Title: Determinants of Early Conformance with information security policies

Authors: France Bélanger, Stephane Collignon, Kathy Enget, Eric Negangard

PII: S0378-7206(17)30011-3
DOI: http://dx.doi.org/doi:10.1016/j.im.2017.01.003
Reference: INFMAN 2971

To appear in: *INFMAN*

Received date: 6-2-2016
Revised date: 14-12-2016
Accepted date: 7-1-2017

DETERMINANTS OF EARLY CONFORMANCE WITH INFORMATION SECURITY POLICIES

Dr. France Bélanger **(corresponding author)** R. B. Pamplin Professor Tom & Daisy Byrd Senior Faculty FellowPamplin College of Business, Virginia Tech880 W. Campus Drive, Blacksburg, VA, 24061-0101**belanger@vt.edu**

Stephane Collignon
Teaching Assistant Professor
West Virginia University
Stephane.collignon@mail.wvu.edu

Dr. Kathy Enget
Assistant Professor
Department of Accounting and Law
Massry Center for Business
University at Albany – SUNY
1400 Washington Avenue
Albany, NY 12222
kenget@albany.edu

Dr. Eric Negangard
Assistant Professor of Commerce
McIntire School of Commerce
Rouss & Robertson Halls, East Lawn
University of Virginia
P.O. Box 400173, Charlottesville, VA 22904-4173
ericnegs@virginia.edu

Highlights

- A positive attitude toward a mandatory security change leads to greater intention to comply.
- Intention to comply is related to actual compliance behavior.
- For early conformers, influence of others does not affect their intentions to comply.
- Branding can raise awareness of a security change and intention to comply with the change.

ABSTRACT

Individuals often fail to perform the security behaviors their organizations request to protect informational assets. However, forcing individuals into the compliance can trigger undesired behaviors. We propose a model grounded in Theory of Planned Behavior and information security literature to study determinants of early conformance toward technology-enforced security policies. The model was tested with 535 respondents from a university that implemented new password policies. The results show support for all the proposed relationships, except that subjective norm does not affect intentions. This important finding is explained by the leading role of early conformers, which highlights the importance of context-specific theorizing by researchers.

Keywords: information security; early conformance behavior; perceived security threat; passwords; mandatory security policies; information security awareness

INTRODUCTION

At present, one of the most valuable assets of an organization is its information. In fact, organizations place a major focus on maintaining the security and accuracy of their information systems (IS) because cyber-related security threats continue to increase in both number and magnitude (Berger 2011-2012). Access controls constitute a particularly important area of concern for organizations (Cluley 2013) as “insecure remote access software/policies and weak passwords tied as the vulnerability most exploited by criminals in 2014” (Trustwave 2015). Although security controls specific to the prevention of unauthorized access are continually evolving, individuals asked to accept and implement new policy changes are not always compliant. In fact, many individuals procrastinate or resist such changes, and as a result of their late conformance or nonconformance, they are often seen as the weakest link in security (Anderson and Agarwal 2010; Guo et al. 2011).

According to Willison and Warkentin (2013), most information security (InfoSec) research focuses on noncompliant behaviors. Nonconformant users (i.e., those who procrastinate or, in the most severe cases, intentionally resist the change) pose serious threats to their organizations. In contrast, individuals who choose to conform with new policies early present several benefits for organizations. For example, early conformers are less costly to support than late or nonconformers who create last minute rushes to security changes that may crash the system, overload the help desk, or cause hotline traffic jams. In fact, much can be learned by focusing on individuals who are not only compliant with but also conform to policy requirements early in the process. By studying what motivates these individuals to conform early, new insights can be obtained that are currently missing from our understanding of individuals’ perceptions and behaviors related to security policies.

To avoid both voluntary and involuntary nonconformant behavior, some institutions use technological means to enforce some or part of their information security policies. Unfortunately for these institutions, reactions to mandatory and technology-enforced security policy changes are varied. They range from immediate acceptance and compliance from early conformers to costly resistance and complete nonconformance (Brown et al. 2002). In certain cases, mandating enforcement of coercive security policy changes (e.g., forced password changes, required password strength, and automatic security updates) may act as a precipitating event or catalyst for negative attitudes and undesired behaviors (Nurse et al. 2014). This can be detrimental and costly to an organization if all users procrastinate and delay their compliance until or after the deadline. For example, if the entire population of users waits until the last minute, the organizations needs to increase information technology (IT) support personnel to handle the increased volume of calls. Failure to handle all cases may prevent users from the timely performance of some operational tasks, even leading to the incapacity of users to perform all work tasks. This could trigger a chain reaction of subsequent curative administrative tasks at high organizational costs. Conversely, early conformance by users to newly implemented security policies can better protect organizations and reduce unnecessary costs. The faster the users adopt the mandated and eventually technology-enforced policy change, the more likely issues related to its implementation are identified and dispersed over time. This allows the IT team to handle the change without any temporary surge in resources and with less impact on the organization's overall operations.

In this research, we specifically focus on how to encourage early conformance through users who proactively accept and enact a required and eventually technologically enforced password security enhancement. In doing so, we differentiate between users who are early conformers, those who conform near the deadline (i.e., late conformers), and those who refuse to conform (i.e., nonconformers). Furthermore, we discuss how early conformance behaviors are more cost-efficient for organizations and can ultimately help prevent intentional undesired security behaviors. Therefore, we chose to study the implementation of a change in password policy because the absence or breakdown of identification and authentication processes is one of the main causes of losses related to cyber-fraud and lost productivity from cyber-attacks (Chandra and Calderon 2003; Herley and Oorschot 2012; Trustwave 2015). Despite continual reminders of the importance of using strong passwords (Mattord et al. 2014; Trustwave 2015) and keeping passwords private (Bonneau et al. 2015; Summers and Bosworth 2004), not all users follow such policies (Furnell 2011; Furnell 2014). However, passwords remain the primary and preferred method for authentication (Bonneau et al. 2015; Herley and Oorschot 2012; Rubens 2014).

To date, most information security (InfoSec) studies focused on behavioral intention as opposed to testing actual behavior (Crossler et al. 2013). This is often justified with technology adoption studies, which suggest intention eventually leads to behavior. However, in the context of information security, measuring intention alone can be troublesome because, in reality, intentions do not always lead to actual behaviors (Anderson and Agarwal 2010; Crossler et al. 2013; Mahmood et al. 2010; Straub 2009). In fact, research indicates many individuals who intend to act in "safe ways" fail to act on this intention (Shropshire et al. 2015). Therefore, we explored both intention to conform early with new security requirements and actual early conformance behavior by answering the following research question: *What are the determinants of early conformance behavior in the context of a new technology-enforced security policy?*

Drawing from the theory of planned behavior (TPB) and the InfoSec literature, we propose a model of early conformance behavior toward a new mandated and technology-enforced security policy. The model was tested with data from 535 respondents (administrators, faculty, and students) from a large university where, after recurring security issues and an appraisal of university members' password practices, the Chief IT Security Officer established a new password requirement. The new security policy included the need for a strengthened password and an annual password change. Consistent with TPB, results show that intention to conform early does predict early conformance behavior, whereas attitude predicts intention. However, an important finding is that subjective norm does not influence intention. This result is explained by the idea that early conformers are the leaders in change and are therefore not influenced by their peers. Results also confirm the effects of perceived security threat severity and vulnerability on attitude and highlight the fact that awareness of the security policy change impacts early conformance behavior. Finally, results show organizational triggers are important in raising awareness of the security policy change.

