THREE ESSAYS ON

ADOPTION AND CONTINUOUS IMPROVEMENT OF INFORMATION SECURITY MANAGEMENT IN ORGANIZATIONS

by

FERESHTEH GHAHRAMANI

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

August 2018

To Mom and Dad,

for their big heart, unwavering love, timely encouragement,

unconditional support, unlimited faith, and endless patience.

ACKNOWLEDGEMENT

My deepest gratitude and respect for my advisor and dissertation chair, Dr. Jingguo Wang, for teaching me how to be a critical thinker, independent scholar, and responsible teacher. Thank you for helping me realize the power of analytical reasoning, hard work, and self-confidence.

My sincere thanks must also go to the members of my dissertation committee for their valuable comments and encouragement through this process. Dr. Wendy Casper, thank you for being such an amazing role model. Dr. Sridhar Nerur, thank you for the invaluable and timely support you provided.

It has been a great privilege and wonderful experience to be part of University of Texas at Arlington. I would like to thank the ISOM department professors for their support and guidance, each in their own way. Special thanks to the (NSF) National Science Foundation (under grant SES-1420758) and University of Texas at Arlington (interdisciplinary research grant) for financially supporting my dissertation.

I cannot forget friends whom we went through the years of our Ph.D. studies together: Adel Yazdanmehr, Somaye Ramezanpour Nargesi, and Faezeh Amirkamali. Thank you for listening, sharing your experience, offering me advice, and supporting me through this journey. Special thanks to my Mississippi family.

Most importantly, I will remain forever grateful to my wonderful parents. This journey was impossible without their support, love, and patience. They inspired me to fly toward my dreams. Thank you for sharing your smiles, words of encouragement, and all the countless times you've been there for me. The most beautiful thing in this world is to see you smiling. Heartfelt thanks to my brother for his love and emotional support.

June 08, 2018

ABSTRACT

THREE ESSAYS ON ADOPTION AND CONTINUOUS IMPROVEMENT OF INFORMATION SECURITY MANAGEMENT IN ORGANIZATIONS

Fereshteh Ghahramani, PhD

The University of Texas at Arlington, 2018

Supervising Professor: Jingguo Wang

In information intensive organizations secured management of information has become an important issue. Although organizations have been actively investing on information security, crime rate in this area keep increasing. Practitioners and academics have started to realize that information security cannot be achieved through only technological tools. Effective organizational information security depends on how to manage such activities in organizations.

Empirical research on the management side of information security behaviors and factors influencing them is still in its infancy. The aim of this three essay dissertation is to focus on adoption and continuous improvement of information security management practices in organizations and uncover factors that play a significant role on IT professionals' and managers' decisions in dominant security contexts.

More specifically, the first essay explores the factors which affect decision makers' intention to adopt novel authentication systems. It examines how usability, deployability and security, as evaluation criteria of authentication systems, influence IT professionals' decision making process in this regard. Further, the second essay elaborates on information security activities in organizations which occur prior to the incident. Taking a prototype-willingness model perspective, this essay aims to investigate how both rational and heuristic aspects of decision

making can affect IT professionals' proactive information security behavior. Finally, the third essay focuses on continuous improvement in information security management. Drawing upon organizational learning perspective, this study suggests organizational absorptive capacity enhances the way organizations dynamically and repeatedly make improvements in their information security management processes.

Table of Contents

INTRODUCTION

In information intensive organizations secured management of information has become an important issue. Although organizations have been actively investing on information security, crime rate in this area keeps increasing (The Economist Intelligence Unit 2016). Practitioners and academics have started to realize that information security cannot be achieved through only technological tools. Effective organizational information security depends on how to manage such activities in organizations (Padayachee 2012). Information security management is a process of protecting critical systems and information from internal and external information security risks and threats effectively (Barlas et al. 2007; Tu and Yuan 2014), and mainly includes guidelines for comprehensively identifying vulnerable information assets, establishing security objectives, evaluating risks, and actions to deal with those risks (Dubois et al. 2010; Stoneburner et al. 2002; Hoo 2000). Empirical research on the management side of information security behaviors and factors influencing them is still in its infancy (Padayachee 2012). The aim of this dissertation is to focus on adoption and continuous improvement of information security management practices in organizations and uncover factors which play a significant role on IT professionals' and managers' decisions in dominant security contexts.

More specifically, in the first essay, I explore the factors which affect decision makers' intention to adopt novel authentication systems. Authentication systems were chosen purposefully, as they are tightly integrated with organizational routine jobs, and users need to constantly interact with them to access information (Mare and Gummeson 2016). Despite the development of novel authentication systems, organizations today are relying on traditional passwords as their main authentication method for employees' access to their internal systems, and the adoption of a variety of alternatives has been slow. Taking a decision-making perspective, in this study we bring new

insights to the organizational adoption of novel authentication systems. Results of an online survey from 193 IT professionals indicate that usability, deployability and security, as evaluation criteria of authentication systems, increase decision makers' intention to adopt an authentication scheme. Usability has the strongest effect. Further, for the organizations that are more IT-intensive, the effects of usability and security features on adoption intention are stronger. Also, for organizations that are experiencing a higher level of competitive pressure, the effect of usability on adoption intention is weaker, while that of deployability is stronger.

In the second essay, I elaborate on information security activities in organizations that occur prior to the incident (Kwon and Johnson 2014). Proactive information security management in organizations has been suggested to be an effective approach for preventing data breaches and security incidents. What motivates IT professionals to adopt such practices or behaviors for their organizations, however, is not clear. Taking a prototype-willingness model perspective, this essay aims to investigate how both rational and heuristic aspects of decision making can affect IT professionals' proactive information security behavior. Findings from an online survey which was conducted among 193 IT professionals show that both aspects impact their proactive behavior. Further, dominant external environmental characteristics such as competitive pressure, environmental uncertainty, and regulatory environment strength the effect of IT professionals' willingness to pursue proactive information security behavior on the organizations' actual behavior.

In the third essay, I focus on continuous improvement in information security management. Drawing upon organizational learning perspective, this study suggests organizational absorptive capacity is an essential driver and enhances the way organizations dynamically and repeatedly make improvements in their information security management processes. Besides the direct path,

an indirect effect of absorptive capacity to continuous information security management is also proposed, i.e., mediated through the organization's adaptiveness to information security threats. Furthermore, this study suggests that the influence of absorptive capacity to adaptiveness is moderated by the nature of regulatory environment. Survey data collected from 130 U.S.-based organizational managers familiar with information security practices provide support to our research hypotheses.

Chapter One:

Toward an Organizational Innovation Approach: Adoption of Novel Authentication Systems Perspective

1.1.INTRODUCTION

Authentication refers to the procedure of providing evidence to verify users' identity (Panko 2009). Its purpose is to make sure system resources are genuinely accessed or used by authorized users (Liao et al. 2006). It is one of the core approaches to the growing requirement of assuring legitimate access and authorized use of information resources (Reid 2004; Tipton and Krause 2003; Alhussain and Drew 2012). Authentication systems are software and hardware solutions that implement authentication methods (Dasgupta et al. 2016).

At the 2004 RSA Security conference, Bill Gates pointed out traditional password-based authentication systems should be replaced. According to a 2016 survey by Gigya (2016), only 16 percent of internet users in the U.S. and U.K. had a unique password for each of their accounts; and in the same survey, more than 25 percent of respondents had at least one of their online accounts compromised in the past year. According to Verizon's report, more than 60 percent of verified data breaches are a result of weak, stolen, or default passwords (Verizon 2016). Users often employ easy-to-guess passwords (Chang 2016), rely on the same passwords for different systems, and sometimes even share their password with others (Theofanos et al. 2016; Eich et al. 2016; Habib et al. 2017).

A number of novel authentication systems (Bonneau et al. 2012) have been developed. Such schemes are either using a totally alternative system for authenticating legitimate users such as biometrics like fingerprint or retina patterns (Jain et al. 2006; Bachmann 2014) and keystroke dynamics (Monrose and Rubin 2000), or combining more than one scheme in order to lessen information susceptibilities (D'Costa-Alphonso and Lane 2010; Stanislav 2015; Ryan 2016). However, the adoption of novel authentication systems has been slow (U.S. Department of Health & Human Services 2015). As it is critical for an organization to have a strong authentication system

to prevent data breach and information loss (Dasgupta et al. 2016), it is puzzling why novel authentication schemes have not taken root at organizations (Reynolds 2016).

This study attempts to explore how the attributes of authentication systems influence IT professionals' choices in selecting an authentication system considering their organizational situations. IT professionals are one of the most important and influential groups which impact security management in organizations. Most everyday tactical functions and operations in information security are the responsibility of IT professionals. IT professionals, including staffers and teams, are organizations' forefront in implementation and operationalization of cybersecurity strategies, and are in charge of preventing attacks and finding solutions for breaches (The Global Information Security Workforce Study 2017). Therefore, considering the important role of IT professionals in organizations' cybersecurity strategies, understanding how they make choices regarding security management is critically important.

Taking a perspective of choice and decision-making, the first aim of this study is to examine how the attributes of an authentication system influence decision makers' intentions to adopt. Each technology has its characteristics which often play a significant role in influencing organizations' selection decisions (Damanpour and Schneider 2009). Such characteristics can be either primary attributes, which are intrinsic to the technology such as actual cost price, or secondary attributes, which are the characteristics perceived by individual adopters such as the perception of cost (Downs et al. 1976; Moore and Benbasat 1991). Usability, deployability and security have been suggested to be the main aspects used to evaluate and compare authentication systems (Bonneau et al. 2012). This study will help us understand if security of an authentication system is the most important consideration or if other characteristics may be more important for decision makers' choice.

Unlike other security solutions such as firewalls, intrusion detection systems, and antivirus software, authentication systems are often tightly integrated with organizational routine jobs, and users need to constantly interact with them to access information (Mare and Gummeson 2016). Different organizations may have different demands for authentication systems due to the extent of which information technology is utilized in the organizations' environment. Information technology (IT) intensity refers to the degree to which IT appears in the products, services, decisions, and processes of an organization (Chou et al. 1998; Thong and Yap 1995; Thong 1999). As organizations use more and more IT in their activities and processes, it is important for them to align their strategies with this organizational context and consider the level of IT intensity in their decisions. Organizations' level of IT intensity may modify the effect of different technological characteristics of authentication systems on adoption intention. More specifically, the second aim of the study is to investigate the moderating role of IT intensity.

Moreover, organizations typically establish and implement technical and managerial innovations (Goel and Shawky 2009) such as authentication systems in order to minimize security breaches and, as a result, maintain their competitive advantage among other competitors who are active in the industry (Goel and Shawky 2009). However, as the competition becomes more intense, the likelihood of successful implementation of such innovations decreases (Yoon and Lilien 1985). Therefore, it is more important for organizations that are experiencing high competitive pressure to precisely evaluate each systems' features and allocate additional weight to the systems' features while evaluating various alternatives and making decisions. Hence, the third aim of this study is to investigate how decision makers adjust the effect of authentication system characteristics when forming their adoption intention given the level of competitive-related pressure in their industry. We investigate the moderating role of competitive pressure.

We collected survey data for hypothesis testing. The respondents were limited to full-time employees who have more than three years of working experience as an IT professional, and have technical knowledge about user authentication systems in their organization. Our results suggest that the usability, deployability, and security of authentication systems affect organizational decision makers' intention to adopt authentication systems. Usability has the strongest effect. Moreover, for the organizations with higher IT intensity, the effect of usability and security features on adoption intention is stronger. For organizations that are active in hypercompetitive industries, the effect of usability and deployability features on adoption intention are weaker and stronger, respectively. Findings of these moderating effects will help security service providers offer systems that adapt to the organizations' both internal and external environment.

1.2.RELATED LITERATURE

Generally there are three types of information that authentication relies on (Bolle et al. 2004; Miller 1994; O'Gorman 2003): something users know such as a PIN or password; something that users have, such as smart cards or tokens; and something that users are, such as biometrics. The first two types are the most commonly used for authentication (Scott et al. 2005). While not as popular, the last type concerning users' behavioral and biological characteristics is considered to be more reliable and trustworthy (Elliott et al. 2004; Alhussain and Drew 2012).

From the users' point of view, James et al. (2006) applied technology acceptance model (TAM) constructs in addition to physical invasiveness and perceived need for privacy and security to predict individuals' intentions to use biometric devices. Pooe & Labuschagne (2011) explored the factors which affect the adoption of biometric technology among banking staff in South Africa. They argued that legacy systems, culture, legislation, standards, and technology maturity are key factors that affect users' adoption of biometric technology.

A few other studies have empirically examined the important factors which influence decision makers' intentions to adopt biometric authentication systems in their organizations (Laux 2007; Laux et al. 2011; Lease 2005). Based on responses from managers in Credit Union company, Laux and his colleagues (Laux 2007; Laux et al. 2011) showed that the perceived benefits of the technology, financial resources of the company, and competitive factors drive the intentions to adopt biometric authentication system for organizations. Lease (2005) also suggested the important role of perceived effectiveness, business need, and reliability of biometrics in explaining the intentions of IT managers to adopt authentication schemas. Most of the aforementioned studies emphasize the importance of user experience.

While theoretical frameworks such as TAM may provide us an understanding of adoption intentions in terms of usefulness and ease of use from a user's perspective, they do not take into account how decision makers make a choice with different yet conflicting objectives to achieve. It is unclear how decision makers weigh technological characteristics in forming their adoption intention, for example, which characteristics are the most important ones. Other theories, such as protection motivation theory (PMT) (e.g. Johnston and Warkentin 2010; Boss et al. 2015) and technology threat avoidance theory (TTAT) (e.g. Liang and Xue 2009), have been mostly used to analyze individuals' intentions to adopt a certain self-protective behavior or a safeguarding measure in response to a particular threat in the environment. Authentication systems are often introduced into an organization as a holistic security solution mitigating a range of security issues to ensure the confidentiality, availability, and integrity of information. Therefore, it may be too simplified to assess a particular threat (e.g. data breach) in forming the adoption intentions of a decision maker for an authentication system. Furthermore, studies in the authentication system literature do not take into account the impacts of organizational contexts. Examining the

moderating roles of organizational contexts helps us to find out how decision makers adapt to their organizations when forming their adoption intentions.

1.3.THEORETICAL BACKGROUND

1.3.1. Structured Decision Making Process and Systems Adoption

Adopting a new idea or technology in an organization is referred to as an organizational innovation (Zaltman et al. 1973; Daft 1978; Damanpour 1991). Considered a source of financial and technological growth (Damanpour and Schneider 2006), such innovation are expected to benefit organizations (West and Anderson 1996). Adopting a novel authentication system is one form of organizational innovation that could be part of organizational information security management strategies to gain an advantage in the competitive and insecure marketplace. The implementation of such innovations in an organization is typically the result of decisions made by members of the organizations' decision-making unit (Carley and Behrens 1999), who evaluate how the innovation can help achieve different objectives within the organization. Their assessment of an innovation affects their adopt intentions (Ostlund 1974; Tornatzky and Klein 1982; Rogers 1995). Figure 1.1 illustrates the stages of a rational decision making process. Following a structured approach of decision analysis (Keeney 1982; Choo 1996; Cabantous and Gond 2011), decision makers often first formulate the decision problem. Then, they search for, or solicit, a list of alternatives or possible solutions. In assessing different innovative ideas, decision makers may develop a list of criteria based on technological, economical, and strategic viewpoints (Meyer and Goes 1988; Damanpour and Schneider 2006). Information on each alternative is then collected with respect to the criteria. Finally, decision makers compare the various alternatives and choose the one with the maximum utility to adopt.

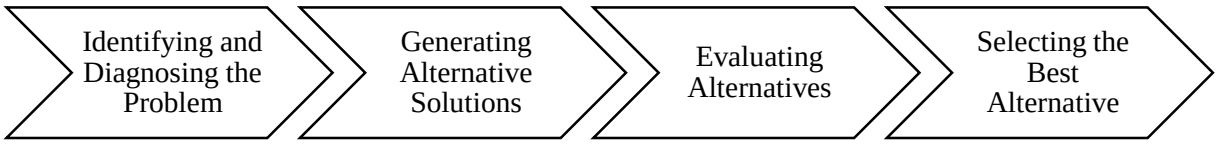

Figure 1.3.1.1: Schematic Representation of the Steps of Decision Making

1.3.2. Characteristics of Authentication Systems

Bonneau et al. (2012) reviewed authentication systems developed in the past 20 years. To compare them, they classified their attributes into three classes of innovation characteristics: usability, deployability, and security. Usability, in general, refers to the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component (Geraci et al. 1991). In this setting, usability is comprised of system characteristics significant to end users working with the system. It is important for decision makers that system users can easily learn how the authentication process works and can authenticate without too much effort.

Secondly, security is defined as the extent to which the system prevents or handles threats and vulnerabilities caused by attackers (Brauch 2011). As the purpose of authentication is to provide data security (Liao et al. 2006), decision-makers' priority is to make sure that the system is secure enough to prevent malicious agents from exploitation. Important to note, the concept of security is different from the concept of response efficacy in other theoretical frameworks such as PMT. Response efficacy evaluates the system in terms of its ability to deal with a particular threat generally, while security, in our study, assesses the system by its capability to prevent or handle a range of all possible threats which organizations might face, possibly from both legitimate and illegitimate users.

Finally, deployability refers to the extent of which an organization needs to put effort into installing, testing, and implementing an authentication system in its environment. This innovation characteristic evaluates the compatibility of a new system with the organizations' settings and includes features related to financial efforts, accessibility, compatibility, and maturity. Bonneau et al. (2012) used eight, eleven, and six features to define usability, security, and deployability in the context of authentication systems (Table 1.1).

1.3.3. Role of Environmental Features in Decision Making Process

Deciding to introduce an innovation in organization does not happen in isolation. Organizational behavior is somehow constrained and controlled by the demand in the environment (Pfeffer 1982). Scholars have shown that environmental forces are powerful enough to modify organizations' strategic plans, decisions and performance (Phillips 1999). So it is essential for organizational decision makers to be responsive to them, and consider them in their decision making (Wang et al. 2012).

Organizational contexts may alter the importance of innovation characteristic on decision makers' adoption intention (Tornatzky et al. 1990; Wolfe 1994; Rogers 1995). With the emergence and growth of information technology in organizations, almost all the procedures, decisions and other environmental features inside the organizations are somehow modified or inspired by these new technologies.

Table 1.1. Features of Authentication Systems (Bonneau et al., 2012)

	Feature	Definition
Usability		
	Memorywise-effortless	The extent to which users have to remember secrets in the authentication process
	Scalable-for-users	Using the system by so many accounts will not raise the cognitive burden on users.
	Nothing-to-carry	Users do not require to carry any extra physical item such, as cards, keys or electronic devices.
	Physically-effortless	The degree to which users are required to put physical effort into the authentication process. Physical effort may refer to just pressing a button or typing a password.
	Easy-to-learn	The extent to which the users who are not familiar with the scheme can figure out, learn, and remember how it works.
	Efficient-to-use	The time users have to devote for authentication each time.
	Infrequent-errors	The degree to which the scheme is reliable and easy to use and does not reject genuine and honest users.
	Easy-recovery-from-loss	The extent to which users are able and convenient to authenticate in cases they lose a physical item or forgot the secrets.
Security		
	Resilient-to-physical-observation	The extent to which the scheme is robust against attackers who imitate users after witnessing them authenticating to the system. Shoulder surfing, and sound recording of keystroke are two possible forms of such attacks.
	Resilient-to-targeted-impersonation	The degree to which a system is resilient to acquaintances who impersonate legitimate users by abusing personal information, such as date and place of birth.
	Resilient-to-throttled-guessing	The extent to which the system is resilient to limited guessing attacks, where the attacker can truly guess or predict the secrets of legitimate users.
	Resilient-to-unthrottled-guessing	The degree to which the system is successfully resilient to unlimited guessing attacks.
	Resilient-to-internal-observation	The extent to which the system is resilient to possible internal observations attacks like key-logging.
	Resilient-to-leaks-from-other-verifiers	The degree to which the system is robust against attackers who imitate users after there is a leak from other verifiers.
	Resilient-to-phishing	The extent to which the system is resilient to phishing attacks.
	Resilient-to-theft	The extent to which a legitimate user's physical item is used by another individual for authentication.
	No-trusted-third-party	The degree to which the scheme is not dependent on reliable third parties for authenticating the user.
	Requiring-explicit-consent	The cases that authentication process requires clear consent of users to start.
	Unlinkable	The extent to which colluding verifiers cannot find out, from the authenticator itself, whether the identical user is authenticating to both.
Deployability		
	Accessible	The degree to which special physical conditions such as disabilities prevent users from using the system.
	Negligible-cost-per-user	The extent to which the entire cost of the system per user is insignificant. This includes the cost at both verifier and prover side.
	Server-compatible	The degree to which providers have to modify the current authentication setup to support the new system.
	Browser-compatible	The extent to which the scheme is compatible with typical web browsers, without requiring extra software.
	Mature	The degree to which the scheme can be used for real authentication intentions, and not only research. It is important to consider how many organizations adopted the scheme so far, and how much literature is available on that.
	Non-proprietary	The case that the scheme is not under patent, or there is no need to pay royalties for using or implementing it.

Besides all the changes inside the organization, IT also changes the way organizations compete in an industry (McFarlan 1984). In the hypercompetitive business environment, it is more

critical for organizations to set up signaling strategies in order to distinguish their services and goods, and persuade prospective customers to consider their organizations (Ang and Cummings 1997; Hsu et al. 2012). Adopting and implementing new technologies and innovations turns out to be the essential means of reducing and managing uncertainties and gaining competitive advantage for organizations (Dewett and Jones 2001; Thompson 1967). However, as the competition becomes more intense among the organizations that are active in an industry, the likelihood of successful implementation of such innovations decreases (Yoon and Lilien 1985). Thus, precise evaluation of a system's features becomes more important for organizations which are active in business environments with higher levels of competition. We believe that such changes in both internal and external environments have moderating roles in the effect of organizational characteristics on intentions to adopt.

1.3.3.1.IT Intensity

The use of information technology in organizations causes fundamental changes in organizational structure. Organizations with high level of IT intensity are more likely to rely on information technologies which support their business processes. How well information systems are integrated with business operations and infused into users' daily jobs are more likely to impact the productivity of the organization. Moreover, IT intensity positively affects the ability of organizations of understanding, engaging and applying information technology knowledge in their routine processes (Han et al. 2011). This understanding adds to the value of the organization by accelerating the creation of new products and services based on novel information technologies (Mittal and Nault 2009; Farrell 2003). Having and using more IT-enabled business processes and services gives organizations an opportunity to obtain further experience in adopting new technologies.

Furthermore, as IT intense organizations have more IT-related products and process innovations (Héroux and Fortin 2016; Bresnahan et al. 2002), the number of ways to illegitimately enter the system and possibly harm the information and system—so-called attack surface (Manadhata 2008; Manadhata and Wing 2011)—is expected to be larger. Since the attack surface of a system is a metric of its security, systems with larger attack surface are more vulnerable (Manadhata 2008; Boyer and McQueen 2008). Consequently, securing such systems would be more demanding. Security could be a more important concern for organizations with higher levels of IT intensity compared to the ones with lower levels.

1.3.3.2.Competitive Pressure

Dynamic forces of external environment and competitive pressures affect organizations' decision-making procedures (Pfeffer and Leblebici 1973) such as gaining a competitive advantage and obtaining long-term accomplishments (Porter 2011; Mburu 2015). Competitive pressure, also known as external pressure, is one of the significant drivers of diffusion of innovation in literature (Grover 1993; Thong 1999b). It refers to the degree of pressure that the company feels from its competitors within the industry in adopting an innovation (Zhu and Kraemer 2005). This pressure and fear of losing competitive advantage is the result of the circumstances of the industry where the organization is active (Elbertsen and Reekum 2008).

Information leakage and security breaches can cause a loss of competitive advantage (Goel and Shawky 2009) such as damage in customers' confidence and trust, a decrease in organization's profits and productivity, a loss of reputation (Kannan et al. 2007), and a drop in market value (Gordon and Loeb 2002; Cavusoglu et al. 2004). In order to protect information assets and minimize the consequences of losing them, organizations normally establish and implement technical and managerial solutions and innovations (Goel and Shawky 2009).

Organizations adopt and implement novel authentication systems as one of the major solutions to improve information security (Liao et al. 2006). As the competition becomes more intense in the industry, the likelihood of successful implementation of such innovations decreases (Yoon and Lilien 1985). Consequently, it is more important for organizations that are active in high competitive industries to carefully evaluate the system's features and therefore, assign additional weight to them while evaluating different options and making decisions.

1.4.HYPOTHESES DEVELOPMENT

1.4.1. Role of Perceived Usability, Deployability and Security

Usability features focus on how effortless it is for users to learn and operate the authentication systems in their daily jobs (Geraci et al. 1991). If an authentication system is more usable, it takes users less time and effort on the process of authentication. Moreover, the chance for users to face errors is lower. Thus, the required amount of effort to learn and work with the system decreases, and users' productivity is less likely to be influenced by the authentication system (Preece 2001). This encourages decision makers to choose a highly usable authentication system as introducing the system into an organization will not be at the cost of organization's work productivity and operational efficiency. In other words, if decision makers perceive an authentication system to be more usable, they are more likely to adopt it in their organization. Therefore, we propose:

H1. Perceived usability of an authentication system is positively related to intention to adopt the system.

To successfully implement and realize the benefits of new technologies, the technology shall be compatible with the existing infrastructure in the organization (Morton 1991; Yusof et al. 2008). Deployability focuses on assessing the degree to which a new system can be fitted to the

existing infrastructure in the context of a particular organization. It is mostly related to implementation risks and costs (Bonneau et al. 2012). As an authentication system is more deployable, it is more compatible with the organization's infrastructure and resources. Consequently, the risk of implementation failure, as well as implementation costs, should be lower. So, if decision makers perceive an authentication system as more deployable, the likelihood of adoption should be higher among organizational decision makers. Therefore, we propose:

H2. Perceived deployability of an authentication system is positively related to intention to adopt the system.

Perceived security reflects the degree to which decision makers believe that the system is safe against various cyberattacks. One of the main purposes of the authentication process is to assure information security (Reid 2004; Tipton and Krause 2003; Alhussain and Drew 2012). Thus, it is important for organizations to consider security features when adopting a new authentication system. More secure systems are expected to be more resilient to different attacks from both legitimate and non-legitimate users. At the same time, the risk of observing, keeping and manipulating users' accounts would be lower in these systems (Bonneau et al. 2012). Thus, the chance for an organizational data breach, or other security incidents, will be lower with a highly secure authentication system. Therefore, if decision makers perceive an authentication system to be more secure, they may have a higher intention to adopt it in their organization. Thus;

H3. Perceived security of an authentication system is positively related to intention to adopt the system.

