing up their important data? Why would an individual routinely scan for viruses or spyware? What motivates an end user to install a personal firewall? Why does one employee change his password regularly? These questions are extremely important not only to individuals, but to large and small businesses that employ individuals who must practice safe computing for the entire organization to be safe. Despite considerable evidence that the greatest source of security risk to most enterprises is the internal threat (the individual employee), most firms spend the majority of their IT security budget on perimeter controls designed to prevent and detect external threats. But because the internal threat is the greatest source of risk, we must pursue vigorous investigations into the individual adoption decision – what can we learn about the reasons for individual decisions with regard to IT security technologies?

The specific purpose of this paper is to present the findings of an initial phase of a multi-phase research endeavor in which IT adoption variables are examined for applicability within an IT security context. Given the recent call to attention within the IS community for a clear distinction between formative vs. reflective constructs (Loch et al. 2003; Petter et al. 2007), this initial phase includes the identification of representative IT adoption constructs and an assessment as to their formative or reflective nature. In the following paragraphs, background literature on technology adoption is reviewed and arguments are

made for how IT adoption constructs may be insufficient for capturing the essence of IT security adoption. The next section describes the research methodology. This includes an identification of two representative constructs, and an evaluation of their reflective or formative nature. Results of the analysis are discussed, and concluding comments are made. Finally, implications associated with the study's findings are suggested.

Background

Technology Adoption

Historically, the principle aim of technology adoption research has been to develop conceptual models which explain individual intention to adopt a given technology (Venkatesh et al. 2003). Following the inception of the Technology Acceptance Model (TAM) (Davis 1989), researchers have established and tested a multitude of derivative models including TAM2 and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003). The majority of these follow-ups were largely a modification of the original TAM, either augmented by new predicting variables, instantiated for a particular technology, or both (Karahanna et al. 2006). Indeed, as new information technologies caught the interest of information systems researchers, variations of TAM were published in many academic research journals (Schepers et al. 2007). The results of a content analysis provide more information on this trend. Several hundred TAM-related articles were reviewed and systematically grouped by categories of technology to be adopted. The groups were subsequently refined; three salient technology paradigms emerged: an era of stand-alone desktop technology in the late eighties and early nineties, the client-server paradigm of the mid to late nineties, and the Internet era following the new millennium (see Table 1).

Table 1. Classification of Technology Adoption Studies

Category	Percentage of Papers in Category	Description	Time of Influence	Example Technologies
Stand-Alone Desktop Technology	24.95%	Software for personal computers; the primary functionality of these applications exists without network connections.	Late Eighties to early Nineties	Personal productivity Suites; word processing, spreadsheet software
Client-Server Technology	25.08%	Software relying on a networked environment for main functionality.	Early to late Nineties	CRM systems; email systems; distributed databases
Internet-Based Technology	49.95%	Technologies which require an internet (IP) connection.	Mid Nineties to present	Web sites; Ecommerce portals; online classes

A rule that might be inferred from this trend is that the publication of models for the adoption of a specific technology lags just behind the identification of the associated technological paradigm. Furthermore, the adoption of each successive paradigm's information technologies seems to have received increasingly greater attention from behavioral researchers, as later eras boast more adoption models than earlier eras. Surprisingly, this heuristic does not hold for the case of information security technologies.

Despite strong interest among practitioners and academics, little research on information technology (IT) security adoption has been conducted (Warkentin et al. 2004). Surveys and interviews of chief information officers, business managers, and IT professionals routinely list information security as a top concern (Leach 2003; Oppliger 2007). On the academic side, a number of journals have been created specifically to address the managerial and technical issues associated IT security. In addition, several leading academic MIS publications have begun accepting security-related articles. However, there has been very little published work on individual adoption of security technologies. A plausible explanation of this phenomenon is the inapplicability of contemporary adoption predictors to the IT security context. Given the universal acceptance of technology adoption theory, along with a newly-piqued interest in IT, it is possible that a number of security adoption research projects were started but never actually completed. If this is true, then it might be because of inadequate performance of adoption predictors in the security context. If the constructs are ill-suited for security adoption, then their associated models would have little or no explanatory power, and the findings would not warrant publication. A closer examination of this question is warranted.