This research provides several contributions to the field. The study is one of few that measures early conformance behavior during an actual policy change implemented in an organization. Most studies only capture general intention regarding password requirements or other security-related behaviors. Therefore, this study avoids drawing conclusions regarding untested influences between intention and behavior, thereby extending prior findings from InfoSec research. By focusing on a nonvolitional setting, the research also provides a better understanding of attitudes surrounding technology-enforced security controls and the potential consequences of these attitudes as they relate to early, late, and nonconformance. Importantly, the research proposes and finds that TPB's suggested impact of subjective norm on intention does not apply for early conformers. Early conformers represent the leading users who enact a security policy change, and therefore, they are not influenced by those around them who are yet to enact these changes. Therefore, it is important for organizations to harness the influence that early conformers can have on their peers such that they can encourage others to conform early. This finding also highlights the importance of context-specific theorizing by researchers. The present study also highlights the importance of awareness in influencing early conformance to policy changes and provides insight for managers who want to best inform users about newly proposed, and eventually technology-enforced, changes in security policies. We also highlight the costs and benefits associated with early, late, and nonconformance. By focusing on early conformance and the avoidance of late and nonconformance, we provide valuable insight into the determinants of successful implementation of organizational security policies.

The remainder of this paper is organized as follows. We first discuss the contextual domain of the study, its theoretical foundation, and our research model. We then describe the methodology and analyses. Finally, we discuss the results, contributions, and implications before we present potential limitations.

THEORETICAL BACKGROUND AND RESEARCH MODEL

From an organizational perspective, information security involves specific controls designed to protect both physical and informational assets from loss, destruction, disclosure, copying, sale, or other misuse (Gelinas et al. 2015). To encourage the proper use of organizational security systems, organizations create and implement information security policies (Lee et al. 2004; Straub 1990). Policies are, in essence, mandatory but can be implemented in more or less coercive ways. Studies show that the level of perceived voluntariness can influence behaviors (Chen et al. 2012; Moore and Benbasat 1991; Siponen and Iivari 2006). The present study's context is a policy change where, after enough time passes, users have no choice but to fully conform or be locked out. This new security policy change forces users to alter their authentication passwords every year while also respecting a new set of enhanced rules for new password generation. Failure to do so results in an inability to use the system.

Passwords remain one of the most commonly used security controls and are a primary method of user authentication (e.g., Barra et al. 2010; Furnell 2014; Mattord et al. 2014; Warkentin et al. 2004). Although many techniques have been explored to enhance the use of passwords (e.g., Gyorffy et al. 2011; e.g., Jobusch and Oldehoeft 1989), creating a strong password and frequent password changes remain key techniques for enhanced security (e.g., Barra et al. 2010; Furnell 2011; Mattord et al. 2014). However, research shows that if such security policies are not enforced, most users fail to perform them, particularly when it comes to strong password requirements (e.g., Barra et al. 2010; Furnell 2011; 2014). In fact, a study of 2500 small business owners in the USA in 2014 revealed that 74.2% keep written logs of passwords and 63% reuse the same password for many systems (Infosecurity_Magazine 2016). However, when security policies are technologically enforced (e.g., through a combination of a password check software and lock-out policy), their effectiveness often increases (Kankanhalli et al. 2003). Unfortunately, restrictive password policies can negatively impact employee productivity (e.g., time lost because of system lock-outs due to invalid login attempts, time spent resetting forgotten passwords) and frustrate users if they perceive these policies to be too demanding (Inglesant and Sasse 2010). Further, research shows that increasing the level of difficulty in a password requirement can lead people to write down their passwords, choose weaker passwords, and/or not fully follow the appropriate policy (Carstens et al. 2004). As such, it is crucial to understand how users react to mandatory password policies and what can be done to encourage early conformance.

Contrary to most InfoSec research where intention to perform a given behavior (e.g., use malware detection software, comply with security policy) is explored (c.f., Crossler et al. 2013), we focus on the actual early conformance behavior regarding the new policy. Although our subjects could not avoid the new password requirements, they had three options. First, they could choose to be early conformers by proactively changing their password. Second, they could choose to be late conformers by waiting until the implementation deadline. Finally, they could wait to change their password after being locked out of the system, which means they would have to ask the IT support staff for help.

Characteristics of Early Conformers, Late Conformers, and Nonconformers

Organizations should not expect all individuals to comply with a new security policy at the same time. In discussing the diffusion of innovation, Rogers (1995) established what has since become a widely accepted method for categorizing individuals depending upon the speed at which they adopt innovations. Using standard deviations from a normal distribution, Rogers classified individuals into five categories (1) innovators, (2) early adopters, (3) early majority, (4) late majority, and (5) laggards. However, Rogers also noted that not all situations or contexts will follow a normal distribution. In fact, the present research shows that conformance to mandatory security policies is skewed toward late and nonconformant users, as will become evident in the "Results" section of this paper. Given user tendency toward late and nonconformance, we combine several of Rogers's categories to make them more context appropriate. In particular, we combine Rogers's "innovators" and "early adopters" into a single category, early conformers; we combine "early majority" and "late majority" into a single category, late conformers; and we refer to laggards as nonconformers.

In differentiating between early and late conformers, we classify early conformers as individuals who enact the change without major consideration of an imposing deadline. Accordingly, we define early conformers as users who are part of the initial wave of conformance, as evidenced by their proactive conformance to the new policy requirements well in advance of a stated deadline. This proactive behavior demonstrates that early conformers are less influenced by the timing of the deadline and more influenced by their desire to conform. Both "innovators" and "early adopters" are part of an initial wave of adopters; however, this initial wave is followed by a discontinuity or lull in change behavior (Rogers 1995). Accordingly, we define late conformers as those who are not part of the initial wave but rather only enact the change when faced with a looming deadline. As is evident in our results, the most common response is in fact to wait to conform at or near the deadline. As the third and final category, nonconformers are defined as those who, because of their procrastination and/or resistance to the new security policy, fail to conform by the deadline and, at least in technology-enforced settings, end up getting locked out. Nonconformant users are often easy to identify as they are the ones who simply have not enacted the change by the implementation deadline.

Table 1 summarizes our definitions and highlights some of the key costs and benefits of early, late, and nonconformance behaviors. Clearly, nonconformers can create major problems for organizations. Conversely, considerable advantages can be gained through the encouragement of early conformance. Although early conformers allow for early problem identification and encourage individual ownership of the change, nonconformers will ultimately experience loss of productivity because they are locked out of the system and require help from the IT support staff (also affecting the productivity of this staff). This will also lead to overwhelmed support staff, resentment toward the change, and other undesired behaviors such as users writing down their passwords. The only benefit of user noncompliance is that it can be used to identify dormant or expired accounts, which can pose additional security risks for an organization. An ideal situation would be for all users except those who no longer need access to the system (i.e., dormant or expired accounts) to act in a manner consistent with early conformance. In fact, the sooner an organization can get users to conform, the earlier the organization can identify dormant and expired accounts.

Research Model

TPB is one of the most widely accepted behavioral theories, which is frequently used to study the effects of beliefs on the constitution of attitude toward a behavior and the influence of that attitude on behavioral intention (Ajzen 1991; Ajzen 2012; Ajzen and Fishbein 1980). TPB postulates that three constructs, attitude, subjective norm, and perceived behavioral control, together lead to an intention to perform a behavior, which leads to an actual behavior. TPB proposes that each of the three constructs is in fact a conceptually independent determinant of intention. Most InfoSec literature studies focus on intentions instead of behaviors. However, this research focuses on an actual early conformance behavior instead of just intention to perform the behavior. Therefore, TPB serves as a solid foundation for the study, given it proposes a link between intention and behavior. However, given the context of the study, we also need to include relevant constructs from the InfoSec literature. Therefore, building on TPB and the InfoSec literature, we propose the model of early conformance behavior that is presented in Figure 1. The constructs and their relationships are further described in the remainder of this section.