1.4.2. Moderating Role of IT Intensity

Organizations with higher IT intensity rely more on IT in their services and business processes (Héroux and Fortin 2016; Bresnahan et al. 2002). As a result, authentication systems are

more frequently used to carry out business operations. Compared to organizations with a lower IT intensity, work productivity of those with higher IT intensity is more likely to be contingent on how their IT resources can be accessed and used efficiently; and usability of the authentication system could be more important for organizations with a higher IT intensity. Thus, we hypothesize:

H4a. The effect of perceived usability on intention to adopt an authentication system is stronger for organizations with a higher level of IT intensity than ones with a lower level of IT intensity.

To successfully install, test, and implement an authentication information system in an organization, such a system should be adaptable to the organization's infrastructure (DeLone and McLean 2003). Organizations with high IT intensity have more projects, systems, and applications that support their business. Such organizations may experience higher risk and loss of productivity due to incompatibility. As a result, organizations with higher levels of IT intensity may consider deployability to be more important while choosing an authentication system for their organizations. Thus, we hypothesize:

H4b. The effect of perceived deployability on intention to adopt a new authentication system is stronger for organizations with a higher level of IT intensity than ones with a lower level of IT intensity.

Organizations with higher IT intensity have and use more IT-based products and services (Bresnahan et al. 2002). Consequently, such organizations may be more likely to encounter information security breaches and data theft as their attack surface is larger (Manadhata 2008; Manadhata and Wing 2011). In other words, organizations with a higher level of IT intensity are more vulnerable to security attacks (Manadhata 2008; Boyer and McQueen 2008); thus, they may be more conscious of the security feature of an authentication system. So, we hypothesis:

H4c. The effect of security on intention to adopt a new authentication system is stronger for organizations with a higher level of IT intensity than ones with a lower level of IT intensity.

1.4.3. Moderating Role of Competitive Pressure

Usable authentication systems require less time and effort to learn and work with. Moreover, productivity of users will be less affected by usable authentication systems (Preece 2001). This will also decrease the user resistance, which can affect an organization's operational efficiency and productivity. As the industry becomes more competitive, it is more critical for organizations to minimize the likelihood of reduction in their productivity and effectiveness. Therefore, as organizations experience more competitive-related pressure, usability becomes more important in their decision to adopt a new authentication system. Thus, we hypothesize:

H5a. The effect of perceived usability on intention to adopt an authentication system is stronger for organizations that experience a higher level of competitive pressure than the ones experiencing a lower level of competitive pressure.

Moreover, if the new system is not fully compatible with the organization's infrastructure, the likelihood of failure in installation, testing, and implementation phases increases (DeLone and McLean 2003). Since organizations normally adopt and implement authentication systems to bring competitive advantage to organizations (Kankanhalli et al. 2003), such failure can lead to losing competitive advantage and reducing market share. For organizations that are experiencing a higher level of competitive pressure, the costs of failure would be greater. As a result, if the system fails to continue functioning due to deployability issues, the consequences would be higher for organizations active in higher levels of competition. Thus, we hypothesize:

H5b. The effect of perceived deployability on intention to adopt an authentication system is stronger for organizations that experience a higher level of competitive pressure than the ones experiencing a lower level of competitive pressure.

Investing in effective and efficient security management techniques can bring a competitive advantage to organizations (Kankanhalli et al. 2003). Organizations generally adopt a novel authentication system in order to gain a competitive advantage. Data and information breaches can destroy the reputation of companies, and a positive reputation of cyber security brings a precious commodity to organizations among the others who are active within the industry (Cooper 2015).

As the competition become more intense, the chance of success in adopting and implementing new innovations decreases (Yoon and Lilien 1985). In industries with a competitive environment, facing security breaches and data theft could lead to loss of competitive advantage and leverage in the market, which highlights the importance of security features. Accordingly, it becomes more important for organizations that are facing higher competitive pressure to ensure that the system is preventing or handling threats and vulnerabilities more effectively. So, we hypothesize:

H5c. The effect of perceived security on intention to adopt an authentication system is stronger for organizations that experience a higher level of competitive pressure than the ones experiencing a lower level of competitive pressure.

Figure 1.2 depicts the research model.

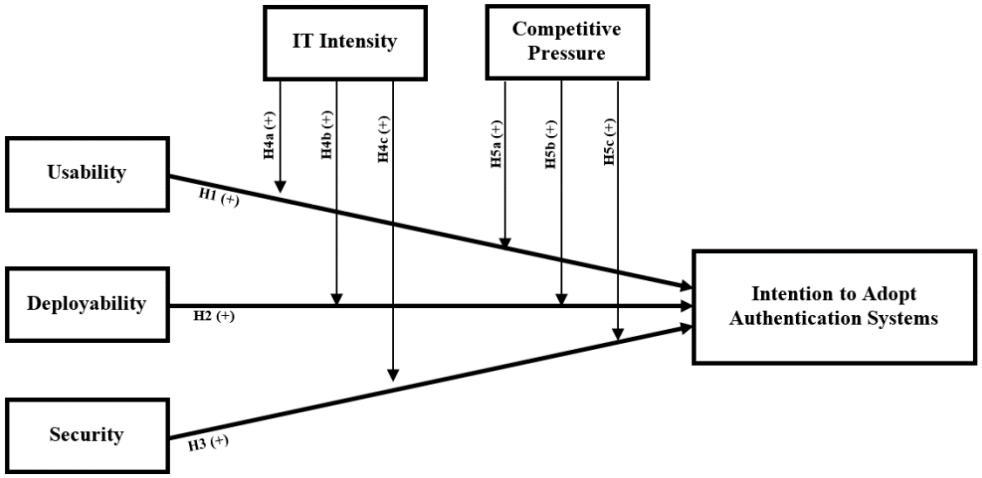

Figure 1.2. Research Model

1.5.RESEARCH METHODOLOGY

1.5.1. Instrument Development

To empirically test the hypothesized model, we developed an online survey. The questionnaire was reviewed by information security faculties and Ph.D. students to ensure content validity. Minor revisions were carried out based on their feedback. To measure "intention to adopt", "deployability", "security" and "usability", two different scenarios were developed and randomly presented to a respondent with the aim of increasing variance among responses. Each scenario describes one authentication system that was developed in research labs, but not yet adopted by any organization. We used a five-point Likert scale for all items. Please refer to Appendix for the scenarios.

At the end of each scenario, respondents were asked their perception of the usability, deployability and security of the described system, and their intention to adopt the system in their organization. Regarding the dependent variable, measures of intention to adopt were adapted from Venkatesh et al. (2003) and Herath & Rao (2009) and modified to fit the context of our study. Measures for usability, deployability and security were based on Bonneau et al. (2012). Items for

IT intensity were from Thong & Yap (1995). Items for competitive pressure were adapted from Grandon and Pearson (2004) and Lin (2006). Table 1.2 summarizes all items. In order to verify the content validity and smoothness of the instrument and measures, a pilot study was conducted using MIS master students in a southwest university in the United States in exchange for course credit. Results were used to make minor changes to the measures and arrangements of the questions.

1.5.2. Sample and Data Collection

The main data collection was conducted through Qualtrics panel services via an online survey hosted by the Qualtrics website. Respondents were full-time employees who have some technical knowledge about authentication systems and security management in an organization. All the respondents should have more than three years of working experience as an IT professional. We assumed that they have enough technical expertise to distinguish which authentication system best fits their organization, and are likely to influence security solution adoptions in their organization. A total of 193 data points were collected.

Around 60% of respondents were male, about 80% were with an age range of 25 to 54. Furthermore, nearly 70% had more than five years of work experience. Table 1.3 summarizes the key demographic variables of the respondents as well as their title and years of work experience in their current organization. Moreover, respondents represent a range of organizations from different industries; about 45% were from organizations with more than 1,000 members, while more than 50% were from organizations older than 26 years. Table 1.4 summarizes this information.

Table 1.2. Instrument Items

Construct	Items	Reference(s)
	Dependent Variable	
Intention to Adopt	• Adoption1: It is my intention to support my organization in adopting such an authentication system. • Adoption2: I am in favor of adopting such an authentication system in my organization. • Adoption3: I am likely to support adopting such an authentication system in my organization.	(Venkatesh et al. 2003, Herath and Rao
	Independent Variables	
Usability	• Usability1: Using this scheme for five to ten accounts is easier than using passwords for those accounts. • Usability2: The scheme is easy to learn. • Usability3: The login time is relatively short. • Usability4: The chance of a user not being able to log in is low. • Usability5: Overall, I found the scheme to be usable. • *It is easy for users to remember secrets for authentication in the scheme. • *Users do not need to worry about carrying additional physical objects like electronic devices, mechanical keys, or pieces of paper in the scheme. • *The login process does not require any more physical efforts for users than pressing a button. • *The scheme provides an easy way to authenticate if the credential is forgotten or the token is lost.	(Bonneau et al. 2012)
Deployability	• Deploy1: The scheme has negligible cost per user. • Deploy2: My organization would not need to change existing setups to support the scheme. • Deploy3: The scheme can be easily made compatible with typical web browsers. • Deploy4: The scheme can be deployed on a large scale for actual authentication purposes. • Deploy5: Overall, I found this authentication scheme deployable in an organization. • *The scheme is accessible to users who are able to use passwords. • *The scheme is not under patent, or I am not going to pay royalties for using or implementing it.	(Bonneau et al. 2012)
Security	• Security1: With this scheme, an attacker cannot impersonate users after observing them authenticating into the system. • Security2: It is impossible for an acquaintance or skilled investigator to impersonate a specific user by exploiting personal knowledge. • Security3: The system is resilient to unlimited password guessing attacks. • Security4: The system is resilient to possible internal observations attacks like key-logging. • Security5: The system is resilient to phishing attacks. • Security6: The scheme is resistant to leaks of other secret information. • Security7: Overall, I found the scheme resilient to security threats. • *The system is resilient to limited guessing attacks. • *The scheme does not rely on any kind of trusted third party (other than the prover and the verifier) for authenticating the user. • *The authentication process cannot be started without the explicit consent of the user.	(Bonneau et al. 2012)
	Moderators	
IT intensity	• Intensity1: My organization is dependent on up-to-date information technology. • Intensity2: It is very important for my organization to have access to reliable, relevant and accurate information technology. • Intensity3: It is very important for my organization to access IT systems quickly.	(Thong and Yap 1995)
Competitive Pressure	• CompPres1: My organization has experienced competitive pressure to implement innovative information security measures. • CompPres2: My organization will experience a competitive disadvantage if innovative information security methods are not adopted. • CompPres3: Competition is a factor in our decision to adopt innovative security measures. • CompPres4: Our industry is pressuring us to adopt innovative security measures.	(Lin 2006, Grandon and Pearson 2004)

* items were dropped due to loadings lower than 0.7.

Table 1.3. Key Demographic Variables, Title, and Work Experience of Respondents

	Variable	Percent		Variable	Percent
Age	18 to 24 years	0.5%	***Race***	White/ Caucasian	76.2%
	25 to 34 years	26.9%		African American	4.7%
	35 to 44 years	25.9%		Hispanic	6.2%
	45 to 54 years	25.4%		Asian	10.9%
	55 to 64 years	19.7%		Native American	1%
	65 years and over	1.6%		Pacific Islander	1%
Education	Less than High School	0%	***Title***	President, Owner, or Managing Director	4.1%
	High School / GED	3.1%		CIO/CTO/VP of IS	11.9%
	Some College / Bachelor's degree	43.5%		IS Manager, Director, Planner	31.1%
	Master's degree	43%		Other manager in IS department	18.1%
	Professional degree	8.8%		Business Operations Manager	1.0%
	Doctoral Degree	1.6%		Administration/Finance Manager	1.0%
				Other	32.6
Income	Less than 20k	0%	***Work Experience***	Less than a year	3.6%
	20K to 40K	3.6%		1 to 3 years	9.3%
	40K to 60K	12.4%		3 to 5 years	18.7%
	60K to 80K	20.7%		5 to 10 years	34.2%
	More than 80K	63.3%		More than 10 years	34.2%
Gender	Male	59.6%			
	Female	40.4%			

Table 1.4. Industry, Size and Age of Organizations

	Variable	Percent
Org Size	Less than 100 employees	12.4%
	100 – 400 employees	19.2%
	401 – 700 employees	12.4%
	701 – 1000 employees	11.4%
	More than 1000 employees	44.6%
Org Age	Less than 5 years	1.6%
	5 to 10 years	12.4%
	11 to 15 years	13.0%
	16 to 25 years	20.7%
	More than 26 years	52.3%
Industry	Education	8.3%
	Finance	11.4%
	Wholesale/Retail	10.9%
	Healthcare	7.8%
	Construction	3.1%
	Insurance	2.6%
	Other	56%

1.5.3. Measurement Model

To evaluate the measurement model, a confirmatory factor analysis (CFA) was conducted. Results are summarized in Table 1.5. All of the latent constructs are modeled to be reflective. For each latent construct, path loadings, t-statistic, and standard error were calculated. At alpha level of 0.05, all the measures' path loadings are significant with a value more than 0.7 (Chin and Marcolin 1995), indicating that more than 50% of the variance is shared between each construct's items (Chin 1998). To examine the convergent validity, composite reliability and average variance extracted (AVE) were obtained (Hair et al. 1995). All of the constructs met the acceptable score of 0.5 for AVE, thereby confirming their reliability (Fornell and Larcker 1981). Moreover, values of composite reliability are between 0.889 and 0.957.

The square root of AVE was also used to verify the discriminant validity (Fornell and Larcker 1981). Results are shown in Table 1.6. For each latent construct, the square root of the AVE is higher than all its cross correlations. Moreover, higher values of inter-construct correlations confirm the greater variance among each construct's specific measures compared to other measures (Gefen et al. 2000). All things considered, we can confirm all the indicators in the measurement model are valid through their constructs.

As the data was collected in a single survey, common method variance (CMV) could be a concern (Podsakoff et al. 2003). We conducted Harman's single factor test (Podsakoff and Organ 1986) to determine the extent of this issue. According to this approach, with a factor analysis, if only a single factor arises, or a factor explains the majority of variance among all the measures, we can conclude that CMV is a significant issue in the sample (Podsakoff et al. 2003). After conducting an exploratory factor analysis among all the items, we obtained seven factors that explained more than 70% of the variance. All extracted factors had an eigenvalue greater than one,

and the highest factor accounted for only 33% of the variance. This indicates CMV is not a serious concern in this dataset.

1.5.4. Structural Model

The results of data analysis, including R-squares, standardized path coefficients, associated t-values and paths significance, are depicted in Figure 1.3. To test the significance of path coefficients in the structural model, we used a bootstrapping approach with 1,000 resamples. The R-square value of intention to adopt new authentication systems is 0.548, indicating that nearly 55% of the variance in intention to adopt can be explained by security, deployability and usability. Because this amount of variance is more than 10 percent, we can claim that the proposed model is valid and acceptable (Falk and Miller 1992).

Table 1.5. CFA Results

Construct	Item	Loading	t-Statistic	Standard Error	Average Variance Extracted (AVE)	Composite Reliability	Cronbach's Alpha
Intention to Adopt	*Adoption1*	0.922	69.033	0.013	0.882	0.957	0.933
	Adoption2	0.948	99.845	0.009			
	Adoption3	0.947	112.542	0.008			
Deployability	*Deploy1*	0.731	16.866	0.043	0.617	0.889	0.845
	Deploy2	0.758	19.373	0.039			
	Deploy3	0.783	21.489	0.036			
	Deploy4	0.827	27.876	0.030			
	Deploy5	0.824	31.422	0.026			
Security	*Security1*	0.728	17.697	0.041	0.570	0.913	0.891
	Security2	0.724	14.203	0.051			
	Security3	0.763	20.041	0.038			
	Security4	0.744	14.767	0.050			
	Security5	0.712	12.677	0.056			
	Security6	0.821	28.029	0.029			
	Security7	0.848	35.124	0.024			
Usability	*Usability1*	0.759	27.771	0.027	0.620	0.891	0.847
	Usability2	0.818	27.640	0.030			
	Usability3	0.738	17.616	0.042			
	Usability4	0.763	19.547	0.039			
	Usability5	0.855	40.373	0.021			
IT Intensity	*Intensity1*	0.802	14.915	0.054	0.747	0.898	0.830
	Intensity2	0.888	28.327	0.031			
	Intensity3	0.899	37.579	0.024			
Competitive Pressure	*ComPres1*	0.836	22.748	0.037	0.680	0.895	0.846
	ComPres2	0.813	21.815	0.037			
	ComPres3	0.839	22.602	0.037			
	ComPres4	0.811	15.549	0.052			

Table 1.6. Matrix of Latent Constructs' Correlations

Construct	Means (S.D.)	1	2	3	4	5	6
1. Intention to Adopt	3.498 (0.982)	**0.939**					
2. Competitive Pressure	3.387 (0.917)	0.449	**0.825**				
3. Deployability	3.536 (0.767)	0.588	0.440	**0.786**			
4. IT Intensity	4.441 (0.577)	0.380	0.365	0.329	**0.864**		
5. Security	3.604 (0.760)	0.487	0.178	0.453	0.225	**0.755**	
6. Usability	3.753 (0.782)	0.674	0.376	0.606	0.326	0.480	**0.788**

Shaded cells in the diagonal row are AVE square roots.

The results of testing direct relationships indicate that usability (β= 0.430, $p<0.001$), deployability (β= 0.211, $p<0.01$), and security (β= 0.171, $p<0.05$) have significant effects on intention to adopt, which supports H1, H2, and H3. To account for individual differences in the proposed model, we counted on the literature and controlled for the effect of the responders' age, education level, gender, and income (Hsu et al. 2012; Venkatesh et al. 2003). None of these variables had significant effect on intention to adopt new authentication systems.

Moreover, to test the moderating effects, a construct was created by cross-multiplying all the items of appropriate constructs, standardized to avoid multicollinearity, and included in the main model (Toothaker 1994). This approach is called product-indicator (Chin et al. 2003). Our results show that IT intensity positively moderates both the relationship between usability and intention to adopt (β= 0.225, $p<0.01$) as well as between security and intention to adopt (β= 0.213, $p<0.05$). These support H4a and H4c. IT intensity, however, does not significantly moderate the effect of deployability on intention to adopt (β= 0.068, t-statistics= 0.783). Therefore, we do not have enough evidence to support H4b.

Moreover, competitive pressure negatively moderates the relationship between usability and intention to adopt (β= -0.118, $p<0.01$), and positively moderates the effect of deployability on intention to adopt (β= 0.155, $p<0.05$). However, the moderation effect of competitive pressure on

the relationship between security and intention to adopt is not statistically significant (β= 0.085, t-statistics= 1.523). Thus, although H5b is supported, we don't have enough evidence to support H5a and H5c.

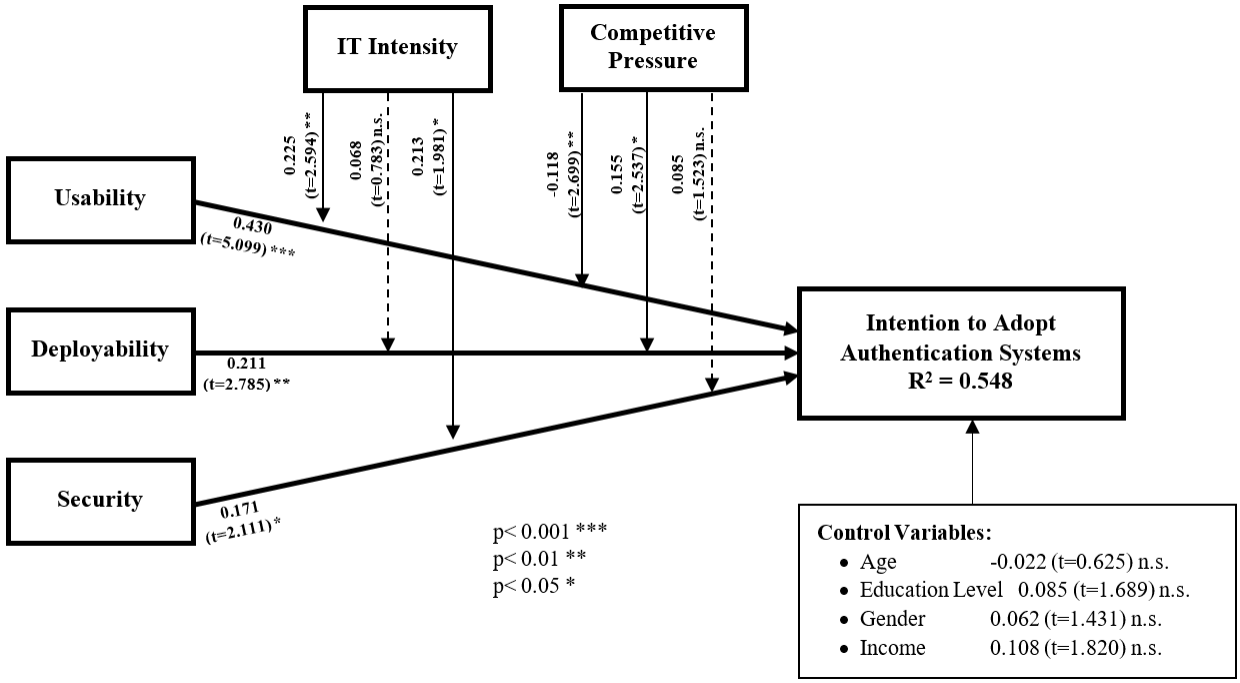

Figure 1.3. Results of PLS

1.5.5. Partial Least Square-Multi Group Analysis (PLS-MGA)

In order to find out whether there is a significant difference in the path coefficients of our two different scenarios, partial least square-multi group analysis (PLS-MGA) was conducted in SmartPLS 3. Henseler's PLS-MGA uses percentile bootstrapping method in order to discover the difference among the two proposed scenarios (Henseler et al. 2009; Sarstedt et al. 2011). Table 1.7 summarizes the differences in the path coefficients and P-values of comparisons among two scenarios.

P-values smaller than 0.05 and higher than 0.95 point toward the significant difference of a particular path coefficient among groups at 5% error level (Henseler et al. 2009). P-values

smaller than 0.05 indicate that the results of bootstrapping for first scenario is higher than the second. However, p-values higher than 0.95 point out that the results of bootstrapping for the second scenario is higher than the first (Henseler et al. 2009).

According to Table 1.7, the effect of deployability on intention to a adopt novel authentication system in second scenario is higher than the first one. Conversely, the effect of security features on intention to adopt authentication system is stronger for the first scenario compare to the second one.

Table 1.7. PLS-MGA Test Results

Path	First Scen Path (n=96)	Second Scen Path (n=97)	Path Coefficients' Difference	P-Value	$t_{Parametric}$	$t_{Welch\text{-}Satterthwaite}$
H1	0.431(3.381)	0.416(4.006)	0.016	0.456	0.095	0.095
H2	-0.097(0.682)	0.435(4.353)	0.532	0.999*	3.106	3.101
H3	0.465(4.905)	-0.101(1.348)	0.566	0.000*	4.723	4.717
H4a	0.047(1.002)	0.048(1.064)	0.033	0.644	0.329	0.328
H4b	0.127(1.941)	0.136(2.188)	0.072	0.245	0.691	0.691
H4c	0.106(1.868)	0.111(1.937)	0.074	0.749	0.649	0.649
H5a	0.151(2.680)	0.157(2.576)	0.032	0.364	0.347	0.347
H5b	0.116(1.980)	0.123(2.198)	0.076	0.780	0.731	0.731
H5c	0.055(0.953)	0.058(1.030)	0.048	0.692	0.414	0.414

* Significant at 0.05 (two-tailed, 5,000 bootstraps)

1.6. DISCUSSION

This study explores the impact of innovation characteristics of an authentication system on decision makers' intention to adopt, from a choice and decision making perspective. Our findings show that perceived usability, deployability, and security of an authentication system are important factors that have a positive impact on decision makers' intentions to adopt in their organizations. An interesting finding is that our results point toward a stronger effect of perceived usability and deployability compared to perceived security. This might be due to the fact that novel authentication systems already have minimum security requirements. Therefore, decision makers largely focus on usability and deployability features of those systems and weigh them more in the decision making process.

Additionally, our findings indicate that organizations have different demands for authentication systems due to the extent to which information technology is used in their environment. Decision makers from organizations with a higher level of IT intensity weigh perceived usability and security more than deployability in their adoption decision. In addition, our results point toward the importance of competitive-related pressure on organizations' decision to adopt authentication systems. Organizations which are active in hypercompetitive industries weigh perceived deployability more and a perceived usability less in their adoption decision. Table 1.8 summarizes the hypotheses testing results.

Table 1.8. Summary of Results

Hypothesis	Result
H1. Usability of authentication systems is positively related to intention to adopt these systems.	Supported
H2. Deployability of authentication systems is positively related to intention to adopt these systems.	Supported
H3. Security of authentication systems is positively related to intention to adopt these systems.	Supported
H4a. IT intensity moderates the relationship between usability and intention to adopt authentication systems.	Supported
H4b. IT intensity moderates the relationship between deployability and intention to adopt authentication systems.	Not Supported
H4c. IT intensity moderates the relationship between security and intention to adopt authentication systems.	Supported
H5a. Competitive pressure moderates the relationship between usability and intention to adopt authentication systems.	Not Supported (opposite)
H5b. Competitive pressure moderates the relationship between deployability and intention to adopt authentication systems.	Supported
H5c. Competitive pressure moderates the relationship between security and intention to adopt authentication systems.	Not Supported

The findings of moderating role of competitive pressure on the relationship between usability and intention to adopt is counter to what we hypothesized, in that we theorized that the effect would be positive, and not negative. The opposite was true. The effect is significant but opposite to its predicted direction, suggesting that for organizations which are experiencing a higher level of competitive pressure, the effect of usability on adoption intention is weaker. In hindsight, it seems rational. As competition further intensifies, organizations experience a higher

threat of losing competitive advantage, and their behavior will be stochastic instead of deterministic as their behavior is greatly affected by competitors' actions (Auh and Menguc 2005). Therefore, adopting new technologies acts as a hedonic motivator which diminishes the existing competitive pressure. As a result, organizations should pay more attention to adopting a technology as a mean to lessen a competitive threat rather than considering whether the technology is usable enough for their end users in long term. This also justifies the non-significant results of competitive pressure moderation effect on the relationship between security and intention to adopt.

Moreover, our findings do not suggest a moderating role of IT intensity on the effect of deployability on intention to adopt. Indeed, deployability assesses features of the system that without them the system is unable or less likely to start working. Therefore, it seems logical that regardless of the level of IT embeddedness, decision makers think about this characteristic and evaluate different alternatives in terms of their compatibility with an organization's setting.

1.6.1. Contribution to Theory

Taken together, the contribution of the study is three-fold. First, our study goes beyond applying well-established technology adoption theories such as TAM and diffusion of innovation theory to identify factors that influence intention to adopt new authentication systems. Such theories focus on evaluating a proposed system in terms of its capability to deal with a general threat in the environment. Considering implementation of an authentication system as an organizational innovation, it helped us introduce a decision making perspective in identifying criteria that affects decision makers' intentions to adopt such systems. The results suggest usability of authentication systems is the most important consideration. Our study is a step forward in the trend of uncovering the factors that influence intention to adopt new authentication systems.

