Society for the Advancement of Information Systems
MBAA Abstract March 27-29, 2019 - Chicago

Author(s):
Anuradha Rangarajan, Indiana State University, Terre Haute, IN
David Batts, East Carolina University, Greenville, NC
Carolyn K. Dunn, East Carolina University, Greenville, NC

Title: Impact of perceived information technology security risks on user resistance to information technology innovations.

Abstract

Information technology security awareness and compliance have far reaching impacts on the long-term success of technology innovations. There are many studies in research literature relating to factors influencing information security adoption behaviors and antecedents to compliance of information security policies. However, few studies discuss the influence of perceived information security risks on user resistance to technology innovations and this creates a research gap. In this paper, the authors draw on current information systems theories and present a conceptual model to address this gap. They posit that perceived information security risks influence an individual's beliefs about outcome of utilizing the information technology innovation. This in turn impacts both the perceived trust in the security and privacy aspects of the innovation and user resistance to the technology innovation.

INTRODUCTION

Adoption of a technology innovation relies on the end user's comfort in utilizing the technology. Technology adoption theories like Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) aim to explain user intention to use an information technology (IT) system from the perspective of ease of use, usefulness and degrees of performance and effort expectancy. User resistance literature on the other hand covers multiple aspects such as reasons, factors and outcomes relating to user resistance (Ali, Zhou, Miller, & Ieromonachou, 2016). Information security features are embedded, often seamlessly, within these technologies. Risks related to information security vulnerabilities may lead to dire consequences including monetary damage, loss of credibility and liability (Bulgurcu, Cavusoglu, & Benbasat, 2010). For example, some empirical studies have shown that a user's perceived risk and fear of security breaches has an impact on adoption of mobile banking and payments (Yiu, Grant, & Edgar, 2007; Zhou,Lu, & Wang, 2011). However these studies lack in two aspects. First, they do not examine the specific elements of information security risks the user is concerned about, and, second, they do not consider how these elements influence a user's beliefs about outcomes which contributes to their resistance in using the IT innovation. Drawing from information systems theories the authors present a conceptual model to address this gap.

THEORETICAL BACKGROUND AND RELATED LITERATURE

This section provides an overview of the various bodies of literature relating to perceived risk, beliefs about outcome, perceived trust and user resistance to technology innovation. While each of these aspects has been individually analyzed and forwarded by researchers, the correlation and/or causation of these factors on user resistance has not been constructed to-date.

Perceived Risk

Multiple definitions of perceived risk exist in research literature. Cunningham (1967) has defined perceived risk as the uncertainty regarding possible negative consequences of adopting a product or service. According to Bettman (1973), perceived risk is an important inhibitor when circumstances of the decision create discomfort, anxiety and conflict in the decision maker. Ackermann, Widjaja, Benlian and Buxmann (2012) have cited multiple studies highlighting the various factors that perceived risk leads to, including overestimation, underestimation and "unrealistic optimism" related to risks.

From an adoption perspective, literature cites how risks and opportunities have impacted adoption of innovations such as IT outsourcing (Quinn & Hilmer, 1994), Application Service Provider model (Jayatilaka, Schwarz, & Hirschheim, 2002) and cloud computing (Ho, Ocasio-Velazquez, & Booth, 2017; Orehovcki, Etinger, & Babic, 2017). In other examples, Verkijika and De Wet (2018) have performed an empirical study on e-government adoption in sub-Saharan Africa and Damghanian, Zarei and Siahsarani Kpjuri (2016) have forwarded a research model that examines the relationship between perceived security and trust with the mediating effect of perceived risk and trust in Internet banking in Iran.

Ackermann et al. (2012) have conceptualized perceived IT security risks in the cloud computing context based on six distinct dimensions drawing from their in-depth literature reviews – *accountability*, *availability*, *confidentiality*, *integrity*, *maintainability and performance*. *Accountability* ensures that there is transparency on which entities have performed actions in the course of accessing the resource being secured. *Availability* indicates that users are able to access the resource when they require it without interruption. *Confidentiality* ensures that only authorized entities have access to resources in the security context. *Integrity* is obtained when the resource being protected cannot be manipulated by unauthorized entities. *Maintainability* ensues when the means by which the resource being secured can be modified and evolved over time, to meet contextual requirements. *Performance* is the characteristic that measures the speed with which the resource being secured is accessible. From an IT innovation standpoint, these requirements can be easily adapted to the product or service being developed. Ackermann et al. have developed an IT security risk measurement instrument based on these dimensions and empirically validated it in the cloud computing context. These factors explicitly seek to characterize various elements of security risks addressing both the technical and user experience aspects and has been utilized in developing the research model.