Early Conformance Behavior

Although an abundance of studies measure intention to conform or violate norms, laws, and policies or to adopt security tools (e.g., Guo et al. 2011; Herath et al. 2014), few studies capture the actual behaviors of users because of the level of difficulty in its measurement (Shropshire et al. 2015). We define early conformance behavior as not waiting until the last minute to enact the required security change. Consistent with the discussion of TPB presented above, we expect that individuals who intend to conform early to the requested change of password are actual early conformers with the required change of password.

H1: Intention to conform early to the security policy change is positively associated with early conformance behavior.

Determinants of Intention to Conform Early

TPB proposes that behavioral intention is impacted by one's attitude, subjective norm, and perceived behavioral control. Attitude toward a particular behavior refers to the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question. For example, in the InfoSec literature, attitude toward a security policy has been defined as "the degree of favor or disfavor expressed by end users about organizational IS security policies" (Guo et al. 2011, p. 211). As theorized by Ajzen and Fishbein (1980), attitude, intention, and behavior are positively related. Furthermore, several studies related to InfoSec have highlighted the key role that attitude plays in predicting security behavioral intention (e.g., Anderson and Agarwal 2010; Bulgurcu et al. 2010; Herath et al. 2014). These studies, however, show mixed results with regard to the relationship between attitude toward security-related policies and behavioral intention. For example, Anderson and Agarwal (2010) show that attitude toward security behavior impacts a person's intention to perform security-related behaviors both online and on their personal computer. Bulgurcu et al. (2010) find that an individual’s attitude toward a company’s security policy is positively associated with the person’s intention to conform with the policy. Conversely, Herath and Rao (2009) find that attitude does not affect intention to conform with security policies in organizations where organizational commitment and monitoring of compliance are high. A key component of each of these studies is their focus on volitional compliance. In the context of mandatory and technology-enforced changes to a security policy (i.e., nonvolitional), it is not about whether individuals will conform but rather when they will conform. In this study, we expect that individuals with positive attitudes are more likely to be early conformers with the mandatory security policy change.

H2: Attitude toward the new mandatory security policy change is positively related to intention to conform early to the new security policy change.

Subjective norm is based on the individuals’ perceptions of what important others would like them to do. Subjective norm is also referred to in prior research as social influence or social norm (although these are conceptually distinct) and refers to the perceived social pressure to perform or not perform a behavior (Fishbein and Ajzen 1975). In the context of this study, an individual’s willingness to enact the mandatory enhancement to security controls may be influenced by her perception of how her social network or referent others view this change. Although it is a core element of TPB (and the theory of reasoned action), the relationship between subjective norm and behavioral intention receives inconsistent support in prior research. This is likely due to the variety of settings studied, i.e., mandatory vs. volitional.

In a review and test of various technology adoption models, Venkatesh et al. (2003) implemented subjective norm as a social influence and found that its relationship to behavioral intention was not significant in voluntary situations.

In the context of our study, early conformers were not forced to change their password but were allowed to do so willingly ahead of others and thus seemed to not worry about what others would like them to do. In essence, they were the leading users who enacted the change. Studies on health, consumption, and innovation behaviors show that early conformers, or in the case of consumption, early purchasers, are generally seen as those who lead popular opinion (Rogers 1995), reduce the stigma of behaving out of the norm (Li et al. 2009), and are characterized by independent judgment making (Manning et al. 1995). Recent studies show that individuals who perform a particular behavior early are generally driven by personal norms (a sense of responsibility/obligation) rather than subjective norms (Jansson 2011; Jansson et al. 2011; Seebauer 2015). For example, in the context of the acceptance and use of electric scooters, Seebauer (2015) demonstrated that injunctive social norms (i.e., what people who matter to the individual think) are mediated by personal norms and have no direct effect on the usage behavior. In the travel industry, researchers using TPB find that social norm has no effect on early consumer behavior and argue that individuals acting earlier than others do not listen to others' opinion (Lam and Hsu 2004). Consistent with these studies, we extend TPB by suggesting that in the context of early conformance behavior, subjective norm will not influence behavioral intentions. In other words, we predict that early conformers' intention to conform early will not be impacted by their perceptions of what others would like them to do.

H3: Subjective norm is not related to intention to conform early to the new security policy change.

TPB's final component is a perceived behavioral control. In TPB, perceived behavioral control refers to the perceived ease or difficulty of performing the behavior and is assumed to reflect experience and anticipated impediments and obstacles. In the InfoSec literature, a user's perception of their capacity to perform a specific action is known as self-efficacy, which impacts the response behavior. Because our study is embedded in an InfoSec environment, we include security self-efficacy as a proxy for TPB's perceived behavioral control.

The InfoSec literature shows a significant impact of self-efficacy on a wide variety of dependent variables such as intention to adopt, intention to conform, or specific behaviors (e.g., Anderson and Agarwal 2010; D'Arcy et al. 2009; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee 2011; Liang and Xue 2010; Workman et al. 2008). For example, in several studies, self-efficacy impacts reported behaviors (Milne et al. 2009; Workman et al. 2008), observed behaviors (Woon et al. 2005), or intentions to perform behaviors (Ifinedo 2012). The last one is the most frequently studied dependent variable as impacted by self-efficacy (e.g., Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009). In most cases, increased self-efficacy is directly related to more favorable security intentions or behaviors. Therefore, in this study, security self-efficacy should positively affect intention to conform early to the new mandatory security policy change.

H4: Security self-efficacy is positively related to intention to conform early to the security policy change.

Determinants of Attitude

Prior InfoSec research suggests some of the key determinants of attitude that can help us better understand individuals' security behaviors. A theory often used by InfoSec researchers is the protection motivation theory (PMT). We integrate two of this theory's key constructs that best capture the determinants of attitude: perceived threat severity and perceived threat vulnerability. (e.g., Herath and Rao 2009; Ifinedo 2012).

Several studies have combined some of the components of TPB, PMT, and the theory of reasoned action when studying information security. For example, Herath and Rao (2009) integrate TPB and PMT to explain the formation of a security policy attitude and compliance intentions. Similarly, Ifinedo (2012) integrates TPB with PMT but removes the construct of attitude in his study of compliance with IS security policies. Although TPB provides a good basis for exploring the behavioral-based beliefs that may impact attitude, PMT offers strong support for including object-based beliefs by evaluating the threat component. The manner in which individuals recognize threats includes various environmental and intrapersonal sources of information (i.e., verbal persuasion, observational learning, personality, and prior experience) (Floyd et al. 2000; Maddux and Rogers 1983; Rogers 1975). In appraising the threat to their security, users evaluate whether they believe they are vulnerable to the threat (perceived threat vulnerability) and the severity of the threat (perceived threat severity). According to Johnston and Warkentin (2010), "once an individual is conscious of a threat, he or she will establish beliefs as to the seriousness of the threat and probability of personally experiencing the threat." (p. 551).

Prior research suggests that perceived threat vulnerability and perceived threat severity affect attitude toward security behaviors (Anderson and Agarwal 2010; Herath et al. 2014; Herath and Rao 2009) and are positively associated with individuals' overall perception of the security threat (Liang and Xue 2010). Perceived threat severity also affects behavioral intention in some instances (Lee 2011; Lee and Larsen 2009; Woon et al. 2005; Workman et al. 2008) but not in others (Ifinedo 2012). Results are also mixed when perceived threat vulnerability is used as an antecedent to behavioral intentions. Some studies find a significant relationship between perceived threat vulnerability and behavioral intentions (Lee 2011; Lee and Larsen 2009;

Workman et al. 2008) and others do not (Woon et al. 2005). However, consistent with TPB, our study includes attitude as a determinant of intention, and therefore, we can predict that perceived security threat vulnerability and perceived security threat severity will impact attitude directly, which then affects intention. The lack of consideration of attitude in some of the prior studies might in fact explain conflicting findings regarding perceived threat vulnerability and security and intentions.

H5: Perceived threat severity is positively related to attitude toward the new mandatory security policy change.