Second, we shed light on the significance of environmental features in the adoption of information security management practices. Our findings on moderating variables suggest that the technology characteristic by its own may not be sufficient to ensure the successful adoption and implementation of a specific innovation, particularly organizational-level innovations such as information security management solutions (Dhillon and Backhouse 2001) such as authentication systems.

Our findings point toward the importance of IT intensity, as a significant variable in organizational context, in the relationship between adoption determinants and intention to adopt and implement an authentication scheme. Our results indicate that considering innovation features on their own is not enough to understand the adoption of information security innovations, such as authentication systems. Advanced use of information technology in organizational activities and processes makes fundamental changes in organizations' structure (Han et al. 2011). Neglecting the degree to which IT is embedded in an organization's processes and products may result in less ideal choices and increase the chance of potential costs and risks for the organization. Further, the findings of this study highlight the role of competitive pressures on decision making processes. Hypercompetitive marketplace and high uncertainty in organizations' external environment can majorly alter the way decision makers evaluate different features of innovations, and diminish the importance of technical characteristics on final decisions.

And finally, from the information security literature point of view, we proposed a framework beyond the existing, well-established theories available to predict organizations' intentions to adopt and implement new security tools. This study is one of the first studies to focus on the specific features of the security innovation and argues those as the key factors affecting an adoption decision. Such frameworks are important in the context of information security, because

the consequences of failure in adoption and implementation could lead to security incidents. Our framework is a significant move toward proposing innovation-specific and more applicable theories which explain security management practices (Hsu et al. 2012).

1.6.2. Implications for Practice

This study also has several implications for practice. First, results can help managers and executives have a better understanding of key criteria and factors in adopting a new authentication system for their organization. For designers, it is important to design a system with high usability, the most important factor. Second, understanding the impact of key features of authentication systems can help designers and developers figure out organizations' expectations of modern authentication systems. This will push them to make an effort to match their products with market expectations. This is mostly helpful and applicable on the markets that are hypercompetitive, and as a result, have more uncertainty. By proactively assessing the market environment, and considering the importance of such factors in designing, inventors and organizations have a chance to gain competitive advantages.

Finally, the research findings highlight the importance of IT intensity and competitive pressure in the decision making process. Along the lines of previous studies (i.e. (Ang and Cummings 1997)), our findings highlight the fact that managers should consider IT intensity and competitive pressure as major decision-making moderating variables. Being more conscious of organizational contexts like IT intensity and competitive pressure gives organizational decision makers a larger perspective on how to effectively choose and adopt an information security innovation. Moreover, being aware of the effect of IT intensity and competitive pressure might help marketing managers suggest more suitable authentication systems, or offer organizations a customized version of their product.

1.6.3. Limitations and Future Research

This study has several limitations. First, respondents are limited to employees in the United States, which raises the possibility of external validity issue. We have to be more cautious about interpreting and duplicating the results in the context of other countries. Secondly, we did not take into account the type of industry and the degree of data sensitivity for the organizations. The sensitivity of data stored in an organization, and the industry which an organization belongs to might play important roles in adoption decisions. Future studies can improve this framework by testing these constructs. And finally, according to the obtained coefficient of determination, there are still some variances in the intention to adopt authentication systems that are unexplained. This also presents a viable future topic of study.

Chapter Two:

IT Professionals' Proactive Information Security Behavior

2.1. INTRODUCTION

Organizations embrace structural changes by incorporating innovative technologies into work routines, and investing in new platforms to keep digital data (e.g., cloud-based computing). Such changes bring new challenges in information security, and likely widen the attack surface in organizations (Kessel and Allan 2015). Organizations have kept increasing investment in resources for information security. In 2016, organizations invested about $75 billion in information security, yet security incidents increased by 38% (The Economist Intelligence Unit 2016).

While it is important to maintain a proper level of investment in security, it matters whether organizations invest proactively or reactively (for example before or after an incident) in influencing security effectiveness (Kwon and Johnson 2014). Proactive information security management refers to the security management practices that focus on dynamically analyzing probable upcoming security threats, evaluating them, and trying to minimize the risk of those threats (Iheagwara et al. 2004). Such practices involve constantly monitoring security attacks and breaches, and neutralizing probable ones before they can harm critical resources in the organization (Kessel and Allan 2015; The Economist Intelligence Unit 2016). Moreover, proactive management in security plays a key role in significantly slowing down the growth of attacks. Recent research on 300 executives who are knowledgeable of cyber-security in their organizations found that proactive security approaches can decrease the number of cyber security breaches and attacks in organizations by 53% (The Economist Intelligence Unit 2016).

This study explores what drives IT professionals to take proactive behavior related to information security in their organizations. We draw upon the prototype/willingness model (Gerrard et al. 2005; Gibbons et al. 2003; Gibbons and Gerrard 1995). The model considers that two modes of decision making affect behavior. The first is a mode of *intention*, which is based on

a rational reasoning system that offers decision makers the opportunity to process and assess information. The second is a *willingness* mode, which is based on a heuristic system, where behavior is a reaction to the conducive situations that enable or accelerate behavior. Accordingly, the first aim of this study is to examine the confluence of 1) rationally thinking about the proactive approaches and 2) being in an encouraging situation that motivates proactive information security behavior. This approach will help us explore the different paths that form proactive behavior, and invest more effectively in the solutions that promote such behavior and improve information security in organizations.

Moreover, decision making in an organization is somehow constrained by the environment (Pfeffer 1982). Environmental forces are powerful enough to modify organizations' strategic decisions (Phillips 1999). So it is essential for decision makers in an organization to be responsive to them, and consider them in their decision making (Wang et al. 2012). The second aim of this study, therefore, is to investigate whether and how the effects of decision makers' intention and willingness to adopt proactive information security behavior varies, given the different levels of dominant environmental characteristics. Exploring the moderating effects of such characteristics gives managers an opportunity to find out the critical role of external environment on the successful adoption and implementation of proactive information security approaches. This will also help them choose the appropriate information security approaches that are readily adaptive to their external environment.

In order to test the hypothesis, data was collected from employees with at least three years of working experience as an IT professional. Our findings suggest that decision makers' rational and heuristic aspects of processing information significantly affect organizations' actual proactive security behavior. Moreover, the positive moderating effect of dominant environmental features

highlights the important role of external environment in organizational behavior. Findings can bring new insights, and help policy makers find new means to promote proactive information security behavior among organizations, considering the level of major features in their external environment.

2.2. LITERATURE REVIEW

Within the information security literature, the concept of proactive behavior is synonymous with preventive or protective behavior. Such concepts can be investigated from two different perspectives, individual users and decision makers. Investigating the factors that affect end users' intention to adopt and continue using proactive information security behaviors has been in the center of attention for scholars in this area. Examples of such behavior are using and updating antivirus software, and retrieving backups frequently (White et al. 2017). For instance, Boss et al. (2015) applied protection motivation theory (PMT) in two information security contexts to find out the factors which influence individuals' intention to use anti-malware software and backup. Warkentin et al. (2016), however, used the same theory along with perceived extraneous circumstances construct to investigate the individual's continued engagement in using anti-malware software as a protective security behavior. Besides PMT, other theories were also used in the literature to explain the underlining motivation of individuals' protective information security behavior (Dodel and Mesch 2017; Ng et al. 2009).

From decision makers' point of view, however, there are not enough studies that investigate what motivates organizations to pursue proactive strategies to secure their information. This study focuses on this gap, and aims to explore such motivators. Moreover, as external environmental features can change decisions and strategies of organizations (Phillips 1999), it is critical for them to dynamically monitor those characteristics and take them into account in their decisions (Wang

et al. 2012). Examining the moderating role of environmental characteristics helps us find out the boundary conditions under which one should frame organizational decisions differently.

2.3. THEORETICAL BACKGROUND

2.3.1. Proactive Information Security Behavior

A growing number of information security attacks and breaches force organizations to make a great effort to create solutions and apply behaviors in order to protect their assets against novel breaches and security problems (Kwon and Johnson 2014; Jong and de Ruyter 2004). Such behaviors typically consist of two components; proactive and reactive (Jong and de Ruyter 2004; Morrison and Phelps 1999; Hartline and Ferrell 1996). In the context of information security, the reactive component focuses on the behaviors that take place after the incident (Kwon and Johnson 2014). Organizations with reactive information security behavior analyze existing breaches (Iheagwara et al. 2004), find creative responses to the security attacks that have already happened, and adjust their behavior accordingly (Jong and de Ruyter 2004). Investing in reactive security behavior gives organizations the opportunity to learn from their failures, and establish defense against probable upcoming ones (Marcellus and Dada 1991).

On the other hand, proactive components concentrate on behaviors that occur prior to the incident (Kwon and Johnson 2014). Organizations with such information security behavior actively analyze and assess security threats and weaknesses that might happen in future, and attempt to lessen the associated risks (Iheagwara et al. 2004). Such organizations have to decide where and by what means they will invest and apply security controls (Kwon and Johnson 2014). Given the fact that proactive methods do not depend on learning from failures in order to find out vulnerable parts of the system, organizations with such behaviors need to foster a better

understanding of information security concepts and concerns, its contributing factors, and industry and government expectations (Kwon and Johnson 2014).

Security professionals believe that since reactive security methods are mainly focusing on existing breaches, they are not appropriate and applicable enough to link the current problems and forthcoming security threats and attacks (Kark et al. 2009; Kwon and Johnson 2014; Pironti 2005). At the same time, using proactive methods is correlated with less failure in security, and investing in such methods is more profitable compared to reactive methods in some industries (Kwon and Johnson 2014). Proactive methods improve organizations' overall effectiveness (Bateman and Crant 1999; Fritz and Sonnentag 2009; Griffin et al. 2007) and help organizations to gain an effective competitive advantage among their rivals in the global economy (Kark et al. 2009; Sonnentag 2003).

In spite of these, since security threats continuously change and become more complex, proactive methods need a great amount of investment in order to get ready for all feasible forms of failure (Rowe and Gallaher 2006). Moreover, extra effort should be used by organizations in order to switch to proactive behavior and stick to it (Frese et al. 1996). As a result, it is essential to encourage organizations to apply proactive information security strategies, and find out what factors predict having such behaviors in organizations.

2.3.2. Prototype-Willingness Model

Decision making is not always based on rational thinking (Hukkelberg and Dykstra 2009; Loewenstein et al. 2001). There has been a considerable amount of interest on developing models –so called dual-processing models- that also explain the less deliberative aspect of decision making (Gerrard et al. 2008). Such models of cognition use two qualitatively distinct systems of information processing to describe the decision making process (Chaiken and Trope 1999; Sloman

1996), and suggest that decision-makers simultaneously engage in both systems (Evans 1984; Reyna and Brainerd 1992; Sloman 1996).

The prototype-willingness model (PWM) is a type of dual-processing model that assumes two modes of decision making and judgement influence behavior (Gerrard et al. 2005; Gibbons et al. 2003). One mode of processing is based on systematic reasoning and rational systems. Since intricate assessment of information slows down the processing procedure, the outcome of this processing is normally delayed decisions (Epstein 2003). This path affect behavior, by means of intention to pursue, is similar to reasoned-choice theories (Hammer and Vogel 2013). PWM primarily establishes this path using theory of reasoned action (Ajzen and Fishbein 1977; Gibbons and Gerrard 1995; Gerrard et al. 2008).

In this path, the PWM considers the reasoned side of decision-making, and assumes that the decision making process consists of taking into account both behavioral options and expected short- and long-term outcomes (Gerrard et al. 2008). Behavior originates in two constructs: first is decision-makers' assessment about what other important organizations do (subjective norms), and the second is the decision-makers' evaluation or attitudes toward the behavior (Hyde and White 2010). Those two determinants proceed to the decision-maker's behavior via intention to pursue, which is commonly defined as goal state (Ajzen 1999).

The second mode of processing is based on heuristic system. Gibbons and Gerrard (1995) believe that besides intention, behavior is also a function of decision makers' response to conducive situations. This path –so called social reaction path- captures decision-makers' unintentional behavior (Gerrard et al. 2008). In such circumstances, decision makers' willingness to pursue, instead of intention to pursue, regulates their behavior.

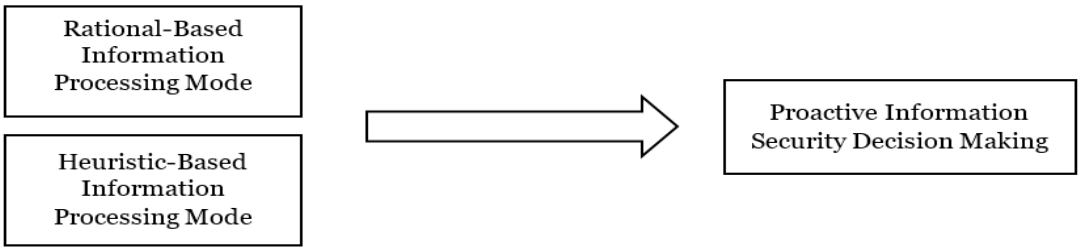

Figure 2.1: Modes of Decision-Making

PWM measures the unintentional side of decision making by willingness to pursue, which is defined as an openness to engage in a particular behavior in a specified social situation (Gerrard et al. 2005; Dohnke et al. 2015; Harper and Hogue 2014). Since it is a reaction to a conductive situation, openness is measured by explaining a hypothetical scenario which does not bring up any peer pressure (Gerrard et al. 2008). PWM believes that under that specific situation, decision makers may take on behaviors that they normally would not consider.

Similar to intention, willingness to pursue is affected by social norms and attitudes (Hammer and Vogel 2013) . However, it is mostly formed by decision makers' assessment of image prototype. This prototype illustrates a cognitive and social representation of the type of organizations who are involved in a specific behavior (Gibbons and Gerrard 1995; Gerrard et al. 2008), and remains in people's longstanding memory (Skowronski and Carlston 1989). Heuristic processing of such images determines whether a decision maker is willing to be involved in a certain behavior (Harper and Hogue 2014). Due to self-enhancement purposes, favorable images of organizations with specific behavior persuade and motivate decision makers to adopt such behaviors to match or become more similar to those organizations (Dunning et al. 1991; Hammer and Vogel 2013; Niedenthal et al. 1985).

In summary, PWM gives us an opportunity to clarify decision-making procedures with more detail (Todd et al. 2016; Stock et al. 2013; Davies et al. 2013). Similar to other dual-process

models, this model suggests that although willingness and intention are correlated, the paths are distinct and performed simultaneously and independently (Epstein and Seymour 1994; Van Gool et al. 2015; Hammer and Vogel 2013; Rivis et al. 2006; Gerrard et al. 2008). PWM has been successfully used to a range of both health-promoting and -risk behaviors (Rivis et al. 2006; Todd et al. 2016), and will be used as the primary theory in this study.

2.3.3. Role of Environmental Factors

Although deciding to apply technological and behavioral innovations in an organization is made by those who have organizational authority to make decisions, organizational behavior is also constrained by the demands in the environment (Pfeffer 1982). The external environment is the source of both threats and opportunities (Lenz 1980), and environmental characteristics are powerful enough to modify organizations' strategic plans, decisions and performance (Phillips 1999). Therefore, it is essential for organizations to actively consider those characteristics in their decision making process (Wang et al. 2012).

In this study, we focus on three dominant environmental factors, environmental uncertainty, competitive pressure, and regulatory environment; and we investigate how these factors can change the effect of decision-makers' intention and willingness to pursue an organizations' proactive information security behavior.

2.3.3.1. Environmental Uncertainty

Uncertainty is a circumstance where it is hard to predict the chance of different upcoming events (Gaur et al. 2011; Milliken 1987; Sutcliffe and Zaheer 1998). Coping with uncertainty is one of the essential skills that organizations are required to have in order to survive in the competitive environment (Duncan 1972; Milliken 1987). Environmental uncertainty is defined as the extent to which the external environment of an organization is unpredictable and experiences

unanticipated changes regarding technology, actions of competitors, and consumers' behavior (Keats and Hitt 1988; Fynes et al. 2004). In the context of information security, environmental uncertainty reflects the unpredictability of probable security threats and risks that are caused by using technologies which enhance organizations' effectiveness and proficiency (Hsu et al. 2012; Straub et al. 2008).

As the environment becomes more ambiguous and uncertain, decision makers are more likely to base their actions on their personal references (Carpenter and Fredrickson 2001; Finkelstein and Hambrick 1996). At the same time, inaccurate decisions have more serious consequences for organizations, and the chance of survival is lower in environments with higher uncertainty compared to the lower (Waldman et al. 2001). In such situations, decision makers perceive themselves as less capable of understanding and controlling the direction and effects of environmental changes on their organizations (Milliken 1987), and as a result, are less confident in their prediction of upcoming events (Anderson and Tushman 2001). The more decision makers observe uncertainty in their organizations' external environment, they are more likely to establish new technologies and strategies to support their organization in coping with such uncertainty (Gordon and Miller 1976; Gordon and Narayanan 1984; Hayes 1977).

As organizations' external environments become more dynamic and unstable, the possibility of being threatened would be higher (Sung and Choi 2012). Moreover, when the level of uncertainty increases in organizations, excessive amounts of technical and strategic information will emerge (Tsai and Huang 2008), resulting in a wider attack surface. This makes organizations more vulnerable to security attacks and breaches (Boyer and McQueen 2008; Manadhata 2008).

2.3.3.2. Competitive Pressure

Dynamic forces of external environment and competitive pressure also affect organizations' decision-making procedures (Pfeffer and Leblebici 1973) in a way to line up with gaining competitive advantage and obtaining long-term accomplishments (Mburu 2015; Porter 2011). Competitive pressure, also known as external pressure, is one of the significant drivers of diffusion of innovation in literature (Grover 1993; Thong 1999c). It refers to the degree of pressure that the company feels from competitors within the industry in adopting an innovation (Zhu and Kraemer 2005). This pressure and fear of losing the competitive advantage is the result of the circumstances of the industry where the organization is active (Elbertsen and Reekum 2008).

As the business environment becomes more competitive, organizations increasingly realize the importance of adopting and implementing strategies which distinguish their organization's services and products from its rivals. Such strategies give organizations the chance to highlight their significant presence to both their prospective customers and other important market participants (Hsu et al. 2012), by changing competition rules, or altering competitive landscape (Porter and Millar 1985). Therefore, in hypercompetitive industries, competitive pressure forces organizations to gain and keep their competitive advantage among other competitors (Zhu and Kraemer 2005).

In the context of our study, investing in effective security management strategies can lead organizations to gain competitive advantage and prevent competitive decline (Kankanhalli et al. 2003). Thus, investing in proactive information security strategies helps organizations which are active in hypercompetitive industries to lessen the amount of pressure. This is an extra motivator for organizational decision makers, and has a stronger intention and openness to adopt proactive information security approach on the actual behavior.

2.3.3.3. Regulatory Environment

The regulatory environment is one of the critical and dominant factors that should be explored while examining the role of the environment (Zhu et al. 2006). It consists of government laws, regulations, and policies (Chen 2007). Well-designed government regulations enhance organizations' understanding of issues in the environment, and decrease uncertainties regarding environmental investment (Porter and Linde 1995; Karagozoglu and Lindell 2000). Furthermore, as government regulations become more flexible, assessment of opportunities and risks in the environment play a more important role in the origination and development of organizational strategies (Maxwell 1996; Rondinelli and Vastag 1996).

In the context of proactive information security behavior, a supportive regulatory environment points toward flexibility of regulations in the adoption and implementation of this new behavior in order to provide incentives and meet goals in promoting proactive strategies in organizations (Porter and Linde 1995). Organizations operating in an environment that the government regulations are less supportive have lower flexibility in implementing innovative technological and behavioral solutions (Karagozoglu and Lindell 2000). Regulations do not make technological and behavioral innovativeness happen by themselves (Karagozoglu and Lindell 2000). Flexibility in supportive regulations, however, provides extra motivation for decision makers, and strengthen the effect of their intention and openness to adopt proactive information security approach on the actual behavior.

2.4. HYPOTHESIS DEVELOPMENT

2.4.1. Rational-Based Decision Making

Following Ajzen and Fishbein (1980), we propose that decision makers' attitudes towards proactive information security approaches positively affects their intention to engage in such

approaches. Attitude is defined as the extent to which decision makers feel positively about the proactive information security behavior (Bock et al. 2005). Decision makers effectively evaluate positive and negative consequences of the behavior, and form their behavior based on this evaluation (Komiak and Benbasat 2006). As decision makers have a more positive feeling about the proactive behavior, they will concentrate more on the benefits, and perceive the benefits of that behavior to outnumber the associated costs (Van Gool et al. 2015). Thus, we hypothesize:

H1. Positive attitudes toward a proactive information security approach is positively related to intention to pursue such an approach in organizations.

Moreover, effective others have a positive influence on forming decision makers' intentions to adopt proactive information security approaches. Normally, adopting a new strategy or innovation aligns with uncertainty about upcoming consequences for probable adopters (Lu et al. 2005). In order to decrease this uncertainty, decision makers tend to monitor influential peers and integrate the collected information to their own cognition (Katz and Tushman 1979; Burkhardt and Brass 1990). As decision makers have a more positive perception regarding the peer organizations who already adopted and incorporated proactive information security approaches, they are more inclined to adopt such approaches for their own organization. Thus, we hypothesize;

H2. Peer influence toward proactive information security approach is positively related to intention to pursue such approach in organizations.

Drawing on PWM, the intention to pursue in the most effective determinant of behavior given that the behavior is "under volitional control" (Van Gool et al. 2015; Ajzen 1991). It demonstrates the degree of motivation to behave in a specific manner, and determines the amount of time and effort that is required to do the actual behavior (Ajzen 1991). Decision makers try to decide rationally based on the available information they have (Kim et al. 2008). As much as

decision makers have more information and are more motivated, there is a higher chance to do the behavior. So, we hypothesize:

H3. Intention to pursue proactive information security approach is positively related to such behavior in organizations.

2.4.2. Heuristic-Based Decision Making

On the heuristic side of decision making, as organizations' information security approaches are typically clear and known by others, organizational decision makers have prototypes of organizations that engage in proactive information security behavior (Gibbons et al. 2003; Gibbons and Gerrard 1995). Such prototypes have a considerable effect on decision makers' own information security behavior. PWM states that decision makers assess the image prototype of organizations with proactive information security behavior, and compare it with their own image. As the prototype becomes more positive, decision makers will be more open to involve in the proactive behavior (Gibbons and Gerrard 1995). Such positive and good prototypes encourage decision makers to enhance their organization, and seek to become more similar to the organizations with such prototypes (Dunning et al. 1991; Hammer and Vogel 2013; Niedenthal et al. 1985). So, we hypothesize:

H4. Prototype favorability of the adopters is positively related to the willingness to pursue such approach in organizations.

Moreover, as a higher number of other organizations become engaged in proactive information security behavior, decision makers are more encouraged to that specific behavior. This will increase their willingness towards that (Gibbons et al. 1998). Thus, we hypothesize:

H5. Peer influence toward proactive information security approach is positively related to willingness to pursue such approach in organizations.

Furthermore, positive feelings about proactive information security behavior diminish the effects of associated drawbacks and costs, and highlight the advantages and benefits of such behavior. As this positive impression increases, decision makers' openness to the behavior also becomes greater (Van Gool et al. 2015; Gibbons et al. 1998). So, we hypothesize:

H6. Attitudes towards a proactive information security approach are positively related to willingness to pursue such an approach in organizations.

Although decision makers might have no intention to be involved in proactive information security behaviors, there might be conducive situations or circumstances that encourage them to take the behavior on (Gerrard et al. 2008; Hukkelberg and Dykstra 2009). For example, they might be invited to an annual meeting where all the pioneer organizations in the industry are participating. Many organizations are talking about their implementation of a new proactive approach in information security management, and decision makers offer to implement one of those approaches. According to PWM, as they are more open to accept proactive behavior under environmental situations, the chance of taking the behavior and deciding to choose it would be higher. Thus, we hypothesize

H7. Willingness to *pursue is positively related to proactive information security behavior.*

2.4.3. Moderating Role of Environmental Factors

We argue that the effects of intention and willingness to pursue proactive information security behavior would be stronger for organizations with higher levels of environmental uncertainty compared to the lower ones. As organizations' external environment become more dynamic and unstable, the possibility of being threatened would be higher (Sung and Choi 2012), making organizations more vulnerable to security attacks and breaches. Therefore, when the environmental uncertainty is perceived to be higher, the effect of decision makers' intention and

openness to adopt proactive information security approach on actual behavior would be stronger, hoping that this approach is the appropriate one (Hsu et al. 2012) to help them predict and prevent probable security breaches, and deal with this high level of uncertainty. Thus, we hypothesize:

H8a. The effect of intention to pursue on proactive information security behavior is stronger for IT professionals in organizations facing higher level of environmental uncertainty than the ones facing lower level of environmental uncertainty.

H8b. The effect of willingness to pursue on proactive information security behavior is stronger for IT professionals in organizations facing higher level of environmental uncertainty than the ones facing lower level of environmental uncertainty.

We also argue that for the organizations that are experiencing a higher level of competitive pressure in the industry, the effect of intention and willingness to pursue proactive information security behavior would be stronger compared to the ones that are experiencing a lower level of competitive pressure. In hypercompetitive industries, organizations need to keep their competitive advantage in order to survive (Zhu and Kraemer 2005). Information security attacks and breaches can easily lead organizations to lose their competitive advantage, especially in the industries where the competitive-related pressure is higher. Thus, adopting and using proactive security approaches is more critical for organizations that are active in hypercompetitive environments in order to prevent or minimize the chance of facing security breaches. This brings extra motivation, and strengthens the effect of decision makers' intention and openness to adopt proactive information security approach on the actual behavior. Thus, we hypothesize:

H9a. The effect of intention to pursue on proactive information security behavior is stronger for IT professionals in organizations under higher level of competitive pressure than the ones under lower level of competitive pressure.

H9b. The effect of willingness to pursue on proactive information security behavior is stronger for IT professionals in organizations under higher level of competitive pressure than the ones under lower level of competitive pressure.

We also believe that for organizations which are active in more supportive regulatory environment, the effect of intention and willingness to pursue proactive information security behavior would be stronger compared to the ones that are active in less supportive regulatory environment. With the intention of promoting proactive behaviors, governments provide supportive environmental regulations (Porter and Linde 1995). Such regulations, however, do not initiate innovations on their own (Karagozoglu and Lindell 2000). Flexibility of supportive environmental regulations offer additional incentives to organizations that are already intended and open to apply proactive strategies for their information security, and encourage them to actually use such strategies. Accordingly, supportive regulations empower the effect of intention and willingness to pursue to adopt proactive information security behavior on organizations actual behavior. We hypothesize:

H10a. The effect of intentions to pursue on proactive information security behavior is stronger for IT professionals in organizations competing in a higher level of regulatory environment than the ones competing in a lower level of regulatory environment.

H10b. The effect of willingness to pursue on proactive information security behavior is stronger for IT professionals in organizations competing in a higher level of regulatory environment than the ones competing in a lower level of regulatory environment.

Figure 2.2 depicts the research model.