To investigate this research domain, we must first select the appropriate measures for consideration. (Please see Figure 1.) Then we must assess whether those scales are reflective or formative in the context of individual security technology adoption. Then we must analyze the validity of the constructs, according to the validation methodologies specified for that type of measure (Step 3a or 3b, depending on the construct's category). If the measures are deemed to be invalid, then new measures must be developed for the security context. New scales for these constructs must be then validated. To begin, we evaluate the first question – what are the most representative constructs for development in this context?

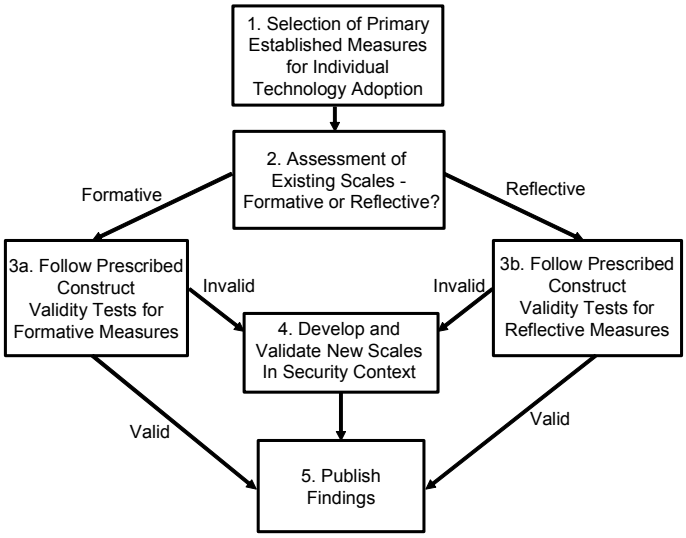

Figure 1. Process for Scale Assessment and Validation

Representative Adoption Constructs

Because a multitude of adoption constructs exist, it was useful to select the most representative constructs for closer examination. This was accomplished by identifying the constructs in the most commonly cited and used model for technology adoption. A comprehensive search of multiple online databases revealed that the Technology Adoption Model (TAM), as originally proposed by Davis (1989), was the most cited conceptual model in the research stream. At the time of the analysis, it was cited by 2116 articles (Google Scholar, 2007). Although dozens of more advanced adoption models have since been proposed, the majority of these models are based on the original TAM, and offer little additional explanatory power considering the relative loss in parsimony. In addition, the original constructs, Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) have been referenced in over 163 academic articles, well more than the constructs from any other adoption model. In sum, the two predictors, PEOU and PU remain highly representative and influential antecedents of technology adoption. The measurement items for PEOU and PU are depicted in Table 2.

Table 2. Measurement Items for Perceived Usefulness (PU) and Perceived Ease of Use (PEOU)

Perceived Usefulness (PU)	Construct	Perceived Ease of Use (PEOU)
Using [insert technology] in my job would enable me to accomplish tasks more quickly.	Item #1	My interaction with [insert technology] would be clear and understandable.
Using [insert technology] would improve my job performance.	Item #2	I would find [insert technology] to be flexible to interact with.
Using [insert technology] would improve increase my productivity.	Item #3	I would find it easy to [insert technology] to do what I want it to do.
Using [insert technology] would enhance my effectiveness on the job.	Item #4	Learning to operate [insert technology] would be easy for me.
Using [insert technology] would make it easier to do my job.	Item #5	It would be easy for me to become skilled at using [insert technology].
I would find [insert technology] useful in my job.	Item #6	I would find [insert technology] easy to use.

IT Security Adoption – A Case of Missing Measures

A plethora of sources consistently suggest that the greatest threat to IT security is not the external threat beyond the perimeter (hackers, malware, etc.), but rather the careless or malicious actions of the individuals behind the computers (Kesar 2006; Anderson et al. 1999). Secure behaviors include making regular backups, changing passwords, scanning for viruses, and many other activities identified by Whitman (2003). Other security activities include updating applications, installing patches, configuring firewalls, and turning off unnecessary ports (Whitman 2003; Rosenthal 2002; Stanton et al. 2003).