H6: Perceived threat vulnerability is positively related to attitude toward the new mandatory security policy change.

Awareness of the Security Policy Change

Some InfoSec research identifies awareness as an important construct to consider in the context of information security behaviors. Awareness is often an essential precursor of a change behavior because individuals need a basic knowledge of the expected change before they can enact the change. Studies suggest that individuals are noncompliant with security controls because of lack of awareness (e.g., Bulgurcu et al. 2010; Hu et al. 2007). Hu et al. (2007) identified three reasons why individuals are often seen as the weakest link in organizational security: lack of awareness, lack of management involvement, and conflicts between security policy and organizational objectives. Bulgurcu et al. (2010) investigated factors that lead to employee compliance with information security policies. Their model stresses the importance of information security awareness, which is made up of an individual's general security awareness and awareness of the information security policy.

The link from awareness to change in behavior first appeared in Rogers (1995)' diffusion of innovation (DOI) theory where awareness represents the initial stage of the innovation diffusion process model (Dinev and Hu 2007). The five stages of DOI, (1) knowledge, (2) persuasion, (3) decision, (4) implementation, and (5) confirmation (Rogers 1995), show the importance of awareness in the decision-making process regarding a behavior because knowledge of the innovation decision requires awareness. Awareness is traditionally defined as the extent to which a target population is conscious of change and formulates a general perception of what the change entails (Dinev and Hu 2007). It is during the awareness stage that an individual is exposed to the existence of the change and is provided information on how the change functions and what the benefits of the change are. Therefore, awareness is crucial to ensure proper security behaviors of individuals (D'Arcy et al. 2009). Accordingly, in this research, we predict that the more aware an individual is of a mandated security policy change, the more likely the individual will be positive about enacting the change early in the implementation process.

H7: Awareness of the mandatory security policy change is positively related to attitude toward the new mandatory security policy change.

Research related to IT implementation uses the terminology "triggers" to refer to events that have the ability to affect user reactions to the implementation (Lapointe and Rivard 2005). In the present study, various triggers were used by the University to raise awareness of the new security policy change. For example, the IT security office included a banner in the online course management site, prepared short articles for various university news outlets (both print and online), and created table cards for the dining facilities, among others. The various forms of "announcements" were meant to inform users of the new requirement and the importance to the organization and themselves. In theory, these communications should ultimately impact the users' behavioral intentions toward the change and their actual behavior through increased awareness (Hu and Dinev 2005; Straub and Welke 1998). This is consistent with prior research that emphasizes that managers' need to implement employee awareness programs to enhance security (Goodhue and Straub 1991). In fact, an entire line of research in InfoSec focuses on security education, training, and awareness (SETA) programs (e.g., Chen et al. 2015; Crossler and Bélanger 2009; Dhillon 1999; Hansche 2001; Straub and Welke 1998). In the present study, we seek to identify the effects triggers can have on user awareness, which can lead to early conformance, and the types of triggers that have the greatest impact.

H8: The type of organizational announcement (trigger) impacts individuals' awareness of the mandatory security policy change.

METHODOLOGY

To test our proposed research model, we surveyed faculty, staff, administrators, and students required by their university's IT department to change their passwords and meet new stronger password requirements before a specified date.

Instrument Development

We used established instrument development procedures (Moore and Benbasat 1991; Straub 1989) to operationalize the study's constructs by adapting existing measures from the IS literature where possible. All scales used in the study are presented in Appendix 1. The online survey was designed such that respondents were presented items contingent upon whether they already enacted the password change requirement. Items were worded either in past or future tense based on whether individuals had changed their passwords or not, respectively. Intention to conform early was measured on a seven-point scale from strongly disagree to strongly agree to the question: “I will wait (I considered waiting) until the very last minute to change my [University] password.” Actual early conformance was measured by a yes/no answer to the question: “Have you already changed your [University] password in accordance with the requirement [stated above]?”

The instrument was pilot-tested twice with minor changes to the wording of some questions between the first and second pilot tests. The first pilot test involved 39 undergraduates and the second involved 24 additional undergraduates. Following satisfactory reliability and validity analyses of the second pilot, a large-scale survey was distributed. Subjects used in pilot tests were not included in the final data collection. Prior to model testing, scales were resubjected to tests of validity and reliability using the final sample.

Timing

An important aspect of this research is the timing of the measurement of the actual change behavior. The initial announcement of the required change was made on February 1, with a deadline of July 1. Individuals would be locked out of their university accounts after failing to conform. Individuals were surveyed in April, approximately halfway through the allowable change period. Several factors played into this decision. Waiting until April allowed enough time for early conformers to enact the change. At the same time, individuals needed to be surveyed before the end of the change period to ensure we could capture the characteristics of late and nonconformers.

As shown in Table 1, costs and benefits vary depending on the timing of conformance. Separate anecdotal evidence provided to the research team by the University’s IT Office suggested that individuals who had not enacted the change by mid-April predominately waited until the last minute, qualifying them as late conformers (those who eventually met the deadline) or nonconformers (those who were locked out of the system). The IT Office also provided us with a schedule of total monthly user changes. Figure 2 indicates the change rate of early conformers remained relatively constant from March to April.

As can be seen from the figure, of the 80,124 users, an average of 7612 individuals (9.5%) per month conformed early and changed their password. The rate drops to 8.2% (6550 individuals) in May before jumping to 16.2% (13,009 individuals) in June. This provides evidence to support using April as the cut off for capturing early conformers as individuals are much more likely to be late or nonconformers at that point. Nearly half of the population (37,729 individuals or 47.1%) is considered to be composed of nonconformers who were locked out of the system. Another 24.4% (19,559 individuals) are considered late conformers.

Data Collection and Sample

The final instrument was primarily administered online through Survey Monkey; however, 51 responses were generated through a paper-based survey. This was necessary to ensure that some of the students from the pilot tests would not end up participating in the final survey. Furthermore, using different data collection approaches reduces issues related to common method bias (discussed further later). To solicit participation, researchers used email, listserv announcements, and in-class visits. All participants were offered entrance into a drawing for a chance to win one of several prizes ranging in value from $5 to $150. To ensure participants read all questions carefully, a control question similar to the technique used by Oppenheimer et al. (2009) was embedded in the survey. In total, 578 people anonymously answered the survey. However, 15 individuals failed to answer the control question properly and 25 individuals failed to complete the survey (stopped soon after starting) or took the survey twice (restarting the survey). One individual indicated hearing about the password change through the survey but stated having already changed his/her password[1]. Further analysis of this participant revealed a pattern of answering all 1s. Two other participants indicated an age of 11 and a similar pattern of all 1s. All three of these participants were removed, resulting in a total usable sample size of 535. At the time of the survey, 67 participants had enacted the password change, whereas 468 had not (consistent with data provided by the IT Office for the overall population). The average age of participants was 27 years, with a range of 19–69 years. Table 2 shows additional demographics for these respondents, which are consistent with the composition of the population at the University.

[1] We present effects of triggers per category (early conformers vs. others) later. All individuals in our final sample who were first made aware of the password requirements via our survey had not changed their passwords yet.

The sample was experienced in terms of computer and Internet usage, with an average of 15.6 and 12.6 years, respectively. To test for differences between online and paper survey responses, independent sample t-tests were run on key variables, and there were no statistical differences. To further test the effects of differences in the samples used, we compared the ratios of early conformers to the total participants per category of respondent (presented in Table 3). A detailed analysis of Table 3 shows there are more early conformers among administrators and fewer among undergraduate students. The lack of early conformance by students, who represent the largest user group, highlights the importance of promoting early conformance to members of the organization who may not be as committed as higher-level employees. We speculate that lower-level employees, or in our case, students, may lack the organizational commitment or ownership that higher-level employees are likely to have. We discuss this further in the discussion section.