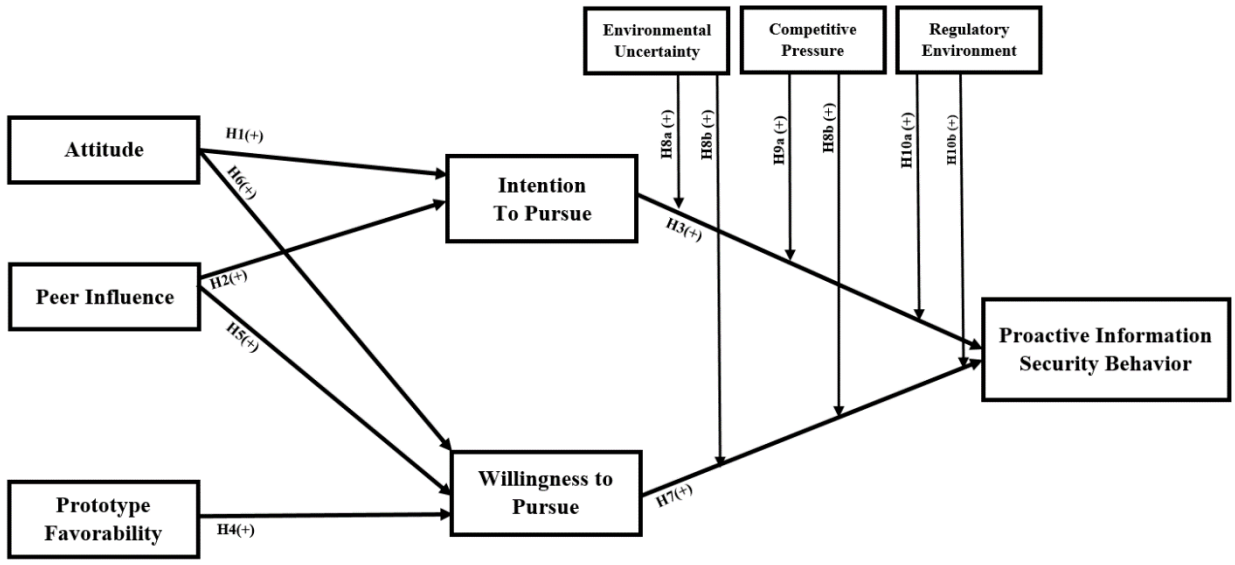

Figure 2.2. Research Model

2.5. RESEARCH METHODOLOGY

2.5.1. Instrument Development

In order to empirically test the hypothesized model, we developed an online survey. The questionnaire was reviewed by two information security faculty and two native English speakers to ensure the content validity and smoothness of the survey, respectively. The survey was then revised based on their comments and feedbacks. Scales were designed to measure six main variables (proactive information security behavior, intention to pursue, willingness to pursue, attitude, peer influence, prototype favorability), and three moderators (environmental uncertainty, competitive pressure, and regulatory environment). All the main constructs were measured using a five-point Likert scale.

Measures of proactive information security behavior were adapted from Jong and de Ruyter (2004). According to literature, measures of proactive behavior are subject- and context-specific (Frese et al. 1996; Morrison and Phelps 1999), and these items had not yet been adapted to the information security context, suggesting adaptation was necessary. In contextualizing this

construct to a new subject (information security), a content validity assessment was conducted to ensure that all the measures best reflect this construct. Results show that three of the measures represent the proactive information security behavior concept.

Measures for intention to pursue were adapted from Venkatesh et al. (2003) and Herath & Rao (2009). In order to measure willingness to pursue, first a new proactive approach in information security management was defined and explained using a recent report from Kessel & Allan (2015). Then a hypothetical situation was explained in which many organizations are talking about their implementation of the new proactive approach in information security management. It was followed by the questions measuring respondents' willingness to pursue that proactive approach (Gibbons and Gerrard 1995, 1997). Attitude and peer influence measures were adapted from Taylor & Todd (1995), and modified to fit the context of our study. Suggested by Gibbons, Gerrard, & McCoy (1995), a prototype approach was first formed in order to assess image. Prototype favorability was measured using questions adapted from Javalgi et al. (1994). Concerning the moderator, environmental uncertainty, competitive pressure, and regulatory environment measures were from Waldman et al. (2001), Zhu, Kraemer, & Xu (2006), and Lin (2006) and Grandon & Pearson (2004), respectively. Final measures are summarized in Table 2.1.

A pilot study was conducted among master students of MIS in a southwest university in United States in exchange for course credit to ensure the validity and smoothness of the survey. Based on the feedback from the pilot test, appropriate changes were made to the questions and the arrangement in the main survey. Prior literature, pilot test, and numerous series of pre-tests gave us the opportunity to confirm the content validity of our instrument and measures (Straub et al. 2004).

Table 2.1. Instrument Items

Construct	Items	Reference(s)
	Main Variables	
Proactive Information Security Behavior	• ProBeh1: In my organization, we seek alternative solutions to information security problems. • ProBeh2: In my organization, we seek innovative solutions to information security problems. • ProBeh3: In my organization, we address information security issues before they become major problems.	(Jong and de Ruyter 2004)
Intention to Pursue	• Int1: It is my intention to support my organization to adopt a proactive approach in information security management. • Int2: I am in favor of adopting a proactive approach in information security management in my organization. • Int3: I am likely to support adopting a proactive approach in information security management in my organization.	(Venkatesh et al. 2003; Herath and Rao 2009)
Willingness to Pursue	Nowadays there is a new proactive approach in information security management to detect and neutralize potential cyber-attacks. It must focus on the future environment and become more confident in its ability to handle more predictable threats, as well as unexpected attacks. It requires organizations to: • Design and implement a Cyber Threat Intelligence strategy • Define and encompass the organization's extended cybersecurity ecosystem • Take a cyber-economic approach • Use forensic data analytics and Cyber Threat Intelligence • Ensure everyone understands what's happening • Prepare for the worst by developing a comprehensive cyber breach response management strategy Suppose you were in the following situation: You are in an annual meeting that all the pioneer organizations in your industry are participating. Many organizations are talking about their implementation of a new proactive approach in information security management. You are suggested to implement one of those approaches. What would you do? [1=Extremely Unlikely, 7= Extremely Likely] • Will1: Accept and plan to implement it soon. • Will2: Do not accept and plan to investigate more about it. • *Say no and have no interest to follow it up.	(Kessel and Allan 2015; Gibbons and Gerrard 1995, 1997)
Attitude	• Attitude1: Adopting such a proactive approach for information security management in my organization is a (bad/ good) idea. • Attitude2: Adopting such a proactive approach for information security management in my organization is a (foolish/ wise) idea. • Attitude3: I (dislike/ like) the idea of adopting a proactive approach for information security management in my organization. • *Adopting a proactive approach for information security management in my organization is (unpleasant/ pleasant)	(Taylor and Todd 1995)

Peer Influence	• PI1: Most successful peer organizations adopt one or more proactive approaches for their information security management. • PI2: For our organization-wide information security management, we have followed the lead of successful peer organizations in investigating proactive approaches. • PI3: For our organization-wide information security management, we have followed the lead of successful peer organizations in incorporating proactive approaches.	(Taylor and Todd 1995)
Prototype Favorability	Imagine an organization that adopted a new proactive approach in information security management. How do the following characteristics fit the organization? The organization: • Image1: Has good product/services. • Image2: Is well managed. • Image3: Is involved in the community. • Image4: Responds to consumer needs. • Image5: Is a good company to work for. • *Only wants to make money.	(Gibbons et al. 1995; Javalgi et al. 1994)
	Moderators	
Environmental Uncertainty	How would you characterize the external environment within which your organization functions? In rating your environment, where relevant, please consider not only the economic but also the social, political, and technological aspects of the environment. • EnvUnc1: Very dynamic, changing rapidly in technical, economic, and cultural dimensions. • EnvUnc2: Very rapidly expanding through the expansion of old markets and the emergence of new ones. • *Very risky, one false step can mean the organization's undoing. • *Very stressful, exacting, hostile, hard to keep afloat.	(Waldman et al. 2001)
Supportive Regulatory Environment	• RegEnv1: The government's laws and regulations support deployment of a proactive information security approach. • RegEnv2: The use of a proactive information security approach is driven by incentives provided by the government. • RegEnv3: The use of a proactive information security approach is legally protected by the government.	(Zhu et al. 2006)
Competitive Pressure	• CompPres1: My organization has experienced competitive pressure to implement innovative information security measures. • CompPres2: My organization will experience a competitive disadvantage if innovative information security methods are not adopted. • CompPres3: Competition is a factor in our decision to adopt innovative security measures. • ComPres4: Our industry is pressuring us to adopt innovative security measures.	(Lin 2006; Grandon and Pearson 2004)

* Items were dropped due to loadings lower than 0.7.

2.5.2. Sample and Data Collection

The main data collection was conducted through Qualtrics panels via an online survey in Qualtrics website. Respondents were full-time employees who have some technical knowledge about user authentication systems and security management in an organization. All the respondents had more than three years of working experience as an IT professional. A total of 193 data points were collected. Around 60% were male. Table 2.2 summarizes the key demographic variables of the respondents; and their title and years of work experience in their current organization. Respondents represent numerous organizations from different industries, with various sizes and ages. Table 2.3 summarizes this information.

Table 2.2. Key Demographic Variables, Title, and Work Experience of Respondents

	Variable	Percent		Variable	Percent
Age	18 to 24 years	0.5%	***Race***	White/ Caucasian	76.2%
	25 to 34 years	26.9%		African American	4.7%
	35 to 44 years	25.9%		Hispanic	6.2%
	45 to 54 years	25.4%		Asian	10.9%
	55 to 64 years	19.7%		Native American	1%
	65 years and over	1.6%		Pacific Islander	1%
Education	Less than High School	0%	***Title***	President, Owner, or Managing Director	4.1%
	High School / GED	3.1%		CIO/CTO/VP of IS	11.9%
	Some College / Bachelor's degree	43.5%		IS Manager, Director, Planner	31.1%
	Master's degree	43%		Other manager in IS department	18.1%
	Professional degree	8.8%		Business Operations Manager	1.0%
	Doctoral Degree	1.6%		Administration/Finance Manager	1.0%
				Other	32.6
Income	Less than 20k	0%	***Work Experience***	Less than a year	3.6%
	20K to 40K	3.6%		1 to 3 years	9.3%
	40K to 60K	12.4%		3 to 5 years	18.7%
	60K to 80K	20.7%		5 to 10 years	34.2%
	More than 80K	63.3%		More than 10 years	34.2%
Gender	Male	59.6%			
	Female	40.4%			

Table 2.3. Industry, Size and Age of Organizations

	Variable	Percent
Org Size	Less than 100 employees	12.4%
	100 – 400 employees	19.2%
	401 – 700 employees	12.4%
	701 – 1000 employees	11.4%
	More than 1000 employees	44.6%
Org Age	Less than 5 years	1.6%
	5 to 10 years	12.4%
	11 to 15 years	13.0%
	16 to 25 years	20.7%
	More than 26 years	52.3%
Industry	Education	8.3%
	Finance	11.4%
	Wholesale/Retail	10.9%
	Healthcare	7.8%
	Construction	3.1%
	Insurance	2.6%
	Other	56%

2.6. DATA ANALYSIS AND RESULTS

2.6.1. Method of Analysis

This study is among the firsts which tests the hypothesized model in the proactive information security behavior, which makes it exploratory by nature. Moreover, PLS technique is more appropriate for evaluating theories that are in the primary phases of development (Fornell and Bookstein 1982). Additionally, the focus of this study is more on assessing the impact of different factors on proactive behavior, instead of highlighting the fit between model parameters and observed correlations (Gefen et al. 2000). As a result, partial least squares (PLS) was used to test the proposed model and associated hypotheses. SmartPLS 3 (Ringle et al. 2015) was used to analyze the data.

2.6.2. Measurement Model Validation

In order to evaluate the measurement model, a confirmatory factor analysis (CFA) was conducted. Results are summarized in Table 2.4. All of the latent constructs are modeled to be reflective. For each latent construct, path loadings, t-statistic, and standard error were calculated.

At alpha level of 0.05, all the measures' path loadings are significant with a value more than 0.7 (Chin and Marcolin 1995), indicating that more than 50% of the variance is shared between each construct's items (Chin 1998).

In order to examine the convergent validity, composite reliability and Average Variance Extracted (AVE) were obtained (Hair et al. 1995). All of the constructs met the acceptable score of 0.5 for AVE, confirming their reliability (Fornell and Larcker 1981). Moreover, values of composite reliability are between 0.849 and 0.942.

Square root of AVE was also used to verify the discriminant validity (Fornell and Larcker 1981). Results are shown in Table 2.5. For each latent construct, the square root of the AVE is higher than all its cross correlations. Moreover, higher values of inter-construct correlations confirm the greater variance among each construct's specific measures compare to other measures (Gefen et al. 2000). All things considered, we can confirm that all the indicators in the measurement model are valid through their constructs.

As data for all the variables was collected in a single survey, common method variance (CMV) could have an excessive effect on the results (Podsakoff et al. 2003). Harman's single factor test was conducted (Podsakoff and Organ 1986) in order to find out the extent of this effect. According to this approach, running a factor analysis, if only a single factor arises, or a factor explains the majority of variance among all the measures, we can conclude that CMV is a significant issue in the sample (Podsakoff et al. 2003). After conducting an exploratory factor analysis among all the items, nine factors were obtained which explained nearly 70% of the variance. All the extracted factors had eigenvalue greater than one, and the highest factor accounted for only 33% of the variance. This indicates that CMV is not a serious concern in this dataset.

Table 2.4. CFA Results

Construct	Item	Loading	t-Statistic	Standard Error	Average Variance Extracted (AVE)	Composite Reliability	Cronbach's Alpha
Proactive InfoSec Behavior	*ProBeh1*	0.901	50.412	0.018	0.802	0.924	0.876
	ProBeh2	0.914	71.434	0.013			
	ProBeh3	0.871	29.694	0.029			
Intention to Pursue	*Int1*	0.909	54.215	0.017	0.844	0.942	0.907
	Int2	0.936	89.307	0.010			
	Int3	0.910	51.342	0.018			
Willingness to Pursue	*Will1*	0.918	35.109	0.026	0.738	0.849	0.659
	Will2	0.797	15.437	0.052			
Attitude	*Attitude1*	0.905	47.472	0.019	0.799	0.923	0.875
	Attitude2	0.896	38.163	0.023			
	Attitude3	0.881	39.763	0.022			
Peer Influence	*PI1*	0.794	22.333	0.036	0.686	0.868	0.774
	PI2	0.848	26.656	0.032			
	PI3	0.841	23.212	0.036			
Prototype Favorability	*Image1*	0.828	27.774	0.030	0.629	0.894	0.851
	Image2	0.744	14.806	0.050			
	Image3	0.706	14.618	0.048			
	Image4	0.829	29.245	0.028			
	Image5	0.848	17.601	0.048			
Environmental Uncertainty	*EnvUnc1*	0.882	36.317	0.024	0.777	0.874	0.712
	EnvUnc2	0.880	32.840	0.027			
Competitive Pressure	*ComPres1*	0.841	28.393	0.030	0.684	0.896	0.846
	ComPres2	0.824	25.235	0.033			
	ComPres3	0.788	16.774	0.047			
	ComPres4	0.853	28.063	0.030			
Regulatory Environment	*RegEnv1*	0.880	36.354	0.024	0.707	0.878	0.800
	RegEnv2	0.806	21.476	0.038			
	RegEnv3	0.835	24.679	0.034			

Table 2.5. Matrix of Latent Constructs' Correlations

Construct	1	2	3	4	5	6	7	8	9
1. Proactive Behavior	**0.895**								
2. Intention to Pursue	0.418	**0.918**							
3. Willingness to Pursue	0.290	0.277	**0.859**						
4. Attitude	0.409	0.541	0.250	**0.894**					
5. Peer Influence	0.567	0.461	0.339	0.474	**0.828**				
6. Prototype Favorability	0.406	0.426	0.449	0.472	0.467	**0.793**			
7. Environmental Uncertainty	0.462	0.451	0.287	0.314	0.413	0.295	**0.881**		
8. Competitive Pressure	0.605	0.396	0.321	0.413	0.551	0.410	0.481	**0.827**	
9. Regulatory Environment	0.475	0.333	0.372	0.256	0.503	0.510	0.360	0.627	**0.841**

Shaded cells in the diagonal row are AVE square roots.

2.6.3. Structural Model

Results of data analysis, including R-squares, standardized path coefficients, associated t-values and paths significance, are depicted in Figure 2.3. In order to test the significance of path coefficients in the structural model, we used a bootstrapping approach with 1000 resamples. R-square value of proactive information security behavior is 0.265, indicating that more than nearly 27% of the variance in proactive information security behavior can be explained by intention and willingness to pursue. Moreover, R-square value for intention to pursue and willingness to pursue is 0.369 and 0.242, respectively. This suggests that approximately 37% of the variance in intention to pursue can be justified by attitude and peer influence. At the same time, nearly 25% of the variance in willingness to pursue can be explained by attitude, peer influence, and image. Since these amounts of variance are more than 10, we can claim that the proposed model is valid and acceptable (Falk and Miller 1992).

The results of testing rational-based decision making relationships indicate that attitude ($\beta= 0.428$, $p<0.001$), and peer influence ($\beta= 0.234$, $p<0.01$) have significant effects on intention to pursue, supporting H1 and H2. Intention to pursue also significantly affect proactive information security behavior ($\beta= 0.347$, $p<0.001$), providing evidence to support H3. Furthermore, testing heuristic-based decision making relationships shows that prototype favorability ($\beta= 0.342$, $p<0.001$) has a significant effect on willingness to pursue, supporting H4. Peer influence ($\beta= 0.134$, t-statistics= 1.719), and attitude ($\beta= 0.013$, t-statistics= 0.287), however, do not significantly affect willingness to pursue. As a result, we do not have enough evidence to support H5 and H6. Willingness to pursue also positively and significantly affect proactive information security behavior ($\beta= 0.146$, $p<0.05$), providing evidence to support H7.

We also controlled for the effect of responders' education level, years of IT experience, and income for proactive information security behavior, intention to pursue, and willingness to pursue. Decision makers with more experience in information technology are less likely to use proactive information security behavior in their organization. They are also less open to pursue proactive information security. Moreover, decision makers with higher level of education are more intended to pursue proactive information security.

In order to test each moderating effect, a construct was created by cross-multiplying all the items of appropriate constructs, standardized in order to avoid multicollinearity, and included in the main model (Toothaker 1994). This approach is called product-indicator (Chin et al. 2003). Moderation results show that environmental uncertainty (β= 0.161, t-statistics= 1.748), competitive pressure (β= 0.123, t-statistics= 1.821), and regulatory environment (β= 0.064, t-statistics= 0.856) do not significantly moderate the effect of intention to pursue on proactive information security behavior. As a result, we do not have enough evidence to support H8a, H9a, and H10a. Furthermore, environmental uncertainty (β= 0.162, $p<0.01$), competitive pressure (β= 0.115, $p<0.05$), and regulatory environment (β= 0.152, $p<0.001$) positively moderate the effect of willingness to pursue on proactive information security behavior. These support H8b, H9b, and H10b.

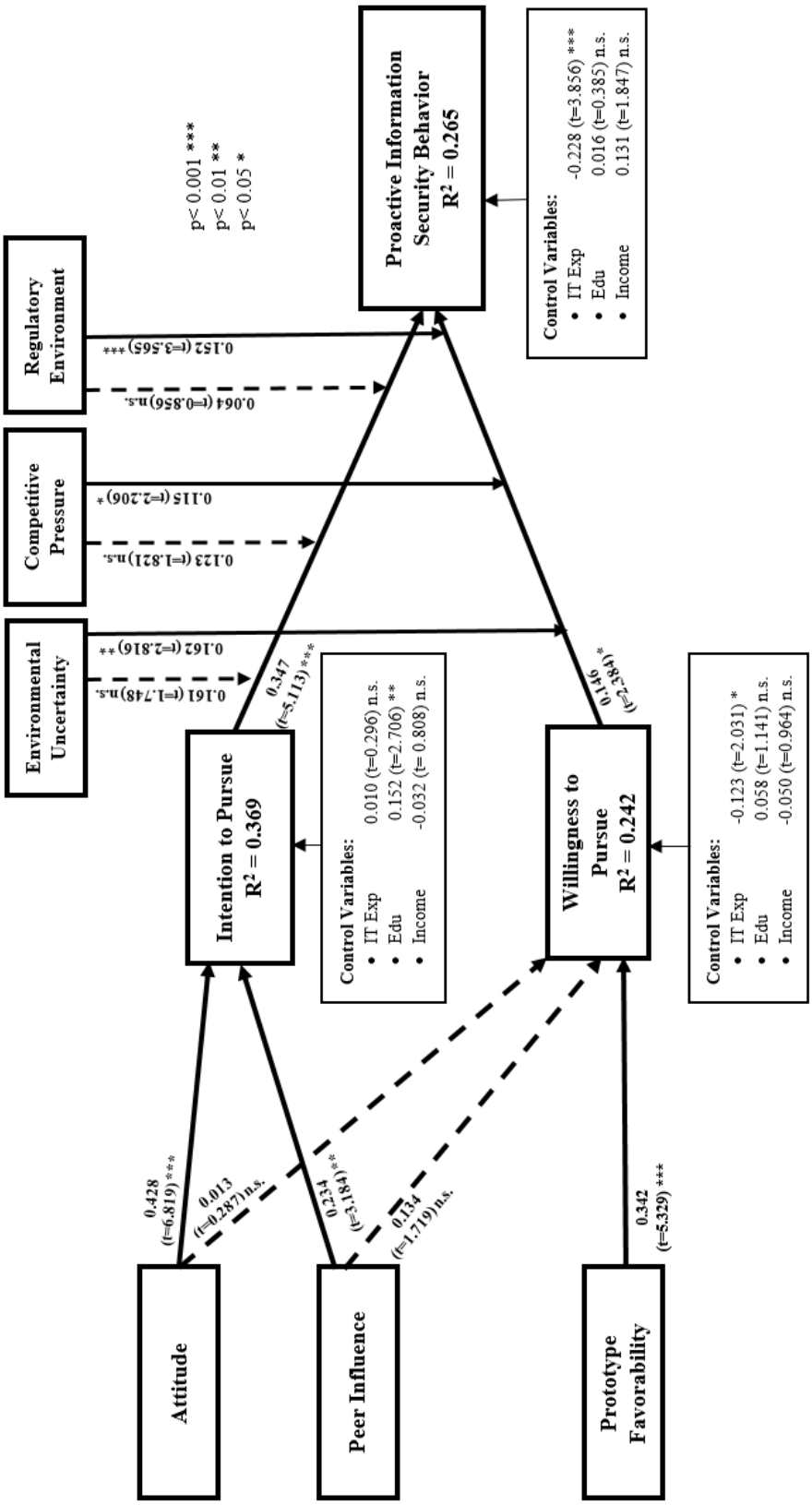

Figure 2.3. PLS Results

2.7. DISCUSSION

This study investigates how both rational and heuristic aspects of decision making can affect IT professionals' proactive information security behavior, from prototype-willingness model perspective. Our findings indicate that both aspects impact their proactive behavior. Further, dominant external environmental characteristics such as competitive pressure, environmental uncertainty, and regulatory environment strength the effect of IT professionals' willingness to pursue proactive information security behavior on the organizations' actual behavior. Table 2.6 summarizes the hypotheses testing results.

Table 2.6. Summary of Results

Hypothesis	Result
H1. Positive attitude toward proactive information security approach is positively related to intention to pursue such approach in organizations.	Supported
H2. Peer influence toward proactive information security approach is positively related to intention to pursue such approach in organizations.	Supported
H3. Behavioral intention to pursue proactive information security approach is positively related to such behavior in organizations.	Supported
H4. Prototype favorability of the adopters is positively related to the willingness to pursue such approach in organizations.	Supported
H5. Peer influence toward proactive information security approach is positively related to willingness to pursue such approach in organizations.	Not Supported
H6. Attitudes toward proactive information security approach are positively related to willingness to pursue such approach in organizations.	Not Supported
H7. Willingness to pursue is positively related to proactive information security behavior.	Supported
H8a. Environmental uncertainty positively moderates the relationship between intention to pursue and proactive information security behavior.	Not Supported
H8b. Environmental uncertainty positively moderates the relationship between willingness to pursue and proactive information security behavior.	Supported
H9a. Competitive pressure positively moderates the relationship between intention to pursue and proactive information security behavior.	Not Supported
H9b. Competitive pressure positively moderates the relationship between willingness to pursue and proactive information security behavior.	Supported
H10a. Supportive regulatory environment positively moderates the relationship between intention to pursue and proactive information security behavior.	Not Supported
H10b. Supportive regulatory environment positively moderates the relationship between willingness to pursue and proactive information security behavior.	Supported

2.7.1. Contribution to Theory

Taken together, this study has several theoretical contributions. To the best of our knowledge, this study is among the first to investigate a dual-processing model in the context of information security. This is specifically important for proactive security approaches in order to uncover various motivators of this efficient approach. Exploring both rational and heuristic aspects of decision making is a step forward in clarifying a part of unexplained variance of proactive behavior construct in prior studies.

Moreover, our findings point towards the importance of three dominant environmental characteristics (pressure, environmental uncertainty, and regulatory environment) on the proactive information security behavior. Results of moderating variables show how the interaction of environmental features and willingness to pursue can significantly shape organizational proactive behavior. This is an important finding as it demonstrates the critical role and effect of external environment specifically on the heuristic-based type of decision making.

2.7.2. Implications for Practice

This study has also implications for practice. The results of this study highlight the role of a less-noticeable aspect of decision making for managers that are planning to enhance proactive security behavior in their organizations. This is especially important for organizations that deal with sensitive data and constantly seek for innovative and novel techniques to decrease the chance of information security risks and threats for their organizations.

Further, findings of this study are particularly important for the organizations which are active in unstable, hypercompetitive, and restricted industries. This can motivate managers and executives to have a better understanding of their organizations' external environment and form their long term information security planning, strategies, and trainings based on that. It can also

persuade policy makers to consider special strategies to promote proactive information security behavior among organizations that are active on the above-mentioned industries.

2.7.3. Limitations and Future Research

Finally, it is important to mention that this study has some limitations. First, targeting responders from only one country may raise the likelihood of regional biases and limit the generalizability of the findings. Conducting the study in various other countries could be a possible future study and an option to enhance the external validity of results. Second, there is part of variance in our dependent variable which our study did not explain. This is apparent form the coefficient of determination and presents a possible topic of study. And finally, as we only collected self-reported data from one source, future empirical studies using multiple sources of data will add to the validity of findings.

Chapter Three:

How to Continuously Improve Information Security Management Practice: An Organizational Learning Perspective

3.1. INTRODUCTION

Information security related risks may cause significant potential and immediate damages to contemporary organizations. These damages include but are not limited to, credibility, monetary, or liability loss (Cavusoglu et al. 2004; Culnan et al. 2008). As such, proactively preparing for and successfully managing information security risks has become a strategic priority for many organizations (Warkentin et al. 2016). Accordingly, IT managers have been increasingly called by the business executives to search for and establish an effective organizational wide information security management program (Tu and Yuan 2014; Ransbotham and Mitra 2009).