Beliefs about outcome

The theory of planned behavior (TPB) (Fishbein and Ajzen, 1975) has long been used to explain an individual's intention to perform a given behavior which can be predicted from their attitudes toward the behavior, subjective norms and perceived behavioral control. These intentions together

account for a considerable amount of variance in actual behavior (Ajzen, 1991). Rational choice theory (RCT) traces its origins several its origins to Becker (1968) in his work on the economic approach to crime. Based on this, McCarthy (2002) proposed a framework to explain how an individual determines their action be balancing the costs and benefits of their options. Since then, RCT has been widely adopted in the study of individual, social and economic behaviors in many contexts (McCarthy, 2002).

Building on TPB and RCT, Bulgurcu et al. (2010) have built a model to establishing antecedents to employee compliance of information security policy. Their proposed model establishes a link between information security awareness, beliefs about outcomes, beliefs about overall assessment of consequences with employee attitude and ultimately their intent to comply with information security policy. They define *beliefs about outcomes* as beliefs that certain events will follow from performing *or* not performing a certain compliance behavior. They make the important observation that the objective of creating information security awareness is to make employees cognizant of risks related to information security and to educate them about their roles and responsibilities concerning those risks.

Based on this, they have postulated seven outcome beliefs: intrinsic benefit, safety, rewards, work impediment, intrinsic cost, vulnerability and sanctions. *Intrinsic benefits, safety of resources* and *rewards* describe those events with positive outcome while intrinsic *cost, vulnerability* and *sanctions* align with inconveniences, stress guilt, self-imposed punishment, perception of security-related risks as a consequence of non-compliance and additional effort the employee has to take on, in order to comply with the information security policies. In this context, they define work impediment as a detriment to the employee's daily job-related tasks and activities due to their compliance with the said policies.

Perceived trust

Because trust is a multifaceted concept that spans several disciplines, multiple definitions exist depending on context (Verkijika & De Wet, 2018). Zhao and Khan (2012) forward trust as the promise made by one party that can be relied by the other party. Trust in the information security context is defined the user's beliefs or faith in the degree to which a service can be regarded to have no security and privacy threats (Gao, Krogstie & Siau, 2011). Research literature is abound on the impact of perceived trust on innovations such as mobile devices (Gao et al., 2011) and e-governance services adoption (Belanche, Casalo, & Flavian, 2012; Verkijika & De Wet, 2018). Verkijika and De Wet (2018) cite many studies that have supported the positive and significant association of trust of an innovation such as e- services to user's behavioral intent to adopt them. In their study of antecedents to adoption of online banking in Iran, Damghanian et al. (2016) showed the positive effect of trust on user adoption of online banking. An additional important conclusion they were able to draw was that the more the perceived risk by users, the less the trust online banking and vice-versa.

User Resistance

User resistance has been studied from multiple perspectives. Early studies by Lewin (1947) approached this from the social standpoint where status quo represents an equilibrium between forces opposing and favoring change. Lewin posited that to enact change at an organizational level, this equilibrium needed to be unfrozen first. Kling (1980) has elaborated this from a people, system

and interaction aspects. Markus (1983) has explained resistance in the context of the technology being implemented and its use, where individuals are inclined to use it if they believe it supports their position of power. The equity-implementation model (Joshi, 1991) attempts to explain resistance to change as a three-level process whereby users evaluate the implications or net gain from changes in their inputs, outputs it produces and comparing it to the relative outcomes with other groups of users. Marakas and Hornik (1996) have presented a model of user rejection based on passive resistance leading to passive-aggressive responses to perceived threats that an individual may associate with a new technology. They have coined the term *passive resistance misuse* to represent cover behavior resulting from fear and stress from the technology's intrusion into the user's previously stable world. Campbell and Grimshaw (2016) have borrowed from social and cognitive psychology to explain user resistance from 28 heuristics and peripheral influences based on the elaboration likelihood model. Ali et al. (2016) have categorized in their literature review of user resistance to IT the major sources of resistance to include distorted perception, low motivation for change, lack of creative response and political and cultural deadlock. They also highlight that several studies have focused on the topic of overcoming user resistance using techniques such as effective change management, training, employing participative as well as supportive approaches with concerns to alleviate employee's moral aspect of resistance.