Organizational Triggers

The university used announcements (i.e., triggers for change) beginning approximately 5 months in advance of the mandated password change. These announcements included banners within online student portals, such as the online classroom management site and webmail, table tents in dining halls, and various email communications that introduced the new requirements (see Table 4).

When asked, 274 of the respondents indicated they first heard of the mandated change requirement through the online course management site (see Figure 3). The next most recognized single trigger, as indicated in Table 5, was our survey, followed by “a friend or colleague” and articles on the university news website. As explained before, all those who learned of the change through the survey had not yet changed their password.

ANALYSES AND RESULTS

The research model was tested using Smart PLS 2.0 (Ringle et al. 2005) in two stages. First, we tested the measurement model to verify the reliability and validity of the instrument. Upon satisfactory results, we analyzed the structural model to test the proposed hypotheses. PLS was used in this research because of its strength in preliminary model building and its ability to handle large models and datasets (Chin et al. 2003; Gefen et al. 2011; Lowry and Gaskin 2014).

Measurement Model Testing

Before model testing, we conducted a test of the measurement model for reflective constructs in the study. Convergent validity was assessed with three *ad hoc* tests recommended by Anderson and Gerbing (1988): the standardized loadings, variance-extracted estimates, and construct composite reliabilities. Appendix 1 shows that all factor loadings exceeded 0.50 (Fornell and Bookstein 1982), and that average variance-extracted estimates exceeded the recommended lower limit of 0.5 (Fornell and Bookstein 1982) with a range of 0.60–0.80. Composite reliabilities were all above 0.70 (Netemeyer et al. 1990), with a range of 0.85–0.94. Finally, all Cronbach's alphas were above 0.70 (Nunnally 1978), with a range of 0.85–0.92. All these tests support the convergent validity of the measurement instrument.

Discriminant validity was assessed with tests recommended by Anderson and Gerbing (1988). Item-total correlations were examined, and the correlation pattern shows that an item posited to form a given subconstruct has a stronger correlation with it than with another construct, providing further evidence of discriminant and convergent validity. An additional discriminant validity criterion is that the variance shared by a construct with its indicators should be greater than the variance shared with other constructs in the model. The average variance extracted was used to assess the variance shared between the construct and its measurement items (Fornell and Bookstein 1982). A construct is considered to be distinct from other constructs if the square root of the average variance extracted for it is greater than its correlations with other latent constructs (Barclay et al. 1995). All constructs passed this test, as can be seen in Table 5, suggesting that the instrument exhibits convergent and discriminant validity.

Common method bias may occur when the predictor and criterion variables are provided by a common source or rater (Podsakoff et al. 2003; Podsakoff and Organ 1986), in this case a survey instrument. We used several approaches to reduce this concern: different instrument types, paper-based and online (Burton-Jones 2009), randomization of some questions on the online version (Podsakoff et al. 2003), and respondent anonymity to reduce evaluation apprehension (Podsakoff et al. 2003). In addition to these preventive measures, we conducted several *post hoc* statistical analyses to reduce concerns regarding the presence of common bias.

A Harman's one-factor test (Podsakoff et al. 2003) was conducted by including the reflective constructs into an exploratory factor analysis. The results show that at least five factors are present, and the most covariance explained by one factor is 39%. Further, as was shown in Table 4, there were no correlations above 0.90, which is also a possible indicator of common-methods bias (Bagozzi et al. 1991; Pavlou et al. 2007). Finally, a correlation matrix between all manifest variables was generated. Lindell and Whitney (2001) and Malhotra et al. (2006) explain that the second to smallest positive value in that matrix is a good conservative proxy for the correlation between the variables and a hidden common-method bias variable. In the present study, this correlation coefficient was 0.111. When squared, this correlation coefficient indicates the maximum amount of shared variance explained by common-method bias; in this study, a maximum of 1.2% of shared variance could be explained by common-method bias. From these analyses, concerns about common-methods bias are minimal in this study.

Structural Model Testing

Hypotheses were tested with SmartPLS[2]. Results for the structural model are presented in Figure 4. The results show intention to conform early is a determinant of early conformance behavior (H1); attitude positively affects intention (H2) but security self-efficacy does not (H4). As predicted, subjective norm (H3) does not affect intention but affects perceived security threat severity and vulnerability, and awareness positively impact attitude, thereby supporting H5, H6, and H7. Overall, the model explains 23.1% of the variance in early conformance behavior, 36.4% of the variance in attitude, and 13.2% of the variance for intention to conform early.

DISCUSSION

This research examines the antecedents of users' early conformance behavior related to a newly proposed security policy change. We focus on early conformance behavior in a context where users are required to change their password and create a new strong password annually, failing which they will be locked out of the system. The results from a survey of 535 respondents suggest that the proposed model can explain substantial variance in early conformance behavior and attitude and some variance in intention to conform early. We discuss the results and implications for research first and then discuss the implications for practice.

[2] Parameters for bootstrapping set mean replacement as missing value algorithm, cases = 535 and samples = 2000.

Behavioral Intention and Early Conformance Behavior

Investigations of end-user behavior are especially important when the behavior involves conformance to policies that improve organizational information security. However, the antecedents to actual conformance behavior remain elusive (Crossler et al. 2013; Shropshire et al. 2015). TPB posits a direct relationship between intention to perform a particular behavior and the actual behavior. However, most InfoSec studies only predict behavioral outcomes by investigating the relationship between antecedents and behavioral intention. This assumes that intention is a proxy for actual behavior, which has led some scholars to suggest that InfoSec research has failed to adequately demonstrate the true relationship between these constructs (Crossler et al. 2013; Shropshire et al. 2015). This is particularly troublesome considering that a few InfoSec studies show a discrepancy or disconnect between intention and behavior (Bagozzi 2007; Limayem et al. 2001; Shropshire et al. 2015). The results of this study confirm that intention to conform early leads to actual early conformance behavior in a real-life change in security policy. This is an important finding for InfoSec research. Further, our findings support the applicability of TPB in this context. We encourage more researchers to measure actual security behaviors in real-life settings as performed in this study to further confirm this important but rarely studied and sometimes conflicting relationship.

Grounded in TPB, this study argues that attitude and security self-efficacy, but not subjective norm, affect behavioral intention. One of the main findings in this respect is the critical role attitude plays in affecting intention and eventually the enactment of an early conformance behavior. A user's positive attitude toward the implementation of a new security policy substantially increases his/her intention to conform early, providing support for H2. In fact, the attitude–intention relationship is one of the three strongest paths in our model, suggesting that a positive attitude is essential to generate greater intention to conform early. This is an important result for researchers and practitioners alike. For researchers, it reaffirms the role of attitude in the encouragement of early conformance. Many prior adoption and InfoSec studies link antecedents directly to intention without measuring attitude even when they claim to use TPB as a theoretical foundation. Our results suggest researchers should be careful in doing so as attitude is critical in its effect on behavioral intention as predicted by the theory. This finding may also help explain why prior studies have mixed results with respect to self-efficacy and subjective norm (discussed further below). It is possible that by not including attitude in their models, researchers found tenuous relationships for subjective norm and/or perceived behavioral control, which are significant in certain studies but not in others. Future research should consider applying the original TPB foundation by consistently including attitude when attempting to understand behaviors in mandatory contexts.

From a theoretical standpoint, it would be interesting to explore how training programs, which focus on the creation of a positive attitude, could also raise the level of accountability of individuals, thereby further influencing positive behaviors (Vance et al. 2013). By exploring attitude within a nonvoluntary setting, our research provides a better understanding of the attitudes surrounding early conformance and the potential consequences of these attitudes.