Within an organizational setting, each employee represents an endpoint of the organization's network, and without security-compliant behavior on the part of each and every employee (and other internal constituents), there can be no organizational security. Employees often lack awareness of safe computing policies and procedures (Adams and Sasse, 1999; Furnell, et al. 2002; Siponen, 2001) and are, therefore, not equipped to be in compliance. Most employees also lack the technical expertise to recognize sources of security threats (downloading files, web surfing behavior, etc.). Even if equipped with the appropriate awareness and skill set to effectively protect their assets, the employee must have a desire to do so. It is therefore the task of IT managers to understand the endpoint security problem in the organization, and to address the sources of threat in an appropriate manner.

In terms of technology adoption, characteristics of most security technologies differentiate them from the technologies most often examined in adoption studies. Previous studies involving adoption behavior examined outcomes and determinants associated with the use of productivity-based technology such as email utilities or spreadsheet applications. For example, Venkatesh et al. (2003) investigated user expectations of performance gains obtained from the use of a database application that could reference product industry standards. Applications such as these provide clear advantages to their users when compared to traditional approaches. However, not all technologies provide such obvious benefits (Warkentin et al. 2004). Information security tools such as anti-spyware programs or biometric access controls may provide a means of controlling computing environments or maintaining a healthy technological baseline from which to employ productivity enhancing technologies. Therefore, performance benefits may not be explicitly recognized.

Security technologies and procedures are intended to thwart unauthorized use of systems, data, and processes. Their goals are to ensure an acceptable level of confidentiality, integrity, and availability. In nearly all cases, the implementation of these technologies and procedures increases the number of controls to the protected assets; thereby elevating the time and effort needed to gain authorized access. By closely examining the language of the items for both PEOU and PU, it is not difficult to see where certain items for PU (items 1 and 5) and PEOU (items 3, 5, and 6) may not adequately capture what they are intended to capture. Security technologies and procedures are not intended to be easy to use and quick to complete. In fact, they are intended to have an opposite effect – to impede access, thereby making unauthorized access attempts a more difficult undertaking. To achieve these goals, a research project is proposed.

Methods and Results

To assess the applicability or utility of current adoption determinants within the IT security context a multi-phased research approach was undertaken. The first step in determining the degree to which current adoption measures can be applied to the IT security context is to validate the scales; and the first step in validating the scales is to determine their reflective or formative nature.

Reflective vs. Formative Constructs

As an initial step in validating PEOU and PU, it was necessary to formally assess the reflective or formative nature of the constructs in a manner such as that outlined by Petter et al. (2007). Petter et al. describe a series of criteria designed to assess a construct's measures and to classify it as formative or reflective (see Table 3). A reflective construct is comprised of reflective indicators that account for observed variances. These measures are unidimensional, such that if an individual measure is removed from the construct for validity purposes, the content validity of the construct is unaffected. In contrast, a formative construct is "formed" by its measures such that each indicator focuses on a distinct dimension of the construct, contributing to the overall content validity of the variable. When formative constructs are mis-specified as reflective, parameter estimates for models involving the mis-specified constructs are likely to be biased and any statistical conclusion derived from analysis is subject to scrutiny (Jarvis et al. 2003; Petter et al. 2007).

Table 3. Decision Rules to Identify Constructs as Formative or Reflective (Adopted from Petter et al. 2007; adapted from Jarvis et al. 2003)

Decision Rule	Formative Model	Reflective Model
What is the direction of causality between the construct and the measures?	Measures define the construct; therefore, direction of causality is from measures to the construct	Measures are expressions of the construct; therefore, direction of causality is from construct to measures
Are the measures interchangeable?	Measures do not need to be interchangeable The measures need not share a common theme Dropping a measure may affect the content validity of the construct	Measures should be interchangeable Measures should have a common theme Dropping a measure should not affect the content validity of the construct
Do the measures covary with one another?	Not necessary for measures to covary A change in one measure does not suggest that other measures will change as well	Measures are expected to covary A change in one measure suggests that other measures will change as well
Do all of the measures have the same antecedents and consequences?	Measures may or may not have the same antecedents and consequences	Measures must have the same antecedents and consequences