Issues related to information security have also drawn growing attention from IT management scholars over the past decade. For example, researchers have examined a wide range of topics related to information security, including organizational security policies compliance (Herath and Rao 2009) and violations (D'Arcy et al. 2009), IT security training (Puhakainen and Siponen 2010) and risk management (Spears and Barki 2010), as well as user behavior to take safeguarding measures (Anderson and Agarwal 2010; Johnston and Warkentin 2010). Nevertheless, the units of analysis in most of these studies are individual computer users. Few studies have taken an organizational perspective to examine how to improve an organization's overall capacity to deal with information security challenges.

In this study, we aim to bridge the above research gap. We submit information security management should be regarded as an ongoing organizational effort. As business environments have become more complex and competitive, organizations no longer compete on the processes but on their capability to constantly improve such processes (Teece 2007). Correspondingly, we are interested in addressing the overall question of how an organization could continuously improve its information security management program. We define continuous improvement in

information security management as a tactic to signify persistent and systematic efforts of organizations in searching and applying innovative methods of improving information security management (Anand et al. 2009; Peng et al. 2008).

Prior literature largely suggests organizational learning is a powerful driver of continuous improvement in organizations (Zangwill and Kantor 1998; Helfat et al. 2007). Organizational learning is "the process of improving actions through better knowledge and understanding" (Fiol and Lyles 1985). Building on this, we propose that in order to ensure the best results out of continuous improvement programs, organizations need more than the simple explorative aspects of learning, which is the creation and gain of knowledge (Zahra and George 2002). They should also master the exploitative aspect of learning, which is the utilization of the gained and created knowledge (Lane et al. 2006; Zahra and George 2002; Todorova and Durisin 2007). These two aspects of learning comprise the notion of absorptive capacity (Zahra and George 2002). Therefore, our first specific research question is: How can an organization's level of absorptive capacity affect its continuous improvement of information security management?

Furthermore, over and above the direct effect, we propose that absorptive capacity may also indirectly affect an organization's continuous improvement of information security management through enhancing another important organizational capability, the adaptiveness to information security threats, defined as the degree to which the organization is capable of reconfiguring actions and activities in response to changing information security threats (Simsek 2009; Smit 2015). Because adaptiveness helps organizations incorporate more ongoing and incremental changes (Boer et al. 2017; Boynton 2007), it can be viewed as a critical and direct source of superior continuous improvement. High levels of absorptive capacity can help organizations anticipate and neutralize potential information security threats (Santos-Vijande et al.

2012). We propose that absorptive capacity supports the development of adaptiveness to information security threats, thereby influencing continuous improvement of information security management. In other words, our second research question is: Can an organization's absorptive capacity improve continuous improvement of information security management through adaptiveness to information security threats?

We are also interested in exploring if some organizations could be more effective than their peers in adapting to information security threats with equivalent levels of absorptive capacity. We investigate an external environmental characteristic that may moderate the absorptive capacity-adaptiveness relationship: regulatory environment. A supportive regulatory environment is the one under which regulations are flexible in order to provide incentives for organizations to promote adaptive strategic initiatives (Porter and Linde 1995). Extant studies have shown that organizations operating in less supportive regulatory environments are less flexible in adopting and implementing novel technical and behavioral solutions (e.g. Karagozoglu and Lindell 2000). Following this logic, our third research question is: How do supportive regulatory environments moderate the effects of absorptive capacity on adaptiveness to information security threats?

An integrative research model was developed corresponding the above research questions (Figure 3.1). Survey data was collected and analyzed to test the research hypotheses. The respondents were limited to managers who have knowledge about security management at organizational level and with more than three years of working experience in IT-related functions. Our results suggest that absorptive capacity could both directly and indirectly (through adaptiveness to information security threats) affect continuous improvement of information security management. Moreover, for organizations competing in more supportive regulatory

environments, the effects of absorptive capacity to adaptiveness to information security threats are stronger.

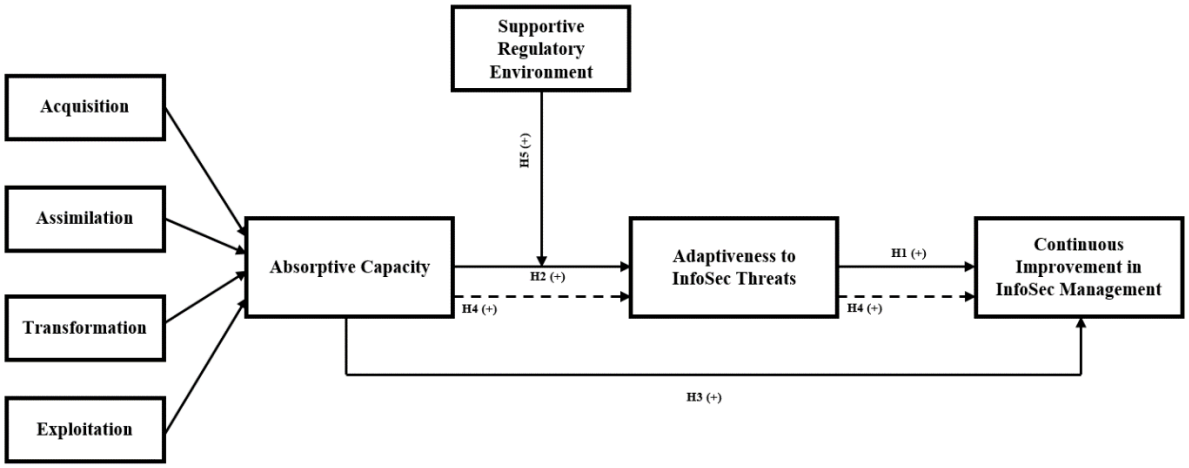

Figure 3.1. Research Model

3.2. THEORETICAL BACKGROUND

3.2.1. Information Security Management as a Continuous Organizational Practice

Information security management is a process of protecting critical systems and information from internal and external information security risks and threats effectively (Barlas et al. 2007; Tu and Yuan 2014), and mainly includes guidelines for comprehensively identifying vulnerable information assets, establishing security objectives, evaluating risks, and taking actions to deal with those risks (Dubois et al. 2010; Stoneburner et al. 2002). After finding out and setting up effective information security management programs in the organization, managers need to continuously monitor and improve such programs in order to meet evolving threats (Fogalin 2009; General 2002) and enhance the competitive level of their organization in the globalized industries (Gonzalez and Martins 2016). Therefore, information security management is not a one-time effort. Rather, it is a journey that needs continuous improvement (Conner and Coviello 2004). In other words, organizations should repeatedly consider making dynamic improvements in their

information security management processes and search for chances to remove or lessen the roots of imperfections in the information security strategies and processes (Bhuiyan and Baghel 2005).

Continuous improvement in information security, by definition, "is a systematic effort to seek out and apply new ways of doing work" (Anand et al. 2009). The aim of continuous improvement is to enhance organizations' information security effectiveness and, as a result, bring significant contributions to the overall organizational-wide performance (Bessant and Caffyn 1997; Wu and Chen 2006; Gonzalez and Martins 2016; Kohlbacher and Gruenwald 2011; Kohlbacher 2013). Such improvements take into account both actions that last continuously (such as frequent monitoring of information security risks in order to minimize the likelihood of attacks) as well as periodical projects (such as a critical system upgrade to protect information against a new malware) (Lillrank et al. 2001). In other words, continuous improvement to information security management program consists of ongoing incremental as well as radical changes (Boer et al. 2017; Boynton and C. 2007), ranging from minor to significant initiatives and even changes to the entire existing information security management program (Anand et al. 2009; Brajer-Marczak 2014).

Therefore, the organizational capability to make continuous improvement is particularly considered as a dynamic capability (Oxtoby et al. 2002; Glover et al. 2015; Anand et al. 2009; Helfat et al. 2007) which enables firms to constantly make incremental and radical changes (Schreyögg and Kliesch-Eberl 2007). In practice, continuous improvement requires managers' never ending (i.e., an "always on the road" mentality) commitments to excellence (Hoem and Lodgaard 2016). Although executives and managers understand the significance of constantly improving processes in their organizations, the complex nature of continuous improvement makes it a challenging task for them to engage in (Anand et al. 2009; Pullin 2005). Prior studies have

shown that only 2% of organizations that have continuous improvement programs achieved their expected outcomes (Hoem and Lodgaard 2016; Liker and Franz 2011).

The aim of this study is to explore forces that shape an organization's capacity to continuously improve its information security management practices. According to the literature, organizational learning is a primary driver to continuous improvement (Zangwill and Kantor 1998; Helfat et al. 2007). Organizational learning helps managers keep their continuous improvement practices in a sustainable way (Bessant and Caffyn 1997; Jaber et al. 2010; Sun et al. 2008). It also facilitates the application of the newly created and obtained knowledge towards a firm level infrastructure supporting continuous improvement (Anand et al. 2009; Linderman et al. 2004). More importantly, organizational learning generates knowledge and understanding on what types of improvements to make, and how to do such improvements faster and better (Anand et al. 2009; Zangwill and Kantor 1998).

3.2.2. Absorptive Capacity and Organizational Learning

Absorptive capacity is an essential organizational learning capability which enables knowledge management (Malhotra et al. 2005; Wheeler 2002; Zahra and George 2002) and explains why some organizations are more capable of effectively managing environmental uncertainties compared to others (Patel et al. 2012). By definition, absorptive capacity is an organization's ability to realize the value of new external knowledge along with assimilating and applying that knowledge through competitive actions and innovations (Cohen and Levinthal 2000; Tu et al. 2006; Zahra and George 2002; Roberts et al. 2012). It consists of a series of actions to manage a company's existing knowledge and build new knowledge based on prior related-knowledge, rich communication, and learning routines (Malhotra et al. 2005; Tu et al. 2006). Absorptive capacity enables firms to quickly examine and interpret information about

environmental and organizational changes, and originate essential reconfiguration, rearrangement, and renewal of associated capabilities, thereby enhancing their flexibility in response to various technological, competitive, and demand uncertainties (Patel et al. 2012).

In addition, absorptive capacity allows organizations to quickly sort out their internal knowledge (Liu et al. 2013; Tsai 2001; Cohen and Levinthal 2000), obtain and tie together the newly gained knowledge (Cohen and Levinthal 2000; Malhotra et al. 2005; Zahra and George 2002), apply both to reengineer their processes, identify novel business opportunities, and take advantage of such opportunities before competitors recognize them (Liu et al. 2013; Cohen and Levinthal 2000; Roberts et al. 2012). An organization with a high level of absorptive capacity could better understand how to take innovative actions (Lane et al. 2006; Zahra and George 2002) and is also capable of taking more effective and efficient actions in processing new information. Moreover, the likelihood of proactively responding to changes is higher for such organizations (Cohen and Levinthal 1989).

Following the established literature, we frame absorptive capacity as a second-order construct with four dimensions: acquisition, assimilation, transformation, and exploitation (Jansen et al. 2005; Malhotra et al. 2005; Zahra and George 2002). The acquisition dimension emphasizes the ability to recognize, gather and develop new and relevant knowledge from various sources. The assimilation aspect focuses on the ability to absorb and understand the newly gained knowledge. The transformation dimension reflects the ability to integrate the existing and newly gained knowledge. The exploitation aspect describes the ability to apply the new knowledge to accomplish organizational objectives and meet market requirements (Liu et al. 2013; Setia and Patel 2013).

3.2.3. Adaptiveness to Information Security Threats

Accompanied by the increasing investments in novel information and communication technologies (ICTs), organizations become more susceptible to different forms of information security threats (Jouini et al. 2014). By definition, a security threat is "a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and fraud, waste, and abuse" (Kalakota and Whinston 1996). With the growing dependence of businesses on information generated by ICTs, managers have been struggling extensively to find out and understand what are the specific threats to their organizations' information resources, and how they can gain the essential means to prevent or fight against such threats (Hoffman et al. 1999; Jouini et al. 2014). Given the fact that organizations are constantly facing information security threats, their ability to quickly change attitudes and appropriately reconfigure activities is crucial to their success in sustaining their competitive advantage (Hitt et al. 1998; Volberda 1996).

In other words, an organization must embrace its adaptiveness to information security threats, defined as the degree to which the organization is capable of reconfiguring actions and activities in response to changing information security threats (Simsek 2009; Smit 2015). Adaptiveness allows organizations to proactively look for new information security threats and find novel tactics and techniques, or change the current ones to adjust to unexpected consequences of new and updated threats (Basadur et al. 2014; Lei et al. 1996). Therefore, organizations with high levels of adaptiveness to information security threats are the ones being flexible both in terms of allocation of resources to the new actions and creation of new internal values (Kortmann et al. 2014; Zhou and Wu 2009; Shimizu and Hitt 2004) in order to grasp the opportunities and tackle the threats faster (Chin et al. 2016).

According to the literature, adaptability in organizations is mainly a function of their capability to learn (Argyris and Schon 1978). Such a learning capability helps organizations capture and take the appropriate information at the right time in a more precise way, anticipate changes and tendencies in the market, and discard the activities that are no longer effective (Santos-Vijande et al. 2012). For that reason, organizations with high levels of learning capability are more flexible in terms of detecting problems and opportunities that take place in their environment (Beer et al. 2005; Lumpkin and Lichtenstein 2005) and act more effectively and rapidly with regards to allocating resources, neutralizing environmental threats and taking of opportunities (Argyris and Schon 1978; Santos-Vijande et al. 2012).

3.2.4. Regulatory Environment

Organization adaptiveness should not only be understood as a straight intra-organizational process (Kraatz 1998; Keister 2002). The regulatory sector of the environment in which organizations compete normally represents a key source of uncertainty for these organizations. The regulatory sector consists of government laws, regulations, and policies (Chen 2007). Well-designed government regulations enhance organizations' understanding of issues in the environment, and decrease environmental uncertainties (Porter and Linde 1995; Karagozoglu and Lindell 2000). Furthermore, when government regulations become more supportive, the assessment of opportunities and risks in the environment will play a more important role for firms to originate and develop strategic initiatives (Maxwell 1996; Rondinelli and Vastag 1996). However, if not supportive, regulatory legislation expectations could bring severe anxiety to those organizations that are affected, as appropriate adjustments are needed for organizations to be compatible with such regulatory constraints (Carter 1990).

Supportive regulatory environment points toward flexibility of regulations in order to provide incentives for organizations to meet their goals through the development of adaptive strategies (Porter and Linde 1995). Organizations operating in an environment that government regulations are less supportive have lower flexibility in implementing innovative technological and behavioral solutions (Karagozoglu and Lindell 2000). Flexibility promoted under supportive regulations provides extra motivation for organizations, and may strengthen the effect of organizational learning on their adaptiveness.

3.3. HYPOTHESES DEVELOPMENT

Based upon the conceptual background described in the previous section, we developed the hypotheses for this study. First, organizations with higher level of adaptiveness to information security threats are more capable of discovering potential information security threats and reacting in a way to neutralize or lessen the harm of those threats (Simsek 2009; Smit 2015). Such actions consequently enhance organizations' information security management level. Therefore, higher levels of adaptiveness help organizations incorporate more ongoing effective changes (Boer et al. 2017; Boynton 2007) in their information security management activities and keep improving their security management processes. Thus, we hypothesis:

H1. An organization's adaptiveness to information security threats is positively related to its continuous improvement in information security management.

Second, organizations with a higher level of absorptive capacity are able to process and use information more effectively and efficiently. Moreover, the chance of responding to changes in a proactive manner would be higher for such organizations (Cohen and Levinthal 1989). By effectively deploying current and newly gained information, organizations become more professional in sensing potential information security threats (Malhotra et al. 2005). Besides,

organizations that have a higher level of absorptive capacity would be amenable to change (Pavlou and El Sawy 2006; Zahra and George 2002) and have a higher capability in anticipating and neutralizing potential information security threats (Santos-Vijande et al. 2012). Accordingly, we hypothesize:

H2. An organization's absorptive capacity is positively related to its adaptiveness to information security threats.

Third, continuous improvement in organizations is mainly determined by how capable they are in obtaining and processing information (Zangwill and Kantor 1998; Helfat et al. 2007). By constantly obtaining timely and useful information, organizations can keep improving their information security practices in a sustainable way, and use the obtained knowledge to enhance their current information security processes (Anand et al. 2009; Linderman et al. 2004). Organizations with higher levels of absorptive capacity have a more accurate and precise understanding of why continuous improvement in information security management is important, what forms of information security improvement practices are more effective for them, and how to perform such improvements quicker and better (Anand et al. 2009; Zangwill and Kantor 1998). Thus, we hypothesize:

H3. An organization's absorptive capacity is positively related to its continuous improvement in information security management.

Fourth, an organization's absorptive capacity could influence its capacity to continuously improve its information security management by fostering its adaptiveness to information security threats. Organizations with higher levels of absorptive capacity have a clear understanding on why continuous improvement in information security management is important and which specific forms of information security improvement practices are more effective (Anand et al. 2009;

Zangwill and Kantor 1998). This is mainly due to the fact that such organizations have more experience using their knowledge to discover and neutralize potential information security threats which helps them to be more adaptive in anticipating different types of future threats and constantly improve their current techniques to prevent them (Argyris and Schon 1978; Santos-Vijande et al. 2012). So, we hypothesize:

H4. An organization's adaptiveness to information security threats mediates the relationship between its absorptive capacity and its continuous improvement in information security management.

Fifth, supportive regulations are the mechanisms used by governments to encourage more proactive organizational activities (Porter and Linde 1995). Such regulations, however, do not directly produce innovations on their own (Karagozoglu and Lindell 2000). Instead, a supportive regulatory environment allows more flexibility and freedom for organizations, and makes it more convenient for them to leverage their learning capabilities and to apply their knowledge in finding and neutralizing potential information security threats. In the presence of supportive regulations, organizations enjoy more opportunities to test their newly gained knowledge and techniques and thus, be more successful in predicting potential information security threats. Therefore, we hypothesize:

H5. The effect of absorptive capacity to adaptiveness to information security threats is stronger for organizations that operate in a more supportive regulatory environment.

3.4. RESEARCH METHODOLOGY AND RESULTS

3.4.1. Instrument Development

In order to empirically test the hypothesized model, we developed an online survey. The questionnaire was reviewed by two information security management experts to ensure face validity. The survey was then revised based on their comments and feedbacks. Scales were designed to measure six main variables (Continuous Improvement in Information Security Management, Adaptiveness to Information Security Threats, Acquisition, Assimilation, Transformation, and Exploitation), and one moderator (Supportive Regulatory Environment). All the main constructs were measured using a five-point Likert scale.

Regarding the main variables, measures of continuous improvement in information security management were adapted from Jong and de Ruyter (2004) and modified in a way to fit the context of information security. We then conducted an assessment of the scale's content validity by having experts evaluate the face validity of different items. Results show that three of the measures represent the continuous improvement in information security management concept.

Acquisition, assimilation, transformation, and exploitation measures were adapted from Pavlou and El Sawy (2006). Adaptiveness to information security threats was measured by questions adapted from (Jong and de Ruyter 2004; Spiro and Weitz 1990). Concerning the moderator, supportive regulatory environment measures were adapted from Zhu, Kraemer, & Xu (2006). Final measurement items are summarized in Table 3.1.

A pilot study was conducted among master students of MIS in a southwest university in the United States in exchange for course credit. Minor changes were made to the measures and arrangements of the questions based on the results. Prior literature, pilot tests, and numerous series

of pre-tests gave us the opportunity to confirm the content validity of our instrument and measures (Straub et al. 2004).

Table 3.1. Instrument Items

Construct	Items	Reference(s)
	Dependent Variable	
Continuous Improvement in InfoSec Management	• ContImp1: In my organization, we actively seek out areas for continuous improvement of our information security management. • ContImp2: In my organization, we continuously revise information security management processes. • ContImp3: In my organization, we are constantly on the lookout for improving our information security management effort.	(Jong and de Ruyter 2004)
	Independent Variable	
Absorptive Capacity	• Acq1: We are successful in learning new things within our organization. • Acq2: My organization is effective in developing new knowledge or insights that have the potential to influence our business. • Acq3: My organization is able to identify and acquire internal (e.g., within the organization) and external (e.g., market) knowledge. • Assi1: My organization has effective routines to identify, value, and import new information and knowledge. • Assi2: My organization has adequate routines to analyze the information and knowledge obtained. • Assi3: My organization has adequate routines to assimilate new information and knowledge. • Trans1: My organization can successfully integrate our existing knowledge with the new information and knowledge acquired. • Trans2: My organization is effective in transforming existing information into new knowledge. • Exp1: My organization can successfully exploit internal and external information and knowledge into concrete applications. • Exp2: My organization is effective in utilizing knowledge in new services.	(Pavlou and El Sawy 2006)
	Mediator	
Adaptiveness to InfoSec Threats	• Adp1: When we feel that one effort of managing information security risk is not working, we can easily change to another. • Adp2: In my organization, we feel that each information security problem requires a unique approach. • Adp3: In my organization, our management style may vary from information security risk to risk. • Adp4: In my organization, we try to understand how one information security threat differs from another in risk management expectations. • Adp5: In my organization, it is easy to modify our information security management approach if the situation calls for it. • *My organization is very sensitive to the needs of information security.	(Jong and de Ruyter 2004; Spiro and Weitz 1990)
	Moderator	
Supportive Regulatory Env.	• RegEnv1: The government's laws and regulations support deployment of a proactive information security approach. • RegEnv2: The use of a proactive information security approach is driven by incentives provided by the government. • RegEnv3: The use of a proactive information security approach is legally protected by the government.	(Zhu et al. 2006)

* Items were dropped due to loadings lower than 0.7.

3.4.2. Sample and Data Collection

The main data collection was conducted through Qualtrics panel services via an online survey hosted by the Qualtrics website. Respondents were managers who had technical knowledge about security management in an organization. The selection criterion requires the respondents should have more than three years of working experience in IT related functions. A total of 130 data points were collected. Around 70% of respondents were male, and about 77% were within the age range of 25 to 54. Furthermore, nearly 68% had more than five years of work experience. Table 3.2 summarizes key demographic variables of the respondents as well as their title and years of work experience in their current organization. Moreover, respondents represent organizations from a wide range of industries. Nearly 45% were from organizations with more than 1,000 members, while more than 50% were from organizations older than 26 years. Table 3.3 summarizes this information.

Table 3.2. Key Demographic Variables, Title, and Work Experience of Respondents

	Variable	Percent		Variable	Percent
Age	25 to 34 years	27.5%	***Race***	White/ Caucasian	73.8%
	35 to 44 years	23.1%		African American	5.4%
	45 to 54 years	26.2%		Hispanic	5.4%
	55 to 64 years	21.5%		Asian	13.1%
	65 years and over	1.5%		Native American	1.5%
				Pacific Islander	0.8%
Education	High School / GED	3.1%	***Title***	President, Owner, or Managing Director	6.2%
	Some College / Bachelor's degree	44.6%		CIO/CTO/VP of IS	17.7%
	Master's degree	45.4%		IS Manager, Director, Planner	46.2%
	Professional degree	4.6%		Other manager in IS department	26.9%
	Doctoral Degree	2.3%		Business Operations Manager	1.5%
				Administration/Finance Manager	1.5%
Income	20K to 40K	3.1%	***Work Experience***	Less than a year	5.4%
	40K to 60K	14.6%		1 to 3 years	9.2%
	60K to 80K	21.5%		3 to 5 years	17.7%
	More than 80K	60.8%		5 to 10 years	34.6%
				More than 10 years	33.1%
Gender	Male	68.5%			
	Female	31.5%			

Table 1.3. Industry, Size and Age of Organizations

	Variable	Percent
Org Size	Less than 100 employees	12.3%
	100 – 400 employees	21.5%
	401 – 700 employees	9.2%
	701 – 1000 employees	12.3%
	More than 1000 employees	44.6%
Org Age	Less than 5 years	1.5%
	5 to 10 years	10.8%
	11 to 15 years	13.8%
	16 to 25 years	20.0%
	More than 26 years	53.8%
Industry	Education	6.9%
	Finance	11.5%
	Wholesale/Retail	10.8%
	Healthcare	10.0%
	Construction	1.5%
	Insurance	1.5%
	Other	57.7%

3.5. DATA ANALYSIS AND RESULTS

3.5.1. Method of Analysis

This study is among the first to test a research model examining organizational continuous information security management practices. By nature, the study is exploratory. Moreover, the partial least square (PLS) technique is more appropriate for evaluating theories in the primary phases of development (Fornell and Bookstein 1982). In addition, the focus of this study is more on assessing the impact of independent variable on continuous improvement of information security management, instead of highlighting the fit between model parameters and observed correlations (Gefen et al. 2000). Therefore, PLS is appropriate to test the proposed model and associated hypotheses. SmartPLS 3 (Ringle et al. 2015) was used to analyze the data.

3.5.2. Measurement Model

To evaluate the measurement model, a confirmatory factor analysis (CFA) was conducted. Results are summarized in Table 3.4. All of the latent constructs were modeled to be reflective. For each latent construct, path loadings, t-statistic, and standard error were calculated. At alpha

level of 0.05, all the measurement items' path loadings are significant with a value more than 0.7 (Chin and Marcolin 1995), indicating that more than 50% of the variance is shared between each construct's items (Chin 1998). To examine the convergent validity, composite reliability and average variance extracted (AVE) were obtained (Hair et al. 1995). All of the constructs met the acceptable score of 0.5 for AVE, thereby confirming their reliability (Fornell and Larcker 1981). Moreover, values of composite reliability are between 0.884 and 0.952.

The square root of AVE was also used to verify the discriminant validity (Fornell and Larcker 1981). Results are shown in Table 3.5. For each latent construct, the square root of the AVE is higher than all its cross correlations. Moreover, higher values of inter-construct correlations confirm the greater variance among each construct's specific measures compared to other measures (Gefen et al. 2000). All things considered, we can confirm all the indicators in the measurement model are valid through their constructs.

As the data was collected in a single survey, common method variance (CMV) could be a concern (Podsakoff et al. 2003). We conducted Harman's single factor test (Podsakoff and Organ 1986) to determine the extent of this issue. According to this approach, with a factor analysis, if only one single factor arises, or a factor explains the majority of variance among the measures, we can conclude that CMV is a significant issue in the sample (Podsakoff et al. 2003). After conducting an exploratory factor analysis among all the items, we obtained four factors that explained around 70% of the variance. All extracted factors had eigenvalue greater than one, and the highest factor accounted for 48% of the variance. These results indicate CMV is not a serious concern in this dataset.