As hypothesized, we did not find a significant relationship between subjective norm and intention to conform early (H3). Although prior research shows a positive relationship between social influence and behavioral intentions (e.g., Johnston and Warkentin 2010; Liang and Xue 2010), perceived social pressure is not a factor for early conformers. Consistent with prior research, we attribute subjective norm’s lack of influence on intention to the fact that early conformers are leaders rather than followers. In fact, previous research on eco-friendly consumer behaviors (Jansson 2011; Jansson et al. 2011; Seebauer 2015) shows that early adopters are driven by the impact their behaviors have on society. This concern for society's well-being appears to be shaped by social norms; however, it is deeply espoused by individuals and becomes part of personal norms (Seebauer 2015). Therefore, future research may consider personal norm in lieu of or in complement to subjective norm. For organizations, this indicates that it is critical to take the necessary steps to harness the social influence early conformers can have on those who are destined to be late or nonconformers. Although we are not suggesting that future research omit subjective norm from TPB-based models, we recommend that its influence be considered from the standpoint of early, late, and nonconformance. Furthermore, there is a need in future research to explore whether the lack of significance for the effect of subjective norm on intention would apply to other information security compliance domains beyond password contexts or even in other early uses of IS. Are all early adopters of mandatory IS or early conformers to mandatory changes less influenced by subjective norm? This intriguing finding needs to be further explored in future work.

Contrary to our predictions, our results suggest that security self-efficacy is not a significant predictor of intention to conform early. Although this finding is contrary to the relationship put forth by TPB, it is not completely unexpected because of the conflicting findings around self-efficacy in prior research. For example, several studies found a significant positive link between an employee's self-efficacy and intention to comply with a security policy (Bulgurcu et al. 2010; Son 2011), even in mandatory environments (Kirsch and Boss 2007). Conversely, D'Arcy et al. (2009) reported findings of a negative impact of security self-efficacy on security compliance intentions. Some criminology researchers suggest that people with higher self-efficacy believe they can circumvent security measures and have minimal consideration for security policies (Jacobs 2010; Krueger and Dickson 1994). In their review of research on self-efficacy, Gist and Mitchell (1992) propose that the validity of self-efficacy as a predictor of motivation (or intention in most IS research) to perform a task is linked to the complexity of the task. The authors suggest that instruments generally adopted for measuring self-efficacy may not be appropriate depending on task complexity level. In our case, it is possible that our instrument did not catch enough variation for a relatively simple task, prohibiting us from finding a significant link between self-efficacy and intention to conform early. A closer look at responses for self-efficacy reveals relatively high reported amounts across participants with a mean of 5.08 (on a seven-point Likert scale) and a low standard deviation of 1.38[3]. Therefore, it seems likely that many participants viewed the process of performing the requested password change as one of low complexity. As such, participants were all confident in their ability to perform the change, whether or not they intended to. Given the mixed results of prior research and our lack of a positive finding, we suggest that future research consider the effects of task complexity on self-efficacy (Gist and Mitchell 1992) and provide a clear definition of the self-efficacy construct used (Hardin et al. 2008).

An important finding from the study to discuss is the possibility that compliance is linked to organizational commitment. In our sample, administrators were much more likely to be early conformers than students. In a study based on construal level theory (Trope and Liberman 2003), Tam et al. (2010) found that users who change their passwords early tended to focus more on what is desirable (i.e., password efficacy) rather than what is convenient (i.e., minimal compliance) when the account to be protected contains critical information. However, the quality or success of the password change policy does not depend solely on the timeframe for change.

[3] Means (standard deviations) for attitude and subjective norm were 4.48 (1.52) and 3.67 (1.43), respectively.

Beautement et al. (2009) theorized and Inglesant and Sasse (2010) showed that users (notably students) have a compliance budget that determines whether they will invest efforts in conforming to a particular password policy.

Early conformers' level of conformance could be a good indicator to know if the policy in question is deemed essential enough by a portion of the population that might have lower compliance budgets because of low commitment. If that is the case, network externalities explained by Katz and Shapiro (1985) could apply, and early conformers within a category of employees could influence others of the same category and lead to the acceleration of new conformances. On the contrary, the absence of early conformance within a category of the population could act as a deterrent to others' conformance and even to the appearance of dissatisfaction or resistance in that category of users. A possible fruitful area for future research, therefore, is to study the possible links between early compliance and organizational commitment.

Determinants of Attitude

On the basis of prior InfoSec research involving PMT (Herath and Rao 2009; Ifinedo 2012), we proposed two antecedents to attitude: perceived security threat severity and vulnerability. The results suggest that both constructs are significant determinants of attitude, lending support for H5 and H6. Users who are conscious of a threat evaluate whether they are vulnerable to that threat. If so, the subsequent "fear appeal" (Johnston and Warkentin 2010) positively influences their attitudes toward security (Anderson and Agarwal 2010; Herath and Rao 2009). In this research, the more vulnerable people feel, the more favorable they are to the mandatory security change. Conversely, individuals who fail to perceive the severity of the security threat or their vulnerability to the threat are less likely to have a positive attitude toward the required policy change. This reinforces the importance of educating users on the vulnerabilities resulting from never changing their passwords, which should increase their positive attitude toward the new security policy.

Awareness of the security policy change has a direct and positive impact on attitude toward the security policy change, lending support for H7. Although awareness is included in a variety of InfoSec studies (e.g., Bulgurcu et al. 2010; Hu and Dinev 2005; Hu et al. 2007; Straub and Welke 1998), none of the prior studies specifically considered what factors led to the awareness. Therefore, a significant contribution of this study is the inclusion of triggers, the type of announcements, and their effect on awareness. Results suggest the type of trigger does indeed impact awareness, supporting H8. When mandating the security policy, the university's IT personnel hoped the use of announcements would increase awareness, inform users of the specific requirements, and help them understand the importance of the policy change to the institution and its stakeholders. More than half the respondents indicated that they first heard of the mandated change requirement through the online course management site (see Table 6 and Figure 5). Interestingly, the survey used for this research also triggered awareness. In fact, open-ended comments returned with the survey indicated that the survey itself was a wakeup call: "*I knew that changing my password was recommended, but I did not know it will be mandated for me to change my password. This survey drew that to my attention,"* or *"I hope something else comes out, like a newsletter or email that gives more information about the PID change because this is the first I have heard of it."* Because of the importance of triggers in generating awareness, which positively impacts attitude toward the policy change and encourages early conformance, future research should include measures of what triggers awareness in various settings instead of just including a generic measure of awareness of the security policy.

Implications for Practice

Our findings have various practical implications for organizations and managers. As discussed previously, organizations incur significant costs if a large number of users insist on being late or nonconformers. Procrastination, waiting until the deadline, and nonconformance lead to last minute rushes and may crash the system, overload the help desk, or cause hotline traffic jams. Furthermore, forcing users to enact the change can amplify user negativity toward the policy change, whereas successful encouragement can give users a sense of ownership and lead to full acceptance of the security policy change. Managers can use this understanding to identify ways to alleviate some of the burdens that delayed conformance has on the system. As such, organizations can develop cost-effective implementation strategies that increase awareness, encourage early conformance, and turn would-be-late or nonconformers into early conformers. Although many training programs currently ignore the role of attitude (Karjalainen and Siponen 2011), development of such programs need to consider the effect that attitude has on early conformance. A positive attitude leads to positive intention and, ultimately, the desired behavior. It is critical that organizations consider these findings when designing their SETA programs (e.g., Crossler and Bélanger 2009; Goodhue and Straub 1991; Straub and Welke 1998). Doing so can reduce the procrastination and resistance of late and nonconformers and successfully encourage early conformity.