An examination of the PEOU and PU indicators (Table 2) reveals a direction of causality from the indicators to the construct. This is an indication of the presence of a formative construct. For example, the PU items address improvement in task accomplishment speed (item #1), job performance (item #2), productivity (item #3), effectiveness (#4), job ease (#5), and usefulness of technology (#6). Each of these indicators, if enabled, would "cause" a perception of usefulness. So, the measures define the construct. The same argument can be made for the direction of causality of the PEOU items and the construct. In terms of interaction, the PEOU items address clarity (item #1), flexibility (item #2), purpose (item #3), ease of learning (item #4), ease of becoming skilled (item #5), and ease of use (item #6). All of these indicators, if enabled, help to form a perception of ease of use.

In terms of measure interchangeability, formative indicators are not necessarily interchangeable, do not share a common theme, and the omission of one indicator has negative consequences for the "completeness" of the construct. It is not

difficult to argue that the indicators for both PU and PEOU meet these criteria, as each one addresses a unique aspect or dimension of its respective variable. In terms of covariance, it is also not difficult to see that as one indicator is adjusted, its influence on the language of the others is not negligible. This condition is directly tied to the independence of the indicators from each other in terms of their influence on the overall construct. Since each indicator of PEOU and PU addresses a unique dimension of their respective scale, its influence on other indicators is minimal. Yet, their presence is critical if all aspects of the construct are to be addressed. Finally, in terms of measurement antecedents and consequences, because each measure concerns a unique dimension in forming the constructs, they do not necessarily share a common set of predictors (antecedents) or outcomes (consequences). As each item of the PEOU and PU constructs is independent in terms of its contribution to the formation of the constructs, the theoretical origins of the items are distinct, as are their associated consequences.

As a useful comparison, consider the measures developed by Pavlou and Gefen (2005) to measure psychological contract violation with a community of sellers: "in general, sellers in Amazon's/eBay's auctions have failed to meet their contractual obligations to me during our transactions," "in general, sellers in Amazon's/eBay's auctions have done a good job of meeting their contractual obligations to me during our transactions," and "in general, sellers in Amazon's/eBay's auctions have fulfilled the most important contractual obligations to me during our transactions." By applying the same decision rules to this set of measures, it is concluded that Psychological Contract Violation with a Community of Sellers is a reflective construct.

An initial review indicates that the three associated measures are all expressions of the construct; they do not represent different dimensions of the construct. In addition, any one of the three measures could be removed without altering the construct's meaning. Therefore the direction of causality is from the construct to the measures. Further inspection reveals that the measures are expected to covary. Changes in one measure would almost certainly mean that other measures will change as well. The final requirement for a reflective construct is commonality of antecedents and consequences. This requirement is also met with Psychological Contract Violation with a Community of Sellers; a careful review of the conceptualization of the construct reveals that the antecedents and consequences are the same for all measures.

Discussion and Conclusions

As an initial step in assessing the applicability of current adoption measures within the IT security adoption context, the constructs, Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) were first selected as representative constructs, and then assessed as to their reflective or formative nature. While previous studies in the IS literature treat these constructs as reflective, the findings presented in this study reveal them to be formative. This is an important first step if future research is to assess their validity in the IT security adoption context.

Implications

Security technologies continue to increase in prominence as the artifact of interest in technology adoption studies. As such, the availability of applicable measures of adoption predictors becomes increasingly critical. This study provides an initial assessment of the applicability of two of the most commonly utilized predictive measures of adoption behavior -- perceived ease of use and perceived usefulness. While these variables are certainly applicable within the traditional technology adoption domain, in their original form, their utility within the security domain is questionable. The challenge lays in the fact that security technologies are not intended to be productive in nature. Their purpose is to secure environments in which productivity-oriented technologies operate.

As part of this initial assessment of the applicability of perceived ease of use and perceived usefulness within the security context, the constructs were identified as formative, thereby challenging their treatment as reflective measures in previous adoption literature. As formative, the constructs require approach to validity and reliability testing distinctive from that afforded to reflective constructs. For technology adoption studies in general, the implications are that reliance upon assessments of the scales from previous studies is ill-advised - all constructs must be accurately identified as reflective or formative and appropriately assessed. For security technology adoption studies in particular, the implications are that while some constructs are applicable within the broad technology landscape, scenarios involving computer security and/or information assurance are unique and require verbiage that captures the rationale for adopting technologies in excess of those needed to be productive.