Table 3.4. CFA Results

Construct	Item	Loading	t-Statistic	Standard Error	Average Variance Extracted (AVE)	Composite Reliability	Cronbach's Alpha
Continuous Improvement in InfoSec	*ContImp1*	0.908	48.684	0.019	0.838	0.939	0.903
	ContImp2	0.925	68.667	0.013			
	ContImp6	0.913	44.906	0.020			
Adaptiveness to InfoSec Threats	*Adp1*	0.832	20.682	0.040	0.604	0.884	0.835
	Adp2	0.804	27.749	0.029			
	Adp3	0.711	12.328	0.058			
	Adp4	0.769	20.194	0.038			
	Adp5	0.764	11.511	0.066			
Second-Order Absorptive Capacity	*Acq1*	0.795	22.076	0.036	0.666	0.952	0.944
	Acq2	0.779	17.880	0.044			
	Acq3	0.768	17.619	0.044			
	Assi1	0.794	25.127	0.032			
	Assi2	0.824	24.009	0.034			
	Assi3	0.827	24.894	0.033			
	Trans1	0.820	24.513	0.033			
	Trans2	0.844	29.172	0.029			
	Exp1	0.829	20.945	0.040			
	Exp2	0.877	48.968	0.018			
Acquisition	*Acq1*	0.847	27.802	0.030	0.734	0.892	0.818
	Acq2	0.893	38.115	0.023			
	Acq3	0.829	23.943	0.035			
Assimilation	*Assi1*	0.858	32.978	0.026	0.788	0.917	0.865
	Assi2	0.916	52.982	0.017			
	Assi3	0.887	38.526	0.023			
Transformation	*Trans1*	0.914	57.184	0.016	0.840	0.913	0.809
	Trans2	0.919	57.977	0.016			
Exploitation	*Exp1*	0.937	43.120	0.022	0.870	0.931	0.851
	Exp2	0.929	64.177	0.015			
Supportive Regulatory Env.	*RegEnv1*	0.884	34.583	0.026	0.731	0.891	0.818
	RegEnv2	0.810	17.025	0.048			
	RegEnv3	0.870	24.043	0.036			

Table 3.5. Matrix of Latent Constructs' Correlations

Construct	Means (S.D.)	1	2	3	4	5	6
1. Continuous Improvement	3.682 (0.857)	**0.915**					
2. Adaptiveness to Threats	3.598 (0.759)	0.706	**0.777**				
3. Absorptive Capacity	4.011 (0.702)	0.637	0.673	**0.816**			
4. Supportive Regulatory Env.	3.279 (0.810)	0.463	0.472	0.342	**0.855**		
5. Org Age	-	-0.044	-0.211	-0.086	-0.202	**1.000**	
6. Org Size	-	0.124	-0.032	0.029	0.110	0.434	**1.000**

Shaded cells in the diagonal row are AVE square roots.

3.5.3. Structural Model

The results of data analysis, including R-squares, standardized path coefficients, associated t-values and paths significance, are depicted in Figure 3.2. To test the significance of path coefficients in the structural model, we used a bootstrapping approach with 1,000 resamples. The R-square value of continuous improvement in information security management and adaptiveness to information security threats are 0.565 and 0.480, respectively. The results suggest that nearly 57% of the variance in continuous improvement in information security management can be explained by adaptiveness to information security threats. Moreover, approximately 50% of the variance in the adaptiveness to information security threats can be explained by absorptive capacity. Because the amount of variances explained are larger than 10 percent, we can claim that the proposed model is valid and acceptable (Falk and Miller 1992).

The results of testing direct relationships indicate that adaptiveness to information security threats ($\beta= 0.530$, $p<0.001$) and absorptive capacity ($\beta= 0.280$, $p<0.001$) both have positive significant effects on continuous improvement in information security management, supporting H1 and H3. The results also indicate that absorptive capacity ($\beta= 0.661$, $p<0.001$) has a positive effect on adaptiveness to information security threats, as anticipated in H2. The indirect effect of absorptive capacity on continuous improvement in information security management is also significant ($\beta= 0350$, $p<0.001$). Because the direct path from absorptive capacity to continuous improvement in information security management was still significant when indirect paths were not dropped, we conclude that the relationship between absorptive capacity and continuous improvement in information security management is partially mediated by adaptiveness to information security threats. Therefore, H4 is supported.

We note that in order to account for organizational differences in the proposed model, we have followed the related literature and controlled for the effect of size and age of the respondents' organizations (Hsu et al. 2012). Among these variables, organization age has a marginal effect on adaptiveness to information security threats. This results suggests managers of older organizations are less aware of the needs to be alert and adaptive to information security threats (β= -0.163, $p<0.05$).

Moreover, to test the moderating effect, a construct was created by cross-multiplying all the items of appropriate constructs, standardized to avoid multicollinearity, and included in the main model (Toothaker 1994). This approach is called product-indicator (Chin et al. 2003). Our results show that supportive regulatory environment positively moderates the relationship between absorptive capacity and adaptiveness to information security threats (β= 0.226, $p<0.05$). Therefore, H5 is also supported.

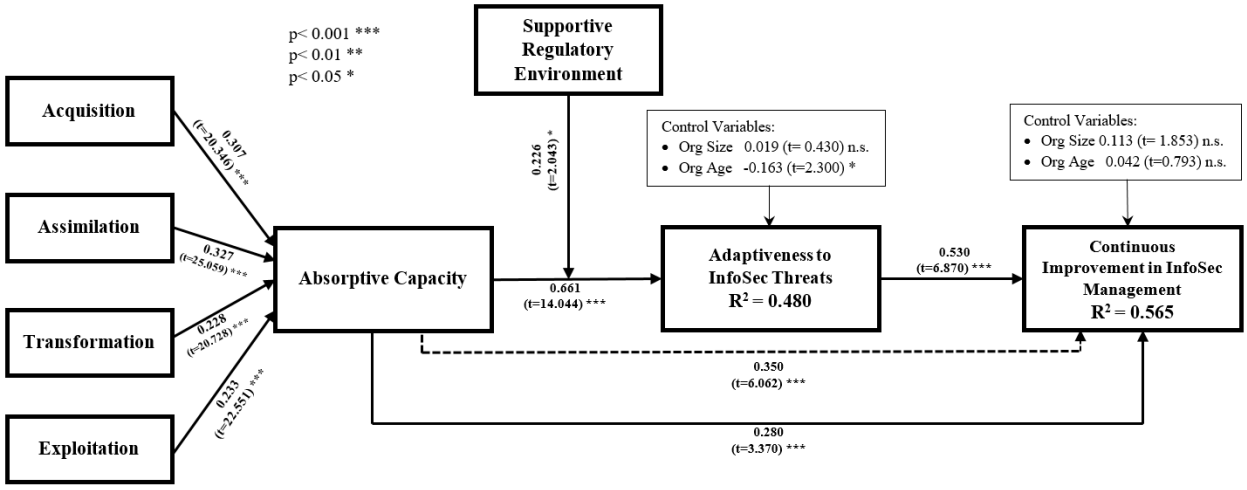

Figure 3.2. PLS Results

3.6. DISCUSSION

The purpose of this study is to explore what influence continuous improvement process in organizations in the context of information security management. By applying the absorptive capacity perspective, this study proposes a conceptual model wherein absorptive capacity affects continuous improvement of information security management both directly and indirectly. Our empirical findings suggest that in addition to the direct impact, absorptive capacity indirectly influence continuous improvement through organizations' adaptiveness to information security threats. Additionally, our findings indicate that for organizations which are active in industries with higher levels of supportive regulatory environment, the effect of organizations' absorptive capacity is stronger on their adaptiveness to information security threats. Table 3.6 summarizes the hypotheses testing results.

Table 3.6. Summary of Results

Hypothesis	Result
H1. An organization's adaptiveness to information security threats is positively related to its continuous improvement in information security management.	Supported
H2. An organization's absorptive capacity is positively related to its adaptiveness to information security threats.	Supported
H3. An organization's absorptive capacity is positively related to its continuous improvement in information security management.	Supported
H4. An organization's adaptiveness to information security threats mediates the relationship between its absorptive capacity and its continuous improvement in information security management.	Supported
H5. The effect of absorptive capacity to adaptiveness to information security threats is stronger for organizations that operate in a more supportive regulatory environment.	Supported

3.6.1. Contribution to Theory

Taken together, this study makes several theoretical contributions. First, to the best of our knowledge, this study is among the first to explore the concept of organizational continuous improvement in the context of information security management. Our conceptualization of information security management as a continuous organizational effort is explicitly important because the significantly increasing dependence on information makes organizations more

vulnerable to information security risks and threats. Moreover, the potential consequence of those risks can lead to competitive disadvantage in hypercompetitive environments.

Second, this study enriches continuous improvement literature by exploring how absorptive capacity could impact this construct through various paths, i.e., directly as well as indirectly by shaping organizational adaptiveness to information security threats. The existing literature has merely examined explorative aspect of organizational learning which is creation and gain of the knowledge (Zahra and George 2002). However, the findings of this study point towards the significant effect of both explorative and exploitative aspects of learning on continuous improvement. Moreover, our findings deepen this understanding by shedding light on the mediation role of adaptiveness capability to this relationship.

Third, the results of the study lend empirical support to the idea that supportive regulations can strength the way through which absorptive capacity affects adaptiveness of organizations. This is an important finding because it provides evidence showing how the interaction of organizational capabilities and external environment can bring benefits to organizations and help them be more flexible in terms of anticipating new information security threats and risks.

3.6.2 Implications for Practice

This study also has several practical implications for managers and policy makers. As we described at the beginning of the paper, although organizations have invested a great amount of resources to constantly improve information security management processes, only a small percent of them could achieve their expected outcomes. In other words, monetary investments per se do not bring the maximum efficiency that organizations have been looking for (Hoem and Lodgaard 2016; Liker and Franz 2011). Thus, it is critical for executives and managers to uncover and develop certain organizational capabilities that facilitate the continuous improvement process and

optimize the obtained outcomes. Our findings presented evidence related to how two of the important organizational capabilities – absorptive capacity and adaptiveness – could both directly and indirectly strengthen such outcomes.

Moreover, our findings provide some essential guidance and knowledge for policy makers in terms of the importance to set up a supportive regulatory environment, which could bring extra motivation for organizations and help them enhance their adaptiveness capability and flexibility in react to information security threats. Such enhancements will have significant effects on reducing the chance of information system failure due to security threats, and minimize the long term risk of information security attacks and breaches for organizations. Furthermore, the results of this study may motivate policy makers to set aside extra funding for organizations that have plans to prioritize and invest more on the acquisition, assimilation, transformation, and exploitation of knowledge in order to strengthen their absorptive capabilities.

3.6.3. Limitations and Future Research

Finally, we acknowledge that it is also important to evaluate this study's contributions in light of some undeniable limitations. First, the data was collected from a single source, i.e., managers with information security knowledge, which makes the study subjective in nature. Even though the results of our data analysis suggests that common method bias is not a serious concern for this dataset, future empirical studies can improve upon this limitation through the use of multiple data sources. Second, conducting this study in the context of United States may raise the possibility of regional biases. This design could possibly limit the external validity of this study and offer viable future opportunities to replicate and extend the current study in the context of other countries and economies. Last, as there are still some unexplained portions of variance in our dependent variable, continuous information security management improvement (according to

the coefficient of determination as suggested by our data analysis results). Future studies should consider examining the effects of other unidentified organizational or environmental factors that may provide more insights to this important phenomenon.

REFERENCES

Abu-Shanab, E. A. 2011. "Education level as a technology adoption moderator," *ICCRD2011 - 2011 3rd International Conference on Computer Research and Development*, (1:August), pp. 324–328 (doi: 10.1109/ICCRD.2011.5764029).

Ajzen, and Fishbein, M. 1980. *Understanding attitudes and predicting social behaviour*, Englewood Cliffs, NJ: Prentice Hall (available at http://www.citeulike.org/group/38/article/235626).

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, (50:2), pp. 179–211 (doi: 10.1016/0749-5978(91)90020-T).

Ajzen, I. 1999. "Dual-Mode Processing in the Pursuit of Insight Is No Vice," *Psychological Inquiry*, (10:2), Lawrence Erlbaum Associates, Inc. , pp. 110–112 (doi: 10.1207/S15327965PL100202).

Ajzen, I., and Fishbein, M. 1977. "Attitude-behavior relations: A theoretical analysis and review of empirical research.," *Psychological Bulletin*, (84:5), American Psychological Association, pp. 888–918 (doi: 10.1037/0033-2909.84.5.888).

Alhussain, T., and Drew, S. 2012. "Developing a Theoretical Framework for the Adoption of Biometrics in M-Government Applications Using Grounded Theory," in *Security Enhanced Applications for Information Systems*, Christos Kalloniatis (ed.), InTech , p. 83.

Anand, G., Ward, P. T., Tatikonda, M. V., and Schilling, D. A. 2009. "Dynamic capabilities through continuous improvement infrastructure," *Journal of Operations Management*, (27:6), Elsevier, pp. 444–461 (doi: 10.1016/J.JOM.2009.02.002).

Anderson, P., and Tushman, M. L. 2001. "Organizational Environments and Industry Exit: the Effects of Uncertainty, Munificence and Complexity," *Industrial and Corporate Change*, (10:3), Oxford University Press, pp. 675–711 (doi: 10.1093/icc/10.3.675).

Ang, S., and Cummings, L. L. 1997. "Strategic Response to Institutional Influences on Information Systems Outsourcing," *Organization Science*, (8:3), INFORMS , pp. 235–256 (doi: 10.1287/orsc.8.3.235).

Argyris, C., and Schon, D. 1978. *Organizational learning: A theory of action approach*, Reading, MA: Addision Wesley.

Auh, S., and Menguc, B. 2005. "Balancing exploration and exploitation: The moderating role of competitive intensity," *Journal of Business Research*, (58:12), Elsevier, pp. 1652–1661 (doi: 10.1016/J.JBUSRES.2004.11.007).

Bachmann, M. 2014. "Passwords are Dead: Alternative Authentication Methods," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, IEEE, September, pp. 322–322 (doi: 10.1109/JISIC.2014.67).

Barlas, S., Queen, R., Radowitz, J., Shillam, P., and Williams, K. 2007. "Top 10 technology concerns," *Strategic Finance*, (88:10), p. 21 (available at https://search.proquest.com/docview/229770014?pq-origsite=gscholar).

Basadur, M., Gelade, G., and Basadur, T. 2014. "Creative Problem-Solving Process Styles, Cognitive Work Demands, and Organizational Adaptability," *The Journal of Applied*

Behavioral Science, (50:1), SAGE PublicationsSage CA: Los Angeles, CA, pp. 80–115 (doi: 10.1177/0021886313508433).

Bateman, T. S., and Crant, J. M. 1999. "Proactive behavior: Meaning, impact, recommendations," *Business Horizons*, (42:3), pp. 63–70 (doi: 10.1016/S0007-6813(99)80023-8).

Beer, M., Voelpel, S. C., Leibold, M., and Tekie, E. B. 2005. "Strategic Management as Organizational Learning: Developing Fit and Alignment through a Disciplined Process," *Long Range Planning*, (38:5), Pergamon, pp. 445–465 (doi: 10.1016/J.LRP.2005.04.008).

Bessant, J., and Caffyn, S. 1997. "High-involvement innovation through continuous improvement," *International Journal of Technology Management*, (14:1), p. 7 (doi: 10.1504/IJTM.1997.001705).

Bhuiyan, N., and Baghel, A. 2005. "An overview of continuous improvement: from the past to the present," *Management Decision*, (43:5), Emerald Group Publishing Limited, pp. 761–771 (doi: 10.1108/00251740510597761).

Bock, G.-W., Zmud, R. W., Kim, Y.-G., and Lee, J.-N. 2005. "Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate," *MIS Quarterly*, (29:1), pp. 87–111 (available at http://eds.a.ebscohost.com/abstract?site=eds&scope=site&jrnl=02767783&AN=16313366&h=ErTmPPE62YNm3LoPzVsoBOOjYNelljvQQeJKiKl32vT9IWE0Hsr3KE%2B8AUo7lWeKA82Qe7qhTENkicGXJBMLow%3D%3D&crl=f&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3Fdir).

Boer, H., Berger, A., Chapman, R., and Gertsen, F. 2017. *CI Changes from Suggestion Box to Organisational Learning: Continuous Improvement in Europe and Australia*, Routledge (available at https://books.google.com/books?hl=en&lr=&id=QflADwAAQBAJ&oi=fnd&pg=PT6&dq=CI+changes:+from+suggestion+box+to+organisational+learning,+Continuous+Improvement+in+Europe+and+Australia&ots=DZ2PMTnoRI&sig=H-jVs-IAti9yQZSaDbXroUGlnh0#v=onepage&q=CI changes%3A).

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., and Senior, A. W. 2004. *Guide to biometrics*, New York: Springer-Verlag.

Bonneau, J., Herley, C., Oorschot, P. C. van, and Stajano, F. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *2012 IEEE Symposium on Security and Privacy*, IEEE, May, pp. 553–567 (doi: 10.1109/SP.2012.44).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly*, (39:4), pp. 837–864 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2607190).

Boyer, W., and McQueen, M. 2008. "Ideal Based Cyber Security Technical Metrics for Control Systems," Springer, Berlin, Heidelberg, pp. 246–260 (doi: 10.1007/978-3-540-89173-4_21).

Boynton, B. C. 2007. "Identification of process improvement methodologies with application in information security," in *Proceedings of the 4th annual conference on Information security curriculum development - InfoSecCD '07*, New York, New York, USA: ACM Press, p. 1 (doi:

10.1145/1409908.1409939).

Brajer-Marczak, R. 2014. “Employee engagement in continuous improvement of processes,” *Management*, (18:2), De Gruyter Open, pp. 88–103 (doi: 10.2478/manment-2014-0044).

Brauch, H. G. 2011. “Concepts of Security Threats, Challenges, Vulnerabilities and Risks,” Springer Berlin Heidelberg, pp. 61–106 (doi: 10.1007/978-3-642-17776-7_2).

Bresnahan, T. F., Brynjolfsson, E., and Hitt, L. M. 2002. “Information Technology, Workplace Organization, and the Demand for Skilled Labor: Firm-Level Evidence,” *The Quarterly Journal of Economics*, (117:1), Oxford University Press, pp. 339–376 (doi: 10.1162/003355302753399526).

Burkhardt, M. E., and Brass, D. J. 1990. “Changing Patterns or Patterns of Change: The Effects of a Change in Technology on Social Network Structure and Power,” *Administrative Science Quarterly*, (35:1), p. 104 (doi: 10.2307/2393552).

Cabantous, L., and Gond, J.-P. 2011. “Rational Decision Making as Performative Praxis: Explaining Rationality’s Éternel Retour,” *Organization Science*, (22:3), INFORMS, pp. 573–586 (doi: 10.1287/orsc.1100.0534).

Camisón, C., and Forés, B. 2010. “Knowledge absorptive capacity: New insights for its conceptualization and measurement,” *Journal of Business Research*, (63:7), Elsevier, pp. 707–715 (doi: 10.1016/J.JBUSRES.2009.04.022).

Carley, K. M., and Behrens, D. M. 1999. *Organizational and individual decision making. Handbook of Systems Engineering and Management.*, New York: Wiley-Interscience.

Carpenter, M. A., and Fredrickson, J. W. 2001. “Top Management Teams, Global Strategic Posture, and the Moderating Role of Uncertainty,” *Academy of Management Journal*, (44:3), Academy of Management, pp. 533–545 (doi: 10.2307/3069368).

Carter, N. M. 1990. “Small firm adaptation: Responses of physicians’ organizations to regulatory and competitive uncertainty.,” *Academy of Management Journal*, (33:2), pp. 307–333 (doi: 10.5465/256327).

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,” *International Journal of Electronic Commerce*, (9:1), Taylor & Francis, Ltd., pp. 69–104 (doi: 10.2307/27751132).

Chaiken, S., and Trope, Y. 1999. *Dual-process theories in social psychology*, Guilford Press (available at https://books.google.com/books?hl=en&lr=&id=5X_auIBx99EC&oi=fnd&pg=PA3&dq=Chaiken+%26+Trope,+1999&ots=OIVU-R9jsh&sig=gZvm91R7p2dPdA5sm1U6RMqpiDs#v=onepage&q=Chaiken %26 Trope%2C 1999&f=false).

Chang, L. 2016. “Is The Death of the Password Near?,” (available at http://www.digitaltrends.com/computing/death-of-the-password/; retrieved January 24, 2017).

Chen, M. A. 2007. “Rethinking the Informal Economy: Linkages with the Formal Economy and the Formal Regulatory Environment,” (available at http://www.un.org/esa/desa/).

Chin, T., Tsai, S.-B., Fang, K., Zhu, W., Yang, D., Liu, R., and Tsuei, R. T. C. 2016. "EO-Performance relationships in Reverse Internationalization by Chinese Global Startup OEMs: Social Networks and Strategic Flexibility," *PLOS ONE*, (F. van Rijnsoever, ed.), (11:9), Public Library of Science, p. e0162175 (doi: 10.1371/journal.pone.0162175).

Chin, W., and Marcolin, B. 1995. "The holistic approach to construct validation in IS research: Examples of the interplay between theory and measurement," in *Administrative Sciences Association of Canada-Annual Conference*, p. Vol. 16, 34-43.

Chin, W. W. 1998. "Commentary: Issues and Opinion on Structural Equation Modeling," *MIS Quarterly*, (22:1), pp. vii–xvi (available at https://www.jstor.org/stable/249674?seq=1#page_scan_tab_contents).

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study," *Information Systems Research*, (14:2), pp. 189–217 (doi: 10.1287/isre.14.2.189.16018).

Choo, C. W. 1996. "The knowing organization: How organizations use information to construct meaning, create knowledge and make decisions," *International Journal of Information Management*, (16:5), pp. 329–340 (doi: 10.1016/0268-4012(96)00020-5).

Chou, T.-C., Robert, R. G., and Powell, P. L. 1998. "An empirical study of the impact of information technology intensity in strategic investment decisions," *Technology Analysis & Strategic Management*, (10:3), Carfax Publishing Company , pp. 325–340 (doi: 10.1080/09537329808524320).

Cohen, W., and Levinthal, D. A. 2000. "Absorptive Capacity: A New Perspective on Learning and Innovation," in *Strategic Learning in a Knowledge Economy*, Elsevier, pp. 39–67 (doi: 10.1016/B978-0-7506-7223-8.50005-8).

Cohen, W. M., and Levinthal, D. A. 1989. "Innovation and Learning: The Two Faces of R & D," *The Economic Journal*, (99:397), WileyRoyal Economic Society, p. 569 (doi: 10.2307/2233763).

Conner, F. W., and Coviello, A. W. 2004. "Information security governance: a call to action," (available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.535.6634&rep=rep1&type=pdf).

Cooper, C. 2015. "Can cybersecurity provide competitive advantage?," *IDG Communications, Inc. ("IDG"), publisher of CSO* (available at http://theartofthehack.com/can-cybersecurity-provide-competitive-advantage/; retrieved December 31, 2017).

Culnan, M. J., Foxman, E. R., and Ray, A. W. 2008. "Why IT executives should help employees secure their home computers," *MIS Quarterly Executive*, (7:1), pp. 49–56 (available at http://misqe.org/ojs2/index.php/misqe/article/view/161).

D'Costa-Alphonso, M., and Lane, M. 2010. "The Adoption of Single Sign-On and Multifactor Authentication in Organizations–A Critical Evaluation Using TOE Framework," in *Information in Motion: The Journal Issues in Informing Science and Information Technology*, (7th ed.), p. 161 (available at https://books.google.com/books?hl=en&lr=&id=fnz6NxSXzGcC&oi=fnd&pg=PA161&dq=The+Adoption+of+Single+Sign-On+and+Multifactor+Authentication+in+Organizations–

A+Critical+Evaluation+Using+TOE+Framework&ots=mGmcWPWpNm&sig=PBfyD1B5Wy74keTiM1lfvhss3So#v=o).

Daft, R. L. 1978. "A Dual-Core Model of Organizational Innovation.," *Academy of Management Journal*, (21:2), Academy of Management, pp. 193–210 (doi: 10.2307/255754).

Damanpour, F. 1991. "Organizational Innovation: A Meta-Analysis Of Effects Of Determinants and Moderators," *Academy of Management Journal*, (34:3), Academy of Management, pp. 555–590 (doi: 10.2307/256406).

Damanpour, F., and Schneider, M. 2006. "Phases of the Adoption of Innovation in Organizations: Effects of Environment, Organization and Top Managers1," *British Journal of Management*, (17:3), Blackwell Publishing Ltd, pp. 215–236 (doi: 10.1111/j.1467-8551.2006.00498.x).

Damanpour, F., and Schneider, M. 2009. "Characteristics of Innovation and Innovation Adoption in Public Organizations: Assessing the Role of Managers," *Journal of Public Administration Research and Theory*, (19:3), Oxford University Press, pp. 495–522 (doi: 10.1093/jopart/mun021).

Dasgupta, D., Roy, A., and Nag, A. 2016. "Toward the design of adaptive selection strategies for multi-factor authentication," *Computers & Security*, (63), pp. 85–116 (doi: 10.1016/j.cose.2016.09.004).

Davies, E. L., Martin, J., and Foxcroft, D. R. 2013. "Young people talking about alcohol: Focus groups exploring constructs in the prototype willingness model," *Drugs: Education, Prevention and Policy*, (20:4), Taylor & Francis, pp. 269–277 (doi: 10.3109/09687637.2012.726662).

DeLone, W. H., and McLean, E. R. 2003. "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems*, (19:4), pp. 9–30.

Dewett, T., and Jones, G. R. 2001. "The role of information technology in the organization: a review, model, and assessment," *Journal of Management*, (27:3), Sage PublicationsSage CA: Thousand Oaks, CA, pp. 313–346 (doi: 10.1177/014920630102700306).

Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, (11:2), Blackwell Science Ltd, pp. 127–153 (doi: 10.1046/j.1365-2575.2001.00099.x).

Dodel, M., and Mesch, G. 2017. "Cyber-victimization preventive behavior: A health belief model approach," *Computers in Human Behavior*, (68), Pergamon, pp. 359–367 (doi: 10.1016/J.CHB.2016.11.044).

Dohnke, B., Steinhilber, A., and Fuchs, T. 2015. "Adolescents' eating behaviour in general and in the peer context: Testing the prototype-willingness model," *Psychology & Health*, (30:4), Routledge, pp. 381–399 (doi: 10.1080/08870446.2014.974604).

Downs, G. W., Mohr, L. B., and Mohr, L. B. 1976. "Conceptual Issues in the Study of Innovation," *Administrative Science Quarterly*, (21:4), Sage Publications, Inc.Johnson Graduate School of Management, Cornell University, p. 700 (doi: 10.2307/2391725).

Dubois, É., Heymans, P., Mayer, N., and Matulevičius, R. 2010. "A Systematic Approach to Define the Domain of Information System Security Risk Management," in *Intentional*

Perspectives on Information Systems Engineering, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 289–306 (doi: 10.1007/978-3-642-12544-7_16).

Duncan, R. B. 1972. "Characteristics of Organizational Environments and Perceived Environmental Uncertainty," *Administrative Science Quarterly*, (17:3), p. 313 (doi: 10.2307/2392145).