It is also important for organizations to realize that awareness plays an extremely important role in early conformance. Without awareness, users do not know what is expected of them, and potentially positive effects of attitude are absent. In our context, although the online class management site proved somewhat successful in making users aware of the change, the University could have done a better job of communicating the change and increasing awareness across all users. Any initiative should have multiple triggers to sufficiently increase awareness for everyone involved. Our results suggest that organizations should increase employee awareness by using targeted communications about the new requirement and reasons for the enhanced controls (Goodhue and Straub 1991) and providing training specific to the security concerns (Straub and Welke 1998). Getting people actively involved in thinking about a change (like those individuals who realized through the survey that change was happening) is also an effective means of increasing awareness. Accordingly, when implementing training, it might be useful to engage users in an activity such as the use of online password check software where they can verify the strength of their passwords (Dell'Amico et al. 2010). Such an activity would likely increase user perceptions of the severity of the threat and of the individuals' vulnerability to the threat, and raise their awareness of the new requirements. Branding also seems to make an important difference as open-ended comments indicate that the logo shown in Figure 5 was "eye-catching" and attracted much attention.

Organizations are well served to understand and maximize the facilitators of early conformance. As leaders rather than followers, early conformers are not similarly affected by the social pressure of their peers. Nevertheless, if the security policy change is managed appropriately, early conformers will likely be able to exert influence on individuals who are predestined to be late or nonconformers. The security policy change becomes less costly for the organization if an organization can capture the social pressure that early conformers might have on their less proactive peers.

Limitations and Additional Future Research

There are possible limitations to this study. One limitation is the use of a public institution to study mandated security policy changes, which may not be fully generalizable to all organizations. The relative simplicity of the task required for compliance with the new security policy may have also impacted our capacity to seize the influence of self-efficacy, particularly because a large portion of our sample was composed of students. Further research with a more complex task and diversified sample may clarify this relationship. In addition, respondents were asked to indicate whether they had changed their passwords. Therefore, in essence, this is a self-reported behavior. However, we believe that respondents, in general, clearly and properly indicated their change status because they were reassured about confidentiality of the survey, and no personally identifiable data were collected. As explained in the description of the sample, one data point was removed because it was not possible for the person to have changed their password and first hear about the change requirement from the survey.

Attitude provides a strong determinant of intention to conform early. However, the results show intention to conform early is the construct with the lowest explained variance in the model. This suggests that other factors should be considered in future studies of early conformance intentions. Some personal characteristics of individuals may have more impact on intentions than their perceptions of the security threats and security policy change. For example, from the literature on pre-existing habits (Limayem et al. 2001; Turel 2015) or on intrinsic and extrinsic motivation (Agrifoglio et al. 2012), it is possible to determine whether different types of motivation impact the usage of technologies. Culture could also have an impact on early conformance. Type of personal/social culture (Aljahdali and Poet 2013) or a “culture of information security” that exists in an organization (Da Veiga and Eloff 2010; Schlienger and Teufel 2002) could be studied in this context. Finally, individuals’ prior experience with a security incident might affect how rapidly they decide to conform with the new security policy.

In the information privacy literature, prior experience with an information privacy violation influences protection intentions (Crossler and Bélanger 2013; Smith et al. 1996; Xu et al. 2012).

CONCLUSION

Information security is a high priority for organizations; however, individuals asked to implement newly mandated changes in security tend to procrastinate, resist, fail to perform, or circumvent the behavior required of the new policy. To better understand what leads individuals to be early conformers, this study uniquely measures actual early conformance to a security change in the context of an implementation of new password policies. Using data collected from 535 respondents, some of whom had enacted the change and others who had not, we are able to explain significant variances in users' attitudes toward the security policy change and actual early conformance behaviors. Importantly, intention to conform early is a predictor of actual early conformance behavior.

The research provides numerous contributions to both research and practice. In terms of research, this study contributes by focusing on and measuring both intention and actual change behavior rather than stopping at user intention. Further, by exploring an actual security change behavior, this study is one of the first to test the links between attitude, intention, and behavior, avoiding conclusions drawn on untested influences between intentions and behaviors. By focusing on a nonvolitional setting, the research provides a better understanding of attitudes surrounding technology-enforced security policies and the potential consequences of these attitudes. It also highlights the importance of awareness in influencing change behavior. Finally, the study contributes to research by measuring which triggers lead to awareness of the newly proposed security policy change. Most studies that measure awareness have not empirically identified how awareness can be increased. We encourage future researchers to consider such measures in their research.

Organizations can better plan for and implement new IS security policies by doing three things: identifying the multifaceted nature of mandated technology-enforced security policy changes, recognizing influences of awareness and branding, and considering the effect of attitude. We provide insight on how organizations can facilitate and embrace early conformance to avoid the many pitfalls and negative consequences that late and nonconformant users present. Importantly, our research suggests that InfoSec researchers may need to shift their efforts from compliance/noncompliance-only studies to research on early, late, and nonconformance because the determinants of overall compliance (such as social norm) can differ from those of early conformance.

APPENDIX 1. Measurement Model Testing and Descriptive Statistics for Reflective Constructs

Construct items (note: PID = personal identification)	**Load.**	**AVE**	**CR**	**Alpha**
Security Policy Change Awareness [Modified from Bulgurcu et al. (2010)]		0.798	0.922	0.874
I am aware of the requirements prescribed by [university] to change my PID password.	0.882			
I understand the rules and requirements regarding the PID password change prescribed by [university].	0.896			
I know my responsibilities to change my PID password as prescribed by [university].	0.903			
Subjective Norm [Modified from social influence concept by Venkatesh et al. (2003)]		0.804	0.925	0.877
I think my classmates and/or colleagues believe I should change my PID password.	0.815			
People who influence my behavior think that I should change my PID password.	0.927			
People who are important to me think I should change my password.	0.942			
Attitude [Modified from Venkatesh et al. (2003)]		0.751	0.938	0.915
Mandating this change of password is a good idea.	0.915			
*Mandating this change of password is a bad idea. (*Reverse Coded Item)	0.735			
This required change of password will make working with my [university] account safer.	0.921			
This required change of PID password will make working with my [university] account safer.	0.832			
I support the process requiring me to change my password.	0.916			
Security Self-efficacy [Modified from Johnston and Warkentin (2010)]		0.596	0.851	0.854
I am able to change my PID password without much effort.	0.949			
Learning how to change my PID password is easy for me.	0.837			
I know how to change my PID password.	0.656			
Perceived Security Threat Vulnerability [Modified from Liang and Xue (2010)]		0.741	0.920	0.884
Having a weak PID password poses a threat to me.	0.887			
The vulnerability caused by a weak PID password threatens me.	0.834			
Weak PID passwords are a danger to my Virginia Tech account.	0.900			
It is risky to use my VT account if it has a weak PID password.	0.897			
Perceived Security Threat Severity [Modified from Johnston and Warkentin (2010); Liang and Xue (2010)]		0.775	0.932	0.903
If my PID password and personal information were compromised, the consequences would be severe.	0.854			
Having someone else figure out my PID password poses a serious threat to my university account.	0.856			
I could incur great losses if my PID password was hacked.	0.879			
It would be dreadful if my PID password was compromised.	0.897			
Intention to Conform Early [Created for this research; Adapted from Lapointe and Rivard (2005)]		1.000	1.000	1.000
I will wait (I considered waiting) until the very last minute to change my PID password.	1.000			
Early Conformance Behavior [Created for this research]		1.000	1.000	1.000
Have you already changed your PID password in accordance with the requirement [stated above]?	1.000			

REFERENCES

Agrifoglio, R., Black, S., Metallo, C., and Ferrara, M. 2012. "EXTRINSIC VERSUS INTRINSIC MOTIVATION IN CONTINUED TWITTER USAGE," *The Journal of Computer Information Systems* (53:1), pp 33-41.

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp 179-211.

Ajzen, I. 2012. "The Theory of Planned Behavior," in *Handbook of Theories of Social Psychology: Volume One,* P. A. M. Van Lange, E. Kruglanski and E. T. Higgins (eds.), Sage Publications Ltd.: London.