Studies have been conducted to investigate the link between user resistance and outcomes in specific technological contexts. Jiang, Muhanna and Klein (2000) have surveyed IT managers across a spectrum of organizations to identify resistance to decision support systems and transaction processing systems and found that each has a different set of underlying resistance reasons with the most significant one being change in decision-making approaches as a result of the newer system's implementation. Laumer, Maier, Eckhardt and Weitzel (2016) have conducted an empirical study of human resource (HR) employees' resistance to utilizing a new HR information system predicated on the Oreg's model (2003) that individuals have a predisposition to resist change. In their model, they posit that a predisposition to resist change influences a perceptual resistance to change, perceived ease of use and usefulness which in turns influences user resistance behavior. Bhattacherjee and Hikmet (2007) have studied physician resistance to healthcare information technology by integrating the technology acceptance and resistance to change literatures using a dual-factor model of technology usage. They have empirically supported the model through a field survey of 129 practicing physicians at a large acute-care hospital. Results show that resistance to change had a significant negative effect on perceived usefulness, while perceived threat to using the technology had a significant positive effect on resistance to change. To study user resistance to healthcare information technology innovations Ngafeeson (2015) draws on the psychological reactance theory to explain the relationship between perceived threat and user resistance to electronic health record adoption.

While the studies above point to a set of antecedents to user resistance to technology adoption, they have each been conducted in isolation from each other. With the growing importance of information security awareness and implications of its breaches, there is a need for a model that helps explain how perceived information security risks may impact user resistance to IT innovations. Such a model is proposed in the next section.

CONCEPTUAL MODEL

This section builds on the research literature reviewed and postulates several hypotheses for antecedents of user resistance to technology innovation from an information security risk perspective. The model is shown in Figure 1. The independent variables fall into three broad categories: (1) perceived information security risks, (2) beliefs about outcome and (3) perceived trust. It is also posited that beliefs about outcome impacts perceived trust. The combined effect of these variables impact the dependent variable of user resistance to technology innovation.

The six constructs of perceived information security risks have been adopted from Ackermann et al. (2012). Each plays a critical part in influencing the user's belief regarding the outcome from utilizing the technology innovation. The first hypothesis has three components, following the constructs of intrinsic benefit, intrinsic cost and work impediment forwarded by Bulgurcu et al. (2010). Intrinsic benefit in the current context is defined as the user's positive emotions such as satisfaction, feeling of safety or perception of reward reaped from using the technology innovation. Intrinsic cost in this context is defined as the user's negative feelings – such as apprehension, stress and anxiety stemming from the perceived security vulnerabilities in the technology. Users may also fear sanctions or penalties - such as loss of social reputation and unfavorable mention among peer groups for not embracing the technology. Work impediment in this context is defined as a detriment to user's daily activities resulting from the technology's use.

> ***H1a:*** *Perceived information technology risks negatively affect user's beliefs about outcome regarding intrinsic benefits of using the technology innovation*
> ***H1b:*** *Perceived information technology risks positively affect user's beliefs about outcome regarding intrinsic cost of using the technology innovation*
> ***H1c:*** *Perceived information technology risks positively affect user's beliefs about work impediment from using the technology innovation*

Similarly, the second hypothesis has three components to delineate the impact of positive, negative beliefs about outcome and work impediment on perceived trust in the technology innovation. Trust as defined by Gao et al. (2011) in the information security context is utilized here.

> ***H2a:*** *User's perceived beliefs about outcome regarding intrinsic benefit, positively affects perceived trust that the technology innovation has no security or privacy threats*
> ***H2b:*** *User's perceived beliefs about outcome regarding intrinsic cost, negatively affects perceived trust that the technology innovation has no security or privacy threats*
> ***H2c:*** *User's perceived work impediment negatively affects perceived trust that the technology innovation has no security or privacy threats*

The third hypothesis as well has three components to depict the impact of positive and negative beliefs of outcome and work impediment on user resistance to the technology innovation.

> ***H3a:*** *User's perceived beliefs about outcome regarding intrinsic benefits of using the technology innovation, negatively affects user resistance to the technology innovation*
> ***H3b:*** *User's perceived beliefs about outcome regarding intrinsic cost of using the technology innovation, positively affects user resistance to the technology innovation*

> ***H3c:*** *User's perceived beliefs about outcome regarding work impediment of using the technology innovation, positively affects user resistance to the technology innovation*

The final hypothesis attempts to identify the relationship between perceived trust and user resistance to the technology innovation.