Dunning, D., Perie, M., and Story, A. L. 1991. "Self-serving prototypes of social categories.," *Journal of Personality and Social Psychology*, (61:6), American Psychological Association, pp. 957–968 (doi: 10.1037/0022-3514.61.6.957).

Eich, J., John, L., Smith, K., and Cankaya, E. C. 2016. "Extended Password Security via Cloud: CloudPass," Springer, Cham, pp. 33–42 (doi: 10.1007/978-3-319-41932-9_4).

Elbertsen, L., and Reekum, R. Van. 2008. "To ERP or not to ERP? Factors influencing the adoption decision," *International Journal of Management and Enterprise Development*, (5:3), p. 310 (doi: 10.1504/IJMED.2008.017434).

Elliott, S. J., Kukula, E. P., and Sickler, N. C. 2004. "The Challenges of the Environment and the Human / Biometric Device Interaction on Biometric System Performance," in *International Workshop on Biometric Technologies-Special forum on Modeling and Simulation in Biometric Technology*, Calgary, Alberta, Canada.

Epstein, S. 2003. "Cognitive-experiential self-theory: an integrative theory of personality," in *Handbook of Psychology: Personality and Social Psychology*, T. Millon and M. J. Lerner (eds.), Hoboken, NJ.: Wiley, pp. 159–184 (available at https://books.google.com/books?hl=en&lr=&id=lBXf1slZBDwC&oi=fnd&pg=PR7&dq=Handbook+of+Psychology:+Personality+and+Social+Psychology&ots=kX3Y2nNhdo&sig=7TOqfT1p3fwohUP3wMrBCHwIzJA#v=onepage&q=Handbook of Psychology%3A Personality and Social Psy).

Epstein, S., and Seymour. 1994. "Integration of the cognitive and the psychodynamic unconscious.," *American Psychologist*, (49:8), American Psychological Association, pp. 709–724 (doi: 10.1037/0003-066X.49.8.709).

Evans, J. S. B. T. 1984. "Heuristic and analytic processes in reasoning*," *British Journal of Psychology*, (75:4), Blackwell Publishing Ltd, pp. 451–468 (doi: 10.1111/j.2044-8295.1984.tb01915.x).

Falk, R. F., and Miller, N. B. 1992. *A primer for soft modeling.*, University of Akron Press.

Farrell, D. 2003. "The real new economy.," *Harvard business review*, (81:10), pp. 104–12, 138 (available at http://www.ncbi.nlm.nih.gov/pubmed/14521102).

Finkelstein, S., and Hambrick, D. 1996. *Strategic leadership: Top executives and their effects on organizations*, South-Western Pub.

Fiol, C. M., and Lyles, M. A. 1985. "Organizational Learning.," *Academy of Management Review*, (10:4), pp. 803–813 (doi: 10.5465/AMR.1985.4279103).

Fogalin, K. 2009. "Improving the Management of Information Security in Canadian Government Departments: Taking Lessons from the ISO/IEC 27001 Standard to Make Continuous, Incremental, and Enduring Improvements," (available at https://www.sans.org/reading-room/whitepapers/leadership/improving-management-information-security-canadian-

government-departments-33063).

Fornell, C., and Bookstein, F. L. 1982. “Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory,” *Journal of Marketing Research*, (19:4), p. 440 (doi: 10.2307/3151718).

Fornell, C., and Larcker, D. F. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *Journal of Marketing Research*, (18:1), pp. 39–50 (doi: 10.2307/3151312).

Frese, M., Kring, W., Soose, A., and Zempel, J. 1996. “Personal initiative at work: Differences between East and West Germany,” *Academy of Management Journal*, (39:1), Academy of Management, pp. 37–63 (doi: 10.2307/256630).

Fritz, C., and Sonnentag, S. 2009. “Antecedents of Day-Level Proactive Behavior: A Look at Job Stressors and Positive Affect During the Workday†,” *Journal of Management*, (35:1), SAGE PublicationsSage CA: Los Angeles, CA, pp. 94–111 (doi: 10.1177/0149206307308911).

Fynes, B., de Búrca, S., and Marshall, D. 2004. “Environmental uncertainty, supply chain relationship quality and performance,” *Journal of Purchasing and Supply Management*, (10:4), pp. 179–190 (doi: 10.1016/j.pursup.2004.11.003).

Gaur, A. S., Mukherjee, D., Gaur, S. S., and Schmid, F. 2011. “Environmental and Firm Level Influences on Inter-Organizational Trust and SME Performance,” *Journal of Management Studies*, (48:8), Blackwell Publishing Ltd, pp. 1752–1781 (doi: 10.1111/j.1467-6486.2011.01011.x).

Gefen, D., Straub, D. W., Boudreau, M.-C., Gefen, D., Straub, D. W., and Boudreau, M. 2000. “Structural equation modeling and regression: Guidelines for research practice,” *Communications of AIS*, (4:7).

General, A. A. 2002. “ACT Auditor General’s office performance audit report V8 car races in Canberra–costs and benefits,.”

Geraci, A., Katki, F., McMonegal, L., Meyer, B., Lane, J., Wilson, P., Radatz, J., Yee, M., Porteous, H., and Springsteel, F. 1991. *IEEE standard computer dictionary : a compilation of IEEE standard computer glossaries, 610*, Institute of Electrical and Electronics Engineers.

Gerrard, M., Gibbons, F. X., Houlihan, A. E., Stock, M. L., and Pomery, E. A. 2008. “A dual-process approach to health risk decision making: The prototype willingness model,” *Developmental Review*, (28:1), pp. 29–61 (doi: 10.1016/j.dr.2007.10.001).

Gerrard, M., Gibbons, F. X., Stock, M. L., Lune, L. S. Vande, and Cleveland, M. J. 2005. “Images of Smokers and Willingness to Smoke Among African American Pre-adolescents: An Application of the Prototype/Willingness Model of Adolescent Health Risk Behavior to Smoking Initiation,” *Journal of Pediatric Psychology*, (30:4), Oxford University Press, pp. 305–318 (doi: 10.1093/jpepsy/jsi026).

Gibbons, F. X., and Gerrard, M. 1995. “Predicting young adults’ health risk behavior.,” *Journal of Personality and Social Psychology*, (69:3), American Psychological Association, pp. 505–517 (doi: 10.1037/0022-3514.69.3.505).

Gibbons, F. X., and Gerrard, M. 1997. *Health images and their effects on health behavior.*, Lawrence Erlbaum Associates Publishers (available at http://psycnet.apa.org/psycinfo/1997-

09050-002).

Gibbons, F. X., Gerrard, M., Blanton, H., and Russell, D. W. 1998. "Reasoned action and social reaction: Willingness and intention as independent predictors of health risk.," *Journal of Personality and Social Psychology*, (74:5), American Psychological Association, pp. 1164–1180 (doi: 10.1037/0022-3514.74.5.1164).

Gibbons, F. X., Gerrard, M., and Lane, D. J. 2003. "A social reaction model of adolescent health risk," in *Social psychological foundations of health and illness*, Blackwell Publishing Ltd, pp. 107–136.

Gibbons, F. X., Gerrard, M., and McCoy, S. B. 1995. "Prototype Perception Predicts (Lack of) Pregnancy Prevention," *Personality and Social Psychology Bulletin*, (21:1), Sage PublicationsSage CA: Thousand Oaks, CA, pp. 85–93 (doi: 10.1177/0146167295211009).

Gigya. 2016. "Survey Guide: Businesses Should Begin Preparing for the Death of the Password," Mountain View, CA.

Glover, W. J., Farris, J. A., and Van Aken, E. M. 2015. "The relationship between continuous improvement and rapid improvement sustainability," *International Journal of Production Research*, (53:13), Taylor & Francis, pp. 4068–4086 (doi: 10.1080/00207543.2014.991841).

Goel, S., and Shawky, H. A. 2009. "Estimating the market impact of security breach announcements on firm values," *Information & Management*, (46:7), North-Holland, pp. 404–410 (doi: 10.1016/J.IM.2009.06.005).

Gonzalez, R. V. D., and Martins, M. F. 2016. "Capability for continuous improvement," *The TQM Journal*, (28:2), Emerald Group Publishing Limited , pp. 250–274 (doi: 10.1108/TQM-07-2014-0059).

Van Gool, E., Van Ouytsel, J., Ponnet, K., and Walrave, M. 2015. "To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model," *Computers in Human Behavior*, (44), pp. 230–239 (doi: 10.1016/j.chb.2014.11.036).

Gordon, L. A., and Loeb, M. P. 2002. "The economics of information security investment," *ACM Transactions on Information and System Security*, (5:4), ACM, pp. 438–457 (doi: 10.1145/581271.581274).

Gordon, L. A., and Miller, D. 1976. "A contingency framework for the design of accounting information systems," *Accounting, Organizations and Society*, (1:1), pp. 59–69 (doi: 10.1016/0361-3682(76)90007-6).

Gordon, L. A., and Narayanan, V. K. 1984. "Management accounting systems, perceived environmental uncertainty and organization structure: An empirical investigation," *Accounting, Organizations and Society*, (9:1), pp. 33–47 (doi: 10.1016/0361-3682(84)90028-X).

Grandon, E. E., and Pearson, J. M. 2004. "Electronic commerce adoption: an empirical study of small and medium US businesses," *Information & Management*, (42:1), pp. 197–216 (doi: 10.1016/j.im.2003.12.010).

Griffin, M. A., NEAL, A., and PARKER, S. K. 2007. "A New Model of Work Role Performance: Positive Behavior in Uncertain and Interdependent Context," *Academy of Management*

Journal, (50:2), Academy of Management, pp. 327–347 (doi: 10.5465/AMJ.2007.24634438).

Grover, V. 1993. "An Empirically Derived Model for the Adoption of Customer-based Interorganizational Systems," *Decision Sciences*, (24:3), Blackwell Publishing Ltd, pp. 603–640 (doi: 10.1111/j.1540-5915.1993.tb01295.x).

Habib, H., Colnago, J., Melicher, W., Ur, B., Segreti, S., Bauer, L., Christin, N., and Cranor, L. 2017. "Password Creation in the Presence of Blacklists," in *Usable Security Mini Conference*, San Diego, California (doi: 10.14722/usec.2017.23043).

Hair, J. F., E., A. R., L., T. R., and C., B. W. 1995. *Multivariate Data Analysis with Readings*, (4th ed.), Englewood Cliffs, NJ: Prentice Hall.

Hammer, J. H., and Vogel, D. L. 2013. "Assessing the utility of the willingness/prototype model in predicting help-seeking decisions.," *Journal of Counseling Psychology*, (60:1), American Psychological Association, pp. 83–97 (doi: 10.1037/a0030449).

Han, K., Chang, Y. B., and Hahn, J. 2011. "Information Technology Spillover and Productivity: The Role of Information Technology Intensity and Competition," *Journal of Management Information Systems*, (28:1), pp. 115–146 (doi: 10.2753/MIS0742-1222280105).

Han, K., Kauffman, R. J., and Nault, B. R. 2011. "Research Note —Returns to Information Technology Outsourcing," *Information Systems Research*, (22:4), pp. 824–840 (doi: 10.1287/isre.1100.0290).

Harper, C. A., and Hogue, T. E. 2014. "A Prototype-Willingness Model of Sexual Crime Discourse in England and Wales," *The Howard Journal of Criminal Justice*, (53:5), pp. 511–524 (doi: 10.1111/hojo.12095).

Hartline, M. D., and Ferrell, O. C. 1996. "The Management of Customer-Contact Service Employees: An Empirical Investigation," *Journal of Marketing*, (60:4), p. 52 (doi: 10.2307/1251901).

Hayes, D. C. 1977. "The Contingency Theory of Managerial Accounting," *The Accounting Review*, (52:1), pp. 22–39 (doi: 10.2307/2490007).

Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M., Singh, H., Teece, D., and Winter, S. G. 2007. *Dynamic capabilities : understanding strategic change in organizations*, Malden, MA: Blackwell Pub (available at https://books.google.com/books?hl=en&lr=&id=u0Tuh5vixLkC&oi=fnd&pg=PR6&dq=Dynamic+Capabilities:+Understanding+Strategic+Change+in+Organizations&ots=uJkY7UavsH&sig=70zZQ53rFPii2cAFU2hmkTMP32Y#v=onepage&q=Dynamic Capabilities%3A Understanding Strategi).

Henseler, J., Ringle, C. M., and Sinkovics, R. R. 2009. "The use of partial least squares path modeling in international marketing," in *New challenges to international marketing*, Advances in International Marketing, (Vol. 20), Bingley: Emerald Group Publishing, pp. 277–319 (doi: 10.1108/S1474-7979(2009)0000020014).

Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, (18:2), Palgrave Macmillan UK, pp. 106–125 (doi: 10.1057/ejis.2009.6).

Héroux, S., and Fortin, A. 2016. "The Influence of IT Governance, IT Competence and IT-

Business Alignment on Innovation," *Cahier de recherche*, (04), p. 38 (available at http://www.cifo.uqam.ca/publications/pdf/2016-04.pdf).

Hitt, M. A., Keats, B. W., and DeMarie, S. M. 1998. "Navigating in the new competitive landscape: Building strategic flexibility and competitive advantage in the 21st century.," *Academy of Management Perspectives*, (12:4), pp. 22–42 (doi: 10.5465/AME.1998.1333922).

Hoem, O., and Lodgaard, E. 2016. "Model for Supporting Lasting Managerial Efforts in Continuous Improvement: A Case Study in Product Engineering," *Procedia CIRP*, (50), Elsevier, pp. 38–43 (doi: 10.1016/J.PROCIR.2016.05.020).

Hoffman, D. L., Novak, T. P., and Peralta, M. 1999. "Building consumer trust online," *Communications of the ACM*, (42:4), ACM, pp. 80–85 (doi: 10.1145/299157.299175).

Hoo, K. J. S. 2000. "How Much Is Enough? A Risk-Management Approach to Computer Security," Stanford, Calif (available at https://cisac.fsi.stanford.edu/sites/default/files/soohoo.pdf).

Hsu, C., Lee, J.-N., and Straub, D. W. 2012. "Institutional Influences on Information Systems Security Innovations," *Information Systems Research*, (23:3-part-2), pp. 918–939 (doi: 10.1287/isre.1110.0393).

Hukkelberg, S. S., and Dykstra, J. L. 2009. "Using the Prototype/Willingness model to predict smoking behaviour among Norwegian adolescents," *Addictive Behaviors*, (34:3), pp. 270–276 (doi: 10.1016/j.addbeh.2008.10.024).

Hyatt, D. E., and Ruddy, T. M. 1997. "An examination of the relationship between work group characteristics and performance: Once more into the breech," *Personnel Psychology*, (50:3), Blackwell Publishing Ltd, pp. 553–585 (doi: 10.1111/j.1744-6570.1997.tb00703.x).

Hyde, M. K., and White, K. M. 2010. "Are organ donation communication decisions reasoned or reactive? A test of the utility of an augmented theory of planned behaviour with the prototype/willingness model," *British Journal of Health Psychology*, (15:2), Blackwell Publishing Ltd, pp. 435–452 (doi: 10.1348/135910709X468232).

Iheagwara, C., Blyth, A., and Singhal, M. 2004. "Cost effective management frameworks for intrusion detection systems," *Journal of Computer Security*, (12:5), IOS Press, pp. 777–798 (doi: 10.3233/JCS-2004-12506).

Jaber, M. Y., Bonney, M., and Guiffrida, A. L. 2010. "Coordinating a three-level supply chain with learning-based continuous improvement," *International Journal of Production Economics*, (127:1), Elsevier, pp. 27–38 (doi: 10.1016/J.IJPE.2010.04.010).

Jain, A., Hong, L., and Pankanti, S. 2000. "Biometric identification," *Communications of the ACM*, (43:2), ACM, pp. 90–98 (doi: 10.1145/328236.328110).

James, T., Pirim, T., Boswell, K., Reithel, B., and Barkhi, R. 2006. "Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model," *Journal of Organizational and End User Computing; Hershey*, (18:3), pp. 1–24 (available at http://search.proquest.com/docview/199927583?pq-origsite=gscholar).

Jansen, J. J. P., Van Den Bosch, F. A. J., and Volberda, H. W. 2005. "Managing Potential and Realized Absorptive Capacity: How do Organizational Antecedents Matter?," *Academy of Management Journal*, (48:6), pp. 999–1015 (doi: 10.5465/AMJ.2005.19573106).

Javalgi, R. G., Traylor, M. B., Gross, A. C., and Lampman, E. 1994. "Awareness of Sponsorship and Corporate Image: An Empirical Investigation," *Journal of Advertising*, (23:4), Taylor & Francis Group , pp. 47–58 (doi: 10.1080/00913367.1943.10673458).

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, (34:3), Management Information Systems Research Center, University of Minnesota, pp. 549–566 (doi: 10.2307/25750691).

Jong, A. de, and de Ruyter, K. 2004. "Adaptive versus Proactive Behavior in Service Recovery: The Role of Self-Managing Teams," *Decision Sciences*, (35:3), Decision Sciences, pp. 457–491 (doi: 10.1111/j.0011-7315.2004.02513.x).

Jouini, M., Rabai, L. B. A., and Aissa, A. Ben. 2014. "Classification of Security Threats in Information Systems," *Procedia Computer Science*, (32), Elsevier, pp. 489–496 (doi: 10.1016/J.PROCS.2014.05.452).

Kalakota, R., and Whinston, A. B. 1996. *Frontiers of electronic commerce*, Reading, MA: Addison-Wesley.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. 2003. "An integrative study of information systems security effectiveness," *International Journal of Information Management*, (23:2), pp. 139–154 (doi: 10.1016/S0268-4012(02)00105-6).

Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce*, (12:1), pp. 69–91 (doi: 10.2753/JEC1086-4415120103).

Karagozoglu, N., and Lindell, M. 2000. "Environmental Management: Testing the Win-Win Model," *Journal of Environmental Planning and Management*, (43:6), Taylor & Francis Group , pp. 817–829 (doi: 10.1080/09640560020001700).

Kark, K., Penn, J., and Dill, A. 2009. "2008 CISO Priorities: The Right Objectives But the Wrong Focus," Cambridge, MA (available at http://www.mag-securs.com/mag/IMG/pdf/Forrester_2008_CISO_Priorities_The_Right_Objectives_But_The_Wrong_Focus.pdf).

Katz, R., and Tushman, M. 1979. "Communication patterns, project performance, and task characteristics: An empirical evaluation and integration in an R&D setting," *Organizational Behavior and Human Performance*, (23:2), pp. 139–162 (doi: 10.1016/0030-5073(79)90053-9).

Keats, B. W., and Hitt, M. A. 1988. "A Causal Model of Linkages Among Environmental Dimensions, Macro Organizational Characteristics, and Performance," *Academy of Management Journal*, (31:3), Academy of Management, pp. 570–598 (doi: 10.2307/256460).

Keeney, R. L. 1982. "Feature Article—Decision Analysis: An Overview," *Operations Research*, (30:5), INFORMS , pp. 803–838 (doi: 10.1287/opre.30.5.803).

Keister, L. A. 2002. "Adapting to Radical Change: Strategy and Environment in Piece-Rate Adoption During China's Transition," *Organization Science*, (13:5), INFORMS, pp. 459–474 (doi: 10.1287/orsc.13.5.459.7811).

Kessel, P. van, and Allan, K. 2015. "Creating trust in the digital world: EY's Global Information Security Survey 2015," (available at https://webforms.ey.com/Publication/vwLUAssets/ey-

global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf).

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2008. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems*, (44:2), pp. 544–564 (doi: 10.1016/j.dss.2007.07.001).

Kohlbacher, M. 2013. "The Impact of Dynamic Capabilities through Continuous Improvement on Innovation: the Role of Business Process Orientation," *Knowledge and Process Management*, (20:2), Wiley-Blackwell, pp. 71–76 (doi: 10.1002/kpm.1405).

Kohlbacher, M., and Gruenwald, S. 2011. "Process ownership, process performance measurement and firm performance," *International Journal of Productivity and Performance Management*, (60:7), Emerald Group Publishing Limited, pp. 709–720 (doi: 10.1108/17410401111167799).

Komiak, S. Y. X., and Benbasat, I. 2006. "he effects of personalization and familiarity on trust and adoption of recommendation agents," *MIS Quarterly*, (30:4), pp. 941–960 (available at http://eds.a.ebscohost.com/abstract?site=eds&scope=site&jrnl=02767783&AN=23112324&h=KZhg1GWxjjlFV77bCuBVKtJZvTBsACKdVKcXKUtROB1Yfl3GFk63bd74WEe3WK%2BBhWLDFTwqQp6xZks19VWLOQ%3D%3D&crl=f&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3Fdir).

Kortmann, S., Gelhard, C., Zimmermann, C., and Piller, F. T. 2014. "Linking strategic flexibility and operational efficiency: The mediating role of ambidextrous operational capabilities," *Journal of Operations Management*, (32:7–8), Elsevier, pp. 475–490 (doi: 10.1016/J.JOM.2014.09.007).

Kraatz, M. S. 1998. "Learning by association? Interorganizational networks and adaptation to environmental change.," *Academy of Management Journal*, (41:6), pp. 621–643 (doi: 10.5465/256961).

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly*, (38:2), pp. 451–471 (available at http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3176&context=misq).

Lane, P. J., Koka, B. R., and Pathak, S. 2006. "The Reification of Absorptive Capacity: A Critical Review and Rejuvenation of the Construct," *Academy of Management Review*, (31:4), pp. 833–863 (doi: 10.5465/AMR.2006.22527456).

Laux, D. 2007. "A study of biometric authentication adoption in the credit union industry," *Retrospective Theses and Dissertations*, Iowa State University (available at http://lib.dr.iastate.edu/rtd/14535).

Laux, D., Luse, A., Mennecke, B., and Townsend, A. M. 2011. "Adoption of Biometric Authentication Systems: Implications for Research and Practice in the Deployment of End-User Security Systems," *Journal of Organizational Computing and Electronic Commerce*, (21:3), Taylor & Francis Group , pp. 221–245 (doi: 10.1080/10919392.2011.590111).

Lease, D. R. 2005. "Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information Technology and Security Managers," Capella University.

Lei, D., Hitt, M. A., and Goldhar, J. D. 1996. "Advanced Manufacturing Technology:

Organizational Design and Strategic Flexibility," *Organization Studies*, (17:3), Sage PublicationsSage CA: Thousand Oaks, CA, pp. 501–523 (doi: 10.1177/017084069601700307).

Lenz, R. T. 1980. "Environment, strategy, organization structure and performance: Patterns in one industry," *Strategic Management Journal*, (1:3), John Wiley & Sons, Ltd., pp. 209–226 (doi: 10.1002/smj.4250010303).

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly*, (33:1), Management Information Systems Research Center, University of Minnesota, pp. 71–90 (doi: 10.2307/20650279).

Liao, I.-E., Lee, C.-C., and Hwang, M.-S. 2006. "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, (72:4), pp. 727–740 (doi: 10.1016/j.jcss.2005.10.001).

Lichtenthaler, U. 2009. "Absorptive Capacity, Environmental Turbulence, and the Complementarity of Organizational Learning Processes," *Academy of Management Journal*, (52:4), pp. 822–846 (doi: 10.5465/AMJ.2009.43670902).

Liker, J. K., and Franz, J. K. 2011. *The Toyota way to continuous improvement: Linking strategy and operational excellence to achieve superior performance.*, McGraw Hill Professional.

Lillrank, P., Shani, A. B. (Rami), and Lindberg, P. 2001. "Continuous improvement: Exploring alternative organizational designs," *Total Quality Management*, (12:1), Taylor & Francis Group , pp. 41–55 (doi: 10.1080/09544120020010084).

Lin, H.-F. 2006. "Interorganizational and organizational determinants of planning effectiveness for Internet-based interorganizational systems," *Information & Management*, (43:4), pp. 423–433 (doi: 10.1016/j.im.2005.10.004).

Linderman, K., Schroeder, R. G., Zaheer, S., Liedtke, C., and Choo, A. S. 2004. "Integrating quality management practices with knowledge creation processes," *Journal of Operations Management*, (22:6), Elsevier, pp. 589–607 (doi: 10.1016/J.JOM.2004.07.001).

Liu, H., Ke, W., Wei, K. K., and Hua, Z. 2013. "The impact of IT capabilities on firm performance: The mediating roles of absorptive capacity and supply chain agility," *Decision Support Systems*, (54:3), North-Holland, pp. 1452–1462 (doi: 10.1016/J.DSS.2012.12.016).

Loewenstein, G. F., Weber, E. U., Hsee, C. K., and Welch, N. 2001. "Risk as feelings.," *Psychological Bulletin*, (127:2), American Psychological Association, pp. 267–286 (doi: 10.1037/0033-2909.127.2.267).

Lu, J., Yao, J. E., and Yu, C.-S. 2005. "Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology," *The Journal of Strategic Information Systems*, (14:3), pp. 245–268 (doi: 10.1016/j.jsis.2005.07.003).

Lumpkin, G. T., and Lichtenstein, B. B. 2005. "The Role of Organizational Learning in the Opportunity-Recognition Process," *Entrepreneurship Theory and Practice*, (29:4), Wiley/Blackwell (10.1111), pp. 451–472 (doi: 10.1111/j.1540-6520.2005.00093.x).

Malhotra, A., Gosain, S., and Sawy, O. A. El. 2005. "Absorptive Capacity Configurations in Supply Chains: Gearing for Partner-Enabled Market Knowledge Creation," *MIS Quarterly*, (29:1), Management Information Systems Research Center, University of Minnesota, p. 145

(doi: 10.2307/25148671).

Manadhata, P. K. 2008. “An Attack Surface Metric,” Carnegie Mellon University (available at http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/2008/CMU-CS-08-152.pdf).

Manadhata, P. K., and Wing, J. M. 2011. “An Attack Surface Metric,” *IEEE Transactions on Software Engineering*, (37:3), pp. 371–386 (doi: 10.1109/TSE.2010.60).

Marcellus, R. L., and Dada, M. 1991. “Interactive Process Quality Improvement,” *Management Science*, (37:11), INFORMS , pp. 1365–1376 (doi: 10.1287/mnsc.37.11.1365).

Mare, S., and Gummeson, J. 2016. “A Study of Authentication in Daily Life,” in *In Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pp. 189–206 (available at https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare).

Maxwell, J. W. 1996. “What to do when win-win won’t work: Environmental strategies for costly regulation,” *Business Horizons*, (39:5), pp. 60–63 (doi: 10.1016/S0007-6813(96)90068-3).

Mburu, P. G. 2015. “Competitive strategies adopted by Wells Fargo (K) Limited to enhance competitive advantage,” University of Nairobi (available at http://erepository.uonbi.ac.ke/bitstream/handle/11295/94432/Mburu Paul Gathitu_Competitive strategies adopted by wells Fargo %28K%29 Limited to enhance competitive advantage.pdf?sequence=1&isAllowed=y).