Outline for Future Research

The findings presented in this manuscript constitute results from an initial phase of a multi-phase research endeavor. The next phase of this project involves validity tests of the PEOU and PU scales using methods appropriate to formative measures. It is expected that the results of these validity tests will lend further evidence that PEOU and PU, in their original form, are not applicable to the security context and that new measures for these scales must be developed. Pending this outcome, new, security domain specific scales of PEOU and PU are to be developed based on a thorough review of the literature and input from an expert panel of security practitioners and academicians. These newly modified scales will then be validated in the manner appropriate of formative measures. The complete research project is expected to yield validated measures of PEOU and PU applicable to the IT security adoption context.

References

Adams, A., and Sasse, M. A. "Users Are Not The Enemy," Communications of the ACM (42:12), 1999, pp. 40-46.

Anderson, R. H., Feldman, P. M., Gerwehr, W., Houghton, B., Mesic, R., Pinder, J. D., Rothenberg, J., and Chiesa, J. "Securing the U.S. Defense Information Infrastructure: A Proposed Approach, Washington, DC: Rand, 1999.

Davis, F. D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly (13:3), 1989, pp. 319-339.

Furnell, S. M., Gennatou, M., and Dowland, P. S. "A Prototype Tool for Information Security Awareness and Training," Logistics Information Management (15:6), 2002, pp. 352 - 357.

Google Scholar. Search conducted March 3, 2007, accessed at http://scholar.google.com/scholar?hl=en&lr=&q=Perceived+usefulness%2C+perceived+ease+of+use%2C+and+user+acceptance+of+information+technology.&btnG=Search

Jarvis, C. B., Mackenzie, S. B., and Podsakoff, P. M. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," Journal of Consumer Research (30:2), 2003, pp. 199-218.

Karahanna, E., Agarwal, R., and Angst, C. "Reconceptualizing Compatibility Beliefs in Technology Acceptance Research," MIS Quarterly (30:4), 2006, pp. 781-804.

Kesar, S. "Legal Issues Alone Are Not Enough to Manage Computer Fraud Committed by Employees," Journal of International Commercial Law and Technology (1:1), 2006, pp. 25-40.

Leach, J. "Improving Security Use Behavior," Computers & Security (22:8), 2003, pp. 685-693.

Loch, K. D., Straub, D. W., Kamel, S. "Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation," IEEE Transactions on Engineering Management (50:1), 2003, pp. 45-63.

Oppliger, R. "IT Security: In Search of the Holy Grail," Communications of the ACM (50:2), 2007, pp. 96-98.

Pavlou, P., and Gefen, D. "Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role," Information Systems Research (16:4), 2005, pp. 372-399.

Petter, S., Straub, D. W., and Rai, A. "Specification and Validation of Formative Constructs in IS Research," Georgia State University, working paper.

Rosenthal, D. A. "Intrusion Detection Technology: Leveraging the Organization's Security Posture," Information Systems Management (19:1), 2002, pp. 35-44.

Siponen, M. T. "Five Dimensions of Information Security Awareness," Computers and Society (31:2), 2001, pp. 24-29.

Schepers, J., and Wetzels, M. "A Meta-Analysis of the Technology Acceptance Model: Investigating Subjective Norm and Moderation Effects," Information & Management (44:1), 2007, pp. 90-103.

Stanton, J. M., Stam, K. R., Guzman, I., and Caldera, C. "Examining the Linkage Between Organizational Commitment and Information Security," Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC, 2003.

Straub, D. W., and Welke, R. J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly (22:4), 1998, pp. 441-469.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly (27:3), 2003, pp. 425-478.

Warkentin, M., Davis, K., and Bekkering, E. "Introducing the Check-off Password System (COPS): An Advancement in User Authentication Methods and Information Security," Journal of Organizational & End User Computing (16:3), 2004, pp. 41-58.

Whitman, M. "Enemy at the Gates: Threats to Information Security," Communications of the ACM (46:8), 2003, pp. 91-95.