> ***H4:*** *Perceived trust that the technology has no security or privacy threats, negatively affects user resistance to the technology innovation*

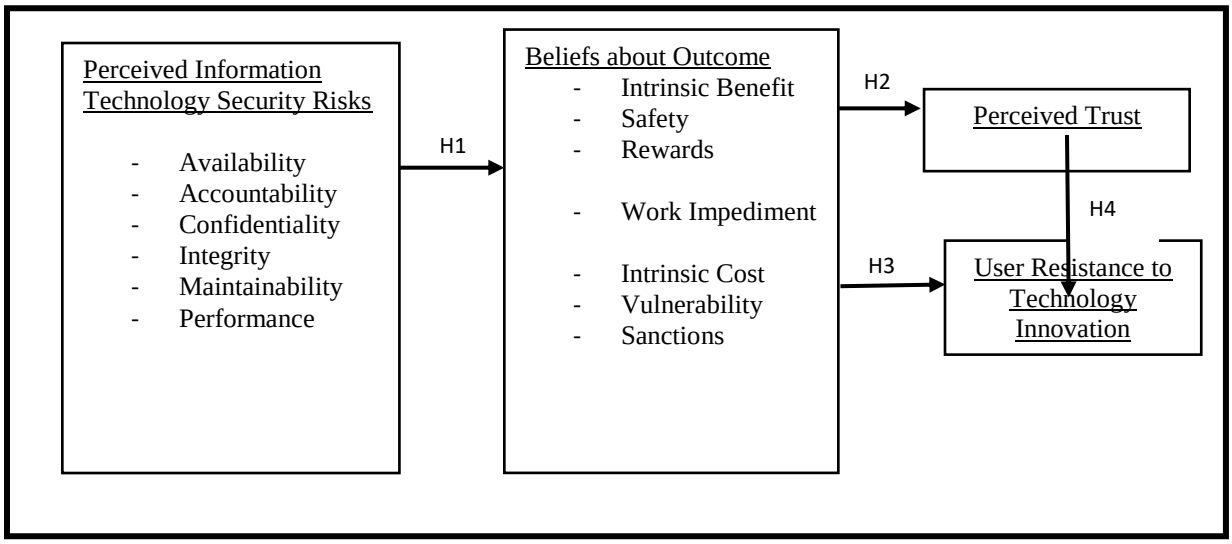

Figure 1. Impact of Perceived Information Technology Security Risks on User Resistance to Information Technology Innovations: A Proposed Model

This study makes several theoretical contributions to the emerging body of knowledge about antecedents to user resistance to technology innovations. First, the current body of literature has investigated user resistance factors from an individual and organizational context, but, this is the first study to draw on impacts of perceived information security risks on user resistance. Second, this study incorporates the notion of intrinsic cost and benefit factors from utilizing the technology, as a determinant to user resistance. Finally, several studies have investigated the impact of trust on user acceptance of technology. However, this model is novel in that it attempts to depict user's trust on the information security aspects of the technology as a factor impacting user resistance to the technology innovation.

LIMITATIONS

The conceptual model has several limitations. First, it does not attempt to capture every aspect of information technology risk that can be potential antecedents. The risk factors included in the model are broadly categorized. Hence, further developments to this model would require that these factors be more narrowly re-defined for the context it is applied in. Second, it does not account for controlling factors such as experience with related technology, or gender bias. Third, the antecedents to user resistance are all examined from an individual user's perspective alone (i.e.) it does not consider organizational factors such as organizational risk appetite and culture.

CONCLUSION

The objective of this study was to develop a conceptual research model that can predict the impact of perceived information technology security risks on user resistance to the technology innovation. It sought to fill the gap in current research literature where the impact of perceived information technology risks on barriers to technology adoption have not been studied in depth. It seeks to add a novel perspective to predicting user resistance to technology innovation by leveraging the belief about outcome framework forwarded by Bulgurcu et al. (2010), based on the rational choice theory. Perceived information security risks can tacitly and subconsciously influence user's behavior of outcome beliefs towards acceptance or resistance to technology. Intrinsic benefits and costs are two critical yet latent factors that can impact a user's perceived trust and ultimately user resistance to the technology innovation. From an academic standpoint, this paper adds to the body of literature by attempting to explain user resistance to technology from a perceived information technology risk standpoint. As a next step to progress this model, an empirical study needs to be conducted to support the hypothesis presented.