McFarlan, W. F. 1984. “Information technology changes the way you compete,” *Harvard Business Review*, pp. 98–109 (available at https://s3.amazonaws.com/academia.edu.documents/3456272/Technology_Changes.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1490150198&Signature=%2FGMEYUthiBPmKIK%2FP2EiyUvMZIs%3D&response-content-disposition=inline%3Bfilename%3DInformation_technology_c).

Meyer, A. D., and Goes, J. B. 1988. “Organizational Assimilation of Innovations: A Multilevel Contextual Analysis,” *Academy of Management Journal*, (31:4), Academy of Management, pp. 897–923 (doi: 10.2307/256344).

Miller, B. 1994. “Vital signs of identity [biometrics],” *IEEE Spectrum*, (31:2), pp. 22–30 (doi: 10.1109/6.259484).

Milliken, F. J. 1987. “Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty.,” *Academy of Management Review*, (12:1), Academy of Management, pp. 133–143 (doi: 10.5465/AMR.1987.4306502).

Mittal, N., and Nault, B. R. 2009. “Research Note —Investments in Information Technology: Indirect Effects and Information Technology Intensity,” *Information Systems Research*, (20:1), pp. 140–154 (doi: 10.1287/isre.1080.0186).

Monrose, F., and Rubin, A. D. 2000. “Keystroke dynamics as a biometric for authentication,” *Future Generation Computer Systems*, (16:4), North-Holland, pp. 351–359 (doi: 10.1016/S0167-739X(99)00059-X).

Moore, G. C., and Benbasat, I. 1991. “Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” *Information Systems Research*, (2:3), INFORMS , pp. 192–222 (doi: 10.1287/isre.2.3.192).

Morrison, E. W., and Phelps, C. C. 1999. "Taking Charge At Work: Extrarole Efforts to Initiate Workplace Change," *Academy of Management Journal*, (42:4), Academy of Management, pp. 403–419 (doi: 10.2307/257011).

Morton, M. S. 1991. *The corporation of the 1990s: Information technology and organizational transformation*, New York: Oxford University Press.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, (46:4), North-Holland, pp. 815–825 (doi: 10.1016/J.DSS.2008.11.010).

Niedenthal, P. M., Cantor, N., and Kihlstrom, J. F. 1985. "Prototype matching: A strategy for social decision making.," *Journal of Personality and Social Psychology*, (48:3), American Psychological Association, pp. 575–584 (doi: 10.1037/0022-3514.48.3.575).

O'Gorman, L. 2003. "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, (91:12), pp. 2021–2040 (doi: 10.1109/JPROC.2003.819611).

Ostlund, L. E. 1974. "Perceived Innovation Attributes as Predictors of Innovativeness," *Journal of Consumer Research*, (1:2), Oxford University Press, p. 23 (doi: 10.1086/208587).

Oxtoby, B., McGuiness, T., and Morgan, R. 2002. "Developing Organisational Change Capability," *European Management Journal*, (20:3), Pergamon, pp. 310–320 (doi: 10.1016/S0263-2373(02)00047-6).

Padayachee, K. 2012. "Taxonomy of compliant information security behavior," *Computers & Security*, (31:5), Elsevier Advanced Technology, pp. 673–680 (doi: 10.1016/J.COSE.2012.04.004).

Panko, R. 2009. *Business data networks and telecommunications*, (7th ed.), Upper Saddle River, New Jersey, USA: Pearson Education (available at https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=Business+data+networks+and+telecommunications+).

Patel, P. C., Terjesen, S., and Li, D. 2012. "Enhancing effects of manufacturing flexibility through operational absorptive capacity and operational ambidexterity," *Journal of Operations Management*, (30:3), Elsevier, pp. 201–220 (doi: 10.1016/J.JOM.2011.10.004).

Pavlou, P. A., and El Sawy, O. A. 2006. "From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development," *Information Systems Research*, (17:3), pp. 198–227 (doi: 10.1287/isre.1060.0094).

Peng, D. X., Schroeder, R. G., and Shah, R. 2008. "Linking routines to operations capabilities: A new perspective," *Journal of Operations Management*, (26:6), Elsevier, pp. 730–748 (doi: 10.1016/J.JOM.2007.11.001).

Pfeffer, J. 1982. *Organizations and organization theory*, Boston, MA: Pitman.

Pfeffer, J., and Leblebici, H. 1973. "The Effect of Competition on Some Dimensions of Organizational Structure," *Social Forces*, (52:2), pp. 268–279 (doi: 10.2307/2576381).

Phillips, P. A. 1999. "Hotel performance and competitive advantage: a contingency approach," *International Journal of Contemporary Hospitality Management*, (11:7), MCB UP Ltd, pp. 359–365 (doi: 10.1108/09596119910293268).

Pironti, J. P. 2005. “Key elements of an information security program,” *Information Systems Control Journal*, (1).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. “Common method biases in behavioral research: A critical review of the literature and recommended remedies.,” *Journal of Applied Psychology*, (88:5), American Psychological Association, pp. 879–903 (doi: 10.1037/0021-9010.88.5.879).

Podsakoff, P. M., and Organ, D. W. 1986. “Self-Reports in Organizational Research: Problems and Prospects,” *Journal of Management*, (12:4), Sage PublicationsSage CA: Thousand Oaks, CA, pp. 531–544 (doi: 10.1177/014920638601200408).

Pooe, A., and Labuschagne, L. 2011. “Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation,” *Southern African Business Review*, (15:1), College of Economic and Management Sciences (UNISA).

Porter, M. E. 2011. *Competitive Advantage of Nations: Creating and Sustaining Superior Performance*, New York: Simon and Schuster (available at https://books.google.com/books?hl=en&lr=&id=CqZzxAxBpfEC&oi=fnd&pg=PT10&dq=Porter,+M.+E.+(1998).+Competitive+Advantage:+Creating+and+sustaining+superior+performance.+New+York:+U.S.A&ots=As4lIN24Vu&sig=EAtiCq7B3BSJJ-eTXBwPbVG4VIM#v=onepage&q=Porter%2C M.).

Porter, M. E., and Linde, C. van der. 1995. “Toward a New Conception of the Environment-Competitiveness Relationship,” *The Journal of Economic Perspectives*, (9:4), American Economic Association, pp. 97–118 (doi: 10.2307/2138392).

Porter, M. E., and Millar, V. E. 1985. “How information gives you competitive advantage,” *Harvard Bus. Rev.*, (63:4), p. 149–160.

Preece, J. 2001. “Sociability and usability in online communities: Determining and measuring success,” *Behaviour & Information Technology*, (20:5), Taylor & Francis Group , pp. 347–356 (doi: 10.1080/01449290110084683).

Pullin, J. 2005. “Room for improvement. Professional Engineering,” *Professional Engineering*, (18:15), p. 35.

Ransbotham, S., and Mitra, S. 2009. “Choice and Chance: A Conceptual Model of Paths to Information Security Compromise,” *Information Systems Research*, (20:1), pp. 121–139 (doi: 10.1287/isre.1080.0174).

Reid, P. 2004. *Biometrics for Network Security*, Prentice Hall Professional (available at https://books.google.com/books?hl=en&lr=&id=NfPYJbxVvs0C&oi=fnd&pg=PR15&dq=Biometrics+for+network+security&ots=Eye35P1Akz&sig=qEUQssbel9jSIx2X13mmqCMFHZs#v=onepage&q=Biometrics for network security&f=false).

Reyna, V. F., and Brainerd, C. J. 1992. “A fuzzy-trace theory of reasoning and remembering: Paradoxes, patterns, and parallelism,” in *From learning processes to cognitive processes: Essays in honor of William K. Estes*, Psychology Press, pp. 235–259 (available at https://books.google.com/books?hl=en&lr=&id=NaXm2AKl2w8C&oi=fnd&pg=PA235&dq=Afuzzy-trace+theory+of+reasoning+and+remembering:+Paradoxes,+patterns,+and+parallelism&ots=fyQXNEHmtx&sig=Zs5k5Mm1MD_vujweeWLnC5_b_3I#v=onepage&q=Afuzzy-trace

theory of reas).

Reynolds, P. 2016. "The Death Of The Password," *AimBrain* (available at https://aimbrain.com/blog/the-death-of-the-password; retrieved January 25, 2017).

Ringle, C., Wende, S., and Becker, J. 2015. *SmartPLS 3*, Boenningstedt: SmartPLS GmbH (available at http://www.smartpls.com).

Rivis, A., Sheeran, P., and Armitage, C. J. 2006. "Augmenting the theory of planned behaviour with the prototype/willingness model: Predictive validity of actor versus abstainer prototypes for adolescents' health-protective and health-risk intentions," *British Journal of Health Psychology*, (11:3), Blackwell Publishing Ltd, pp. 483–500 (doi: 10.1348/135910705X70327).

Roberts, N., Galluch, P. S., Dinger, M., and Grover, V. 2012. "Absorptive Capacity and Information Systems Research: Review, Synthesis, and Directions for Future Research," *MIS Quarterly*, Management Information Systems Research Center, University of Minnesota, pp. 625–648 (doi: 10.2307/41703470).

Rogers, E. M. 1995. *Diffusion of Innovations*, New York: Free Press.

Rondinelli, D. A., and Vastag, G. 1996. "International Environmental Standards and Corporate Policies: An Integrative Framework," *California Management Review*, (39:1) (available at http://cmr.ucpress.edu/content/39/1/106).

Rowe, B. R., and Gallaher, M. P. 2006. "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," in *Fifth workshop on the economics of information security (WEIS06)*, Cambridge, UK (available at https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf).

Ryan, E. 2016. "Enable more secure business growth with multi-factor authentication," (available at https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/multi-factor-authentication-solution-brief.pdf).

Santos-Vijande, M. L., López-Sánchez, J. Á., and Trespalacios, J. A. 2012. "How organizational learning affects a firm's flexibility, competitive strategy, and performance," *Journal of Business Research*, (65:8), Elsevier, pp. 1079–1089 (doi: 10.1016/J.JBUSRES.2011.09.002).

Sarstedt, M., Henseler, J., and Ringle, C. M. 2011. "Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," in *Measurement and research methods in international marketing*, Emerald Group Publishing Limited, pp. 195–218 (doi: 10.1108/S1474-7979(2011)0000022012).

Schreyögg, G., and Kliesch-Eberl, M. 2007. "How dynamic can organizational capabilities be? Towards a dual-process model of capability dynamization," *Strategic Management Journal*, (28:9), Wiley-Blackwell, pp. 913–933 (doi: 10.1002/smj.613).

Scott, M., Acton, T., and Hughes, M. 2005. "An assessment of biometric identities as a standard for e-government services," *International Journal of Services and Standards*, (1:3), pp. 271–286 (doi: 10.1504/IJSS.2005.005800).

Setia, P., and Patel, P. C. 2013. "How information systems help create OM capabilities: Consequents and antecedents of operational absorptive capacity," *Journal of Operations Management*, (31:6), Elsevier, pp. 409–431 (doi: 10.1016/J.JOM.2013.07.013).

Shimizu, K., and Hitt, M. A. 2004. "Strategic flexibility: Organizational preparedness to reverse ineffective strategic decisions.," *Academy of Management Executive*, (18:4), pp. 44–59 (doi: 10.5465/AME.2004.15268683).

Simsek, Z. 2009. "Organizational Ambidexterity: Towards a Multilevel Understanding," *Journal of Management Studies*, (46:4), pp. 597–624 (doi: 10.1111/j.1467-6486.2009.00828.x).

Skowronski, J. J., and Carlston, D. E. 1989. "Negativity and extremity biases in impression formation: A review of explanations.," *Psychological Bulletin*, (105:1), American Psychological Association, pp. 131–142 (doi: 10.1037/0033-2909.105.1.131).

Sloman, S. A. 1996. "The empirical case for two systems of reasoning.," *Psychological Bulletin*, (119:1), American Psychological Association, pp. 3–22 (doi: 10.1037/0033-2909.119.1.3).

Smit, J. 2015. "Journal of international technology and information management.," *Journal of International Technology and Information Management*, (24:3), International Information Management Association (available at http://scholarworks.lib.csusb.edu/jitim/vol24/iss3/4).

Sonnentag, S. 2003. "Recovery, work engagement, and proactive behavior: A new look at the interface between nonwork and work.," *Journal of Applied Psychology*, (88:3), American Psychological Association, pp. 518–528 (doi: 10.1037/0021-9010.88.3.518).

Spiro, R. L., and Weitz, B. A. 1990. "Adaptive Selling: Conceptualization, Measurement, and Nomological Validity," *Journal of Marketing Research*, (27:1), American Marketing Association, p. 61 (doi: 10.2307/3172551).

Stanislav, M. 2015. *Two-Factor Authentication*, IT Governance Ltd. (available at https://books.google.com/books?hl=en&lr=&id=3EU3DwAAQBAJ&oi=fnd&pg=PA5&dq=two-factor+authentication+&ots=b3wzl3Q7uu&sig=O6lCcNtdpjKqLiAw9GBGxxbuOus#v=onepage&q=two-factor authentication&f=false).

Stock, M. L., Litt, D. M., Arlt, V., Peterson, L. M., and Sommerville, J. 2013. "The Prototype/Willingness model, academic versus health-risk information, and risk cognitions associated with nonmedical prescription stimulant use among college students," *British Journal of Health Psychology*, (18:3), pp. 490–507 (doi: 10.1111/j.2044-8287.2012.02087.x).

Stoneburner, G., Goguen, A., and Feringa, A. 2002. "Risk management guide for information technology systems :," Gaithersburg, MD (doi: 10.6028/NIST.SP.800-30).

Straub, D., Boudreau, M.-C., Gefen, D., Straub, D., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems*, (13:13), pp. 380–427 (available at http://aisel.aisnet.org/cais).

Straub, D. W., Goodman, S. E., and Baskerville, R. L. 2008. "Framing the information security process in modern society," in *Information Security: Policy, Processes and Practices*, Armonk, NY: M. E. Sharpe, pp. 5–12 (available at https://books.google.com/books?hl=en&lr=&id=lpEsu3_sejwC&oi=fnd&pg=PA5&dq=Framing+of+information+security+and+practices&ots=NH30wLa252&sig=hQUTTAdDmVuj8CTTS-XTrt1ApaY#v=onepage&q=Framing of information security and practices&f=false).

Sun, H., Ho, K., and Ni, W. 2008. "The empirical relationship among Organisational Learning, Continuous Improvement and Performance Improvement," *International Journal of Learning and Change*, (3:1), p. 110 (doi: 10.1504/IJLC.2008.018871).

Sung, S. Y., and Choi, J. N. 2012. "Effects of team knowledge management on the creativity and financial performance of organizational teams," *Organizational Behavior and Human Decision Processes*, (118:1), pp. 4–13 (doi: 10.1016/j.obhdp.2012.01.001).

Sutcliffe, K. M., and Zaheer, A. 1998. "Uncertainty in the Transaction Environment: An Empirical Test," *Strategic Management Journal*, (19:1), pp. 1–23 (doi: 10.1111/j.1467-6486.1993.tb00317.x).

Taylor, S., and Todd, P. A. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research*, (6:2), INFORMS , pp. 144–176 (doi: 10.1287/isre.6.2.144).

Teece, D. J. 2007. "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance," *Strategic Management Journal*, (28:13), Wiley-Blackwell, pp. 1319–1350 (doi: 10.1002/smj.640).

The Economist Intelligence Unit. 2016. "Data security: How a proactive C-suite can reduce cyber-risk for the enterprise," (available at https://www.eiuperspectives.economist.com/sites/default/files/DataSecurityArticle.pdf).

The Global Information Security Workforce Study. 2017. "IT Professionals are an Underutilized Cybersecurity Resource," (available at https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/09/13/ISC2-Finds-IT-Professionals-are-an--Underutilized-Cybersecurity-Resource).

Theofanos, M., Garfinkel, S., and Choong, Y.-Y. 2016. "Secure and Usable Enterprise Authentication: Lessons from the Field," *IEEE Security & Privacy*, (14:5), pp. 14–21 (doi: 10.1109/MSP.2016.96).

Thompson, J. D. 1967. *Organizations in action : social science bases of administrative theory*, New York: McGraw-Hill (available at https://books.google.com/books?hl=en&lr=&id=8aNwAAAAQBAJ&oi=fnd&pg=PR1&dq=Thompson,+1967&ots=s8M-aeTReN&sig=EzUIcmDYx2bNKnutt-0o38Wr108#v=onepage&q=Thompson%2C 1967&f=false).

Thong, J. Y. L. 1999a. "An Integrated Model of Information Systems Adoption in Small Businesses," *Journal of Management Information Systems*, (15:4), Routledge, pp. 187–214 (doi: 10.1080/07421222.1999.11518227).

Thong, J. Y. L. 1999b. "An Integrated Model of Information Systems Adoption in Small Businesses," *Journal of Management Information Systems*, (15:4), Routledge, pp. 187–214 (doi: 10.1080/07421222.1999.11518227).

Thong, J. Y. L. 1999c. "An Integrated Model of Information Systems Adoption in Small Businesses," *Journal of Management Information Systems*, (15:4), Routledge, pp. 187–214 (doi: 10.1080/07421222.1999.11518227).

Thong, J. Y. L., and Yap, C. S. 1995. "CEO characteristics, organizational characteristics and information technology adoption in small businesses," *Omega*, (23:4), Pergamon, pp. 429–

442 (doi: 10.1016/0305-0483(95)00017-I).

Tipton, H. F., and Krause, M. 2003. *Information Security Management Handbook*, CRC Press.

Todd, J., Kothe, E., Mullan, B., and Monds, L. 2016. "Reasoned versus reactive prediction of behaviour: a meta-analysis of the prototype willingness model," *Health Psychology Review*, (10:1), Routledge, pp. 1–24 (doi: 10.1080/17437199.2014.922895).

Todorova, G., and Durisin, B. 2007. "Absorptive capacity: Valuing a reconceptualization," *Academy of Management Review*, (32:3), pp. 774–786 (doi: 10.5465/AMR.2007.25275513).

Toothaker, L. E. 1994. "Multiple Regression: Testing and Interpreting Interactions," *Journal of the Operational Research Society*, (45:1), Palgrave Macmillan UK, pp. 119–120 (doi: 10.1057/jors.1994.16).

Tornatzky, L. G., Fleischer, M., and Chakrabarti, A. K. 1990. *The processes of technological innovation*, Lexington Books.

Tornatzky, L. G., and Klein, K. J. 1982. "Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings," *IEEE Transactions on Engineering Management*, (EM-29:1), pp. 28–45 (doi: 10.1109/TEM.1982.6447463).

Tsai, M.-T., and Huang, Y.-C. 2008. "Exploratory learning and new product performance: The moderating role of cognitive skills and environmental uncertainty," *The Journal of High Technology Management Research*, (19:2), pp. 83–93 (doi: 10.1016/j.hitech.2008.10.001).

Tsai, W. 2001. "Knowledge Transfer in Intraorganizational Networks: Effects of Network Position and Absorptive Capacity on Business Unit Innovation and Performance," *Academy of Management Journal*, (44:5), pp. 996–1004 (doi: 10.5465/amj.2015.0230).

Tu, Q., Vonderembse, M. A., Ragu-Nathan, T. S., and Sharkey, T. W. 2006. "Absorptive capacity: Enhancing the assimilation of time-based manufacturing practices," *Journal of Operations Management*, (24:5), Elsevier, pp. 692–710 (doi: 10.1016/J.JOM.2005.05.004).

Tu, Z., and Yuan, Y. 2014. "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in *Twentieth Americas Conference on Information Systems*, Savannah, p. 13 (available at https://pdfs.semanticscholar.org/aa02/0f53503050a6e53d6403c6aa48f5dcbc3b9c.pdf).

U.S. Department of Health & Human Services. 2015. "The HIPAA Privacy Rule's Right of Access and Health Information Technology," *U.S. Department of Health & Human Services (HHS)*, pp. 1–8 (available at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf; retrieved January 24, 2017).

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, (27:3), pp. 425–478 (available at https://www.jstor.org/stable/30036540?seq=1#page_scan_tab_contents).

Verizon. 2016. "2016 Data Breach Investigations Report," (available at http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf).

Volberda, H. W. 1996. "Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments," *Organization Science*, (7:4), INFORMS , pp. 359–374 (doi:

10.1287/orsc.7.4.359).

Waldman, D. A., Ramirez, G. G., House, R. J., and Puranam, P. 2001. "DOES LEADERSHIP MATTER? CEO LEADERSHIP ATTRIBUTES AND PROFITABILITY UNDER CONDITIONS OF PERCEIVED ENVIRONMENTAL UNCERTAINTY.," *Academy of Management Journal*, (44:1), Academy of Management, pp. 134–143 (doi: 10.2307/3069341).

Wang, C.-H., Chen, K.-Y., and Chen, S.-C. 2012. "Total quality management, market orientation and hotel performance: The moderating effects of external environmental factors," *International Journal of Hospitality Management*, (31:1), pp. 119–129 (doi: 10.1016/j.ijhm.2011.03.013).

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. "Continuance of protective security behavior: A longitudinal study," *Decision Support Systems*, (92), North-Holland, pp. 25–35 (doi: 10.1016/J.DSS.2016.09.013).

West, M. A., and Anderson, N. R. 1996. "Innovation in top management teams.," *Journal of Applied Psychology*, (81:6), American Psychological Association, pp. 680–693 (doi: 10.1037/0021-9010.81.6.680).

Wheeler, B. C. 2002. "NEBIC: A Dynamic Capabilities Theory for Assessing Net-Enablement," *Information Systems Research*, (13:2), pp. 125–146 (doi: 10.1287/isre.13.2.125.89).

White, G., Ekin, T., and Visinescu, L. 2017. "Analysis of Protective Behavior and Security Incidents for Home Computers," *Journal of Computer Information Systems*, (57:4), Taylor & Francis, pp. 353–363 (doi: 10.1080/08874417.2016.1232991).

Wolfe, R. A. 1994. "Organizational innovation: Review, critique and suggested research directions," *Journal of Management Studies*, (31:3), Blackwell Publishing Ltd, pp. 405–431 (doi: 10.1111/j.1467-6486.1994.tb00624.x).

Wu, C. W., and Chen, C. L. 2006. "An integrated structural model toward successful continuous improvement activity," *Technovation*, (26:5–6), Elsevier, pp. 697–707 (doi: 10.1016/J.TECHNOVATION.2005.05.002).

Yang, Y., Lee, P. K. C., and Cheng, T. C. E. 2016. "Continuous improvement competence, employee creativity, and new service development performance: A frontline employee perspective," *International Journal of Production Economics*, (171), Elsevier, pp. 275–288 (doi: 10.1016/J.IJPE.2015.08.006).

Yoon, E., and Lilien, G. L. 1985. "New industrial product performance: The effects of market characteristics and strategy," *Journal of Product Innovation Management*, (2:3), No longer published by Elsevier, pp. 134–144 (doi: 10.1016/0737-6782(85)90033-5).

Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., and Stergioulas, L. K. 2008. "An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit)," *International Journal of Medical Informatics*, (77:6), pp. 386–398 (doi: 10.1016/j.ijmedinf.2007.08.011).

Zahra, S. A., and George, G. 2002. "Absorptive Capacity: A Review, Reconceptualization, and Extension," *Academy of Management Review*, (27:2), pp. 185–203 (doi: 10.5465/AMR.2002.6587995).

Zaltman, G., Duncan, R., and Holbek, J. 1973. *Innovations and organizations*, John Wiley & Sons.

Zangwill, W. I., and Kantor, P. B. 1998. "Toward a Theory of Continuous Improvement and the Learning Curve," *Management Science*, (44:7), pp. 910–920 (doi: 10.1287/mnsc.44.7.910).

Zhou, K. Z., and Wu, F. 2009. "Technological capability, strategic flexibility, and product innovation," *Strategic Management Journal*, (31:5), Wiley-Blackwell, p. n/a-n/a (doi: 10.1002/smj.830).

Zhu, K., and Kraemer, K. L. 2005. "Post-Adoption Variations in Usage and Value of E-Business by Organizations: Cross-Country Evidence from the Retail Industry," *Information Systems Research*, (16:1), pp. 61–84 (doi: 10.1287/isre.1050.0045).

Zhu, K., Kraemer, K. L., and Xu, S. 2006a. "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business," *Management Science*, (52:10), INFORMS , pp. 1557–1576 (doi: 10.1287/mnsc.1050.0487).

Zhu, K., Kraemer, K. L., and Xu, S. 2006b. "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business," *Management Science*, (52:10), INFORMS , pp. 1557–1576 (doi: 10.1287/mnsc.1050.0487).

APPENDIX

First Scenario:

Recently, researchers proposed an authentication system that would an alternative to traditional passwords. A partial screenshot of the scheme is shown below. The system shows the user five panels of 16 pictures each, where each picture is labeled with a keyword (e.g. "mango"), a fact about the pictured item ("Mangos are the most popular fruit in the world."), and a randomly selected letter from 'a' to 'z' (e.g. 'w'). The user is randomly assigned one of the 16 pictures on each panel and logs in by typing the letter associated with the assigned picture ('w' in our example). This system has been shown to have the following features:

- Random, system-assigned passwords, so there are no weak user-selected passwords
- 20 bits of guessing space (about one million guesses possible)
- 98% of users remember their passwords one week after registration
- 39 seconds to login (median)
- 2 minutes, 43 seconds to register (median)
- Users showed high levels of satisfaction in surveys.
- A basic deployment of the system would be free of any licensing charges.
- The code is open source.
- No special hardware is required, just a typical authentication server.
- A deployment with new images and descriptions (to limit password reuse and confusion) would cost $1,000.

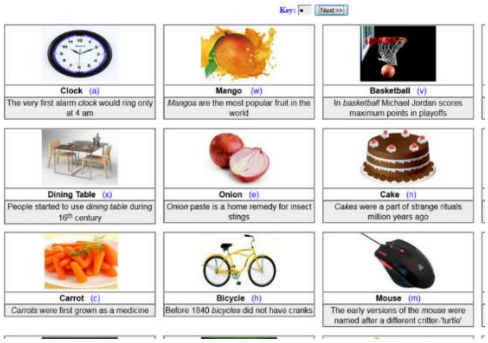

Figure A1. A Partial Screenshot of the First Scenario

Second Scenario:

Recently, an organization has proposed a new authentication scheme based on using a smartphone app and the user's fingerprint as read by the smartphone fingerprint sensor. The smartphone app works like a token, validating that this is the user's device, while the fingerprint helps to show that the user herself is making the current request. To login using a laptop, the user should connect the smartphone to the laptop via Bluetooth and run a small software program on the laptop. The Bluetooth communication is all encrypted. This system has been shown to have the following features:

- No passwords, so no passwords are forgotten, written down, or guessed.
- The false acceptance rate (allowing attackers to login) on the fingerprint scan is set to 1 in 10,000.
- The false rejection rate (preventing the user from logging in) is 2.5%.

- Most users can login on successfully in one more attempt.
- The risk of an attacker being able to use a copied fingerprint is considered low.
- 8 seconds to log in (median).
- 53 seconds to set up the app and register (median).
- Users showed high levels of satisfaction in surveys.
- A deployment would cost an organization of 10K users $50,000.
- The app and software is closed source.