REFERENCES

Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012). *Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development* (No. 58577). Darmstadt Technical University, Department of Business Administration, Economics and Law, Institute for Business Studies (BWL).

Ali, M., Zhou, L., Miller, L., & Ieromonachou, P. (2016). User resistance in IT: A literature review. *International Journal of Information Management*, *36*(1), 35-43.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Bettman, J. R. 1973. "Perceived Risk and Its Components: A Model and Empirical Test," *Journal of Marketing Research* (10:2), pp. 184–190.

Bhattacherjee, A., & Hikmet, N. (2007). Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. *European Journal of Information Systems*, *16*(6), 725-737.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Campbell, R. H., & Grimshaw, M. (2016). User Resistance to Information System Implementations: A Dual-Mode Processing Perspective. *Information Systems Management*, *33*(2), 179-195.

Cunningham, S. 1967. "The Major Dimensions of Perceived Risk", in "*Risk Taking and Information Handling in Consumer Behavior*", D. F. Cox (ed.), Harvard University Press, pp. 102–108.

Damghanian, H., Zarei, A., & Siahsarani Kojuri, M. A. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce*, *15*(3), 214-238.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Gao, S., Krogstie, J., & Siau, K. (2011). Developing an instrument to measure the adoption of mobile services. *Mobile Information Systems*, *7*(1), 45-67.

Ho, S. M., Ocasio-Velazquez, M., & Booth, C. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security*, *70*, 581-595.

Jayatilaka, B., Schwarz, A., and Hirschheim, R. 2002. "Determinants of ASP choice: an integrated perspective," *IEEE*, pp. 2790-2800.

Jiang, J. J., Muhanna, W. A., & Klein, G. (2000). User resistance and strategies for promoting acceptance across system types. *Information & Management*, *37*(1), 25-36.

Joshi, K. (1991). A model of users' perspective on change: the case of information systems technology implementation. *MIS quarterly*, 229-242.

Kling, R. (1980). Social analyses of computing: Theoretical perspectives in recent empirical research. *ACM Computing Surveys (CSUR)*, *12*(1), 61-110.

Laumer, S., Maier, C., Eckhardt, A., & Weitzel, T. (2016). User personality and resistance to mandatory information systems in organizations: a theoretical model and empirical test of dispositional resistance to change. *Journal of Information Technology*, *31*(1), 67-82.

Lewin, K. (1947). Frontiers in group dynamics: Concept, method and reality in social science; social equilibria and social change. *Human relations*, *1*(1), 5-41.

Marakas, G. M., & Hornik, S. (1996). Passive resistance misuse: overt support and covert recalcitrance in IS implementation. *European Journal of Information Systems*, *5*(3), 208-219.

Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM*, *26*(6), 430-444.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, *28*(1), 417-442.

Ngafeeson, M. (2015). Understanding User Resistance to Information Technology in Healthcare: The Nature and Role of Perceived Threats.

Oreg, S. (2003). Resistance to change: Developing an individual differences measure. *Journal of applied psychology*, *88*(4), 680.

Orehovački, T., Etinger, D., & Babić, S. (2017, May). Perceived security and privacy of cloud computing applications used in educational ecosystem. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on* (pp. 717-722). IEEE.

Quinn, J. B., and Hilmer, F. G. 1994. "Strategic Outsourcing," Sloan Management Review (35:4), pp. 43–55.

Verkijika, S. F., & De Wet, L. (2018). E-government adoption in sub-Saharan Africa. *Electronic Commerce Research and Applications*, *30*, 83-93.

Yiu, C.S., K. Grant and D. Edgar, 2007. Factors affecting the adoption of internet banking in Hong Kong implications for the banking sector. International Journal of Information Management, 27 (2) : 336-336

Zhao, F., Khan, M.S., 2013. An empirical study of e-government service adoption: culture and behavioral intention. Int. J. Public Admin. 36 (10), 710–722.

Zhou, T., Lu, Y., and Wang, B. (2010), "Integrating TTF and UTAUT to explain mobile banking user adoption", Computers in Human Behavior , Vol. 26 No. 4, pp. 760-767.