Ajzen, I., and Fishbein, M. 1972. "Attitudes and normative beliefs as factors influencing behavioral intentions," *Journal of Personality and Social Psychology* (21:1), pp 1-9.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, (Prentice-Hall: Englewood Cliffs, NJ.

Aljahdali, H. M., and Poet, R.,2013, The Affect of Familiarity on the Usability of Recognition-Based Graphical Passwords: Cross Cultural Study between Saudi Arabia and the United Kingdom," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1528-1534.

Anderson, C. L., and Agarwal, R. 2010. "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly* (34:3) Sep, pp 613-643.

Anderson, J. C., and Gerbing, D. W. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin* (103:3), pp 411-423.

Bagozzi, R. P. 2007. "The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift," *Journal of the Association for Information Systems* (8:4), pp 244-254.

Bagozzi, R. P., Yi, Y., and Phillips, L. W. 1991. "Assessing Construct Validity in Organizational Research," *Administrative Science Quarterly* (36:3), pp 421-458.

Barclay, D., Higgins, C. A., and Thompson, R. L. 1995. "The Partial Least Squares Approach to Causal Modeling, Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp 285-309.

Barra, R., McLeod, A., Savage, A., and Simkin, M. 2010. "Passwords: Do User Preferences and Website Protocols Differ From Theory?," *Journal of Information Privacy & Security* (6:4), pp 50-69.

Beautement, A., Sasse, M. A., and Wonham, M.,2009, The compliance budget: managing security behaviour in organisations," Proceedings of the 2008 workshop on New security paradigms, ACM, pp. 47-58.

Berger, U. 2011-2012. "CSI/FBI Computer Crime and Security Survey ", C. S. Institute (ed.).

Bonneau, J., Herley, C., van Oorschot, P. C., and Stajano, F. 2015. "Passwords and the Evolution of Imperfect Authentication," *Communications of the Acm* (58:7) Jul, pp 78-87.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., and Burkman, J. R. 2002. "Do I really have to? User acceptance of mandated technology," *European Journal of Information Systems* (11:4), pp 283-295.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Mis Quarterly* (34:3) Sep, pp 523-548.

Burton-Jones, A. 2009. "Minimizing Method Bias Through Programmatic Research," *MIS Quarterly* (33:3), pp 445-447.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., and DeMara, R. F. 2004. "Evaluation of the human impact of password authentication practices on information security," *Informing Science: Journal* (7), pp 67-85.

Chandra, A., and Calderon, T. G. 2003. "Toward a Biometric Security Layer in Accounting Systems," *Journal of Information Systems* (17:2) Sept. 1, pp 51-70.

Chen, Y., Ramamurthy, K., and Kuang-Wei, W. 2015. "Impacts Of Comprehensive Information Security Programs On Information Security Culture," *Journal of Computer Information Systems* (55:3), pp 11-19.

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp 157-188.

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) June 1, 2003, pp 189-217.

Cluley, G. 2013. "55% of net users use the same password for most, if not all, websites. When will they learn?," N. Security (ed.).

Crossler, R. C., and Bélanger, F. 2013. "Mobile Information Privacy Protection Practices (MIP3)," in *IFIP WG8.11/11.13 Dewald Roode Workshop on Information Security*: Buffalo, NY.

Crossler, R. E., and Bélanger, F. 2009. "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage," *Journal of Information Systems Security* (5:3), pp 3-22.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:1), pp 90-101.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* (20), pp 79-98.

Da Veiga, A., and Eloff, J. H. P. 2010. "A framework and assessment instrument for information security culture," *Computers & Security* (29:2) 3//, pp 196-207.

Dell'Amico, M., Michiardi, P., and Roudier, Y.,2010, Password strength: An empirical analysis," INFOCOM 2010 Proceedings, IEEE, pp. 983-991.

Dhillon, G. 1999. "Managing and controlling computer misuse," *Information Management Computer Security* (7:4), pp 171-175.

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp 386-408.

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*, (Addison-Wesley Publishing Company: Reading, MA.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A meta-analysis of research on protection motivation theory," *Journal of Applied Social Psychology* (30:2), pp 407-429.

Fornell, C., and Bookstein, F. 1982. "Two strucutral equation models: LISREL and PLS applied to consumer exit-voice theory," *Journal of Marketing Research* (19), pp 440-452.

Furnell, S. 2011. "Assessing password guidance and enforcement on leading websites," *Computer Fraud & Security* (December), pp 10-18.

Furnell, S. 2014. "Password practices on leading websites - revisited," *Computer Fraud & Security* (December), pp 5-11.

Gefen, D., Straub, D., and Rigdon, E. 2011. " An Update and Extension to SEM Guidelines for Admnistrative and Social Science Research," *MIS Quarterly* (35:2), pp iii-xiv.

Gelinas, U. J., Dull, R. B., and Wheller, P. 2015. *Accounting information systems*, (10th ed.) Thomson South-Western.

Gist, M. E., and Mitchell, T. R. 1992. "Self-efficacy: A theoretical analysis of its determinants and malleability," *Academy of Management Review* (17:2), pp 183-211.

Goodhue, D. L., and Straub, D. W. 1991. "Security concerns of system users : A study of perceptions of the adequacy of security," *Information & Management* (20:1), pp 13-27.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp 203-236.

Gyorffy, J. C., Tappenden, A. F., and Miller, J. 2011. "Token-based graphical password authentication," *International Journal of Information Security* (10:6) Nov, pp 321-336.

Hansche, S. 2001. "Designing a security awareness program: Part 1," *Information Systems Security* (9:6), pp 14-22

Hardin, A. M., Chang, J. C.-J., and Fuller, M. A. 2008. "Clarifying the Use of Formative Measurement in the IS Discipline: The Case of Computer Self-Efficacy," *Journal of the Association for Information Systems* (9:9), pp 544-546.

Herath, T., Chen, R., Wang, J. G., Banjara, K., Wilbur, J., and Rao, H. R. 2014. "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal* (24:1) Jan, pp 61-84.

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) Apr, pp 106-125.

Herley, C., and Oorschot, P. V. 2012. "A Research Agenda Acknowledging the Persistence of Passwords," *IEEE Security & Privacy* (10:1), pp 28-36.

Hu, Q., and Dinev, T. 2005. "Is spyware an Internet nuisance or public menace?," *Communications of the ACM* (48:8), pp 61-66.

Hu, Q., Hart, P., and Cooke, D. 2007. "The role of external and internal influences on information systems security - a neo-institutional perspective," *The Journal of Strategic Information Systems* (16:2), pp 153-172.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security* (31:1), pp 83-95.

Infosecurity_Magazine 2016. "Password Misuse is Rampant at US Businesses."

Inglesant, P., and Sasse, M. A.,2010, The True Cost of Unusable Password Policies: Password Use in the Wild," Computer Human Interaction, Atlanta, Georgia, pp. 383-392.

Jacobs, B. A. 2010. "Deterrence and Deterrability," *Criminology* (48:2), pp 417-441.

Jansson, J. 2011. "Consumer eco-innovation adoption: assessing attitudinal factors and perceived product characteristics," *Business Strategy and the Environment* (20:3), pp 192-210.

Jansson, J., Marell, A., and Nordlund, A. 2011. "Exploring consumer adoption of a high involvement eco-innovation using value-belief-norm theory," *Journal of Consumer Behaviour* (10:1), pp 51-60.

Jobusch, D. L., and Oldehoeft, A. E. 1989. "A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 2," *Computers & Security* (8:7), pp 587-604.

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), pp 548-566.

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An integrative study of information systems security effectiveness," *International Journal of Information Management* (23:2), pp 139-154.

Karjalainen, M., and Siponen, M. 2011. "Toward a new meta-theory for designing information systems (IS) security training approaches," *Journal of the Association for Information Systems* (12:8), pp 518-555.

Katz, M. L., and Shapiro, C. 1985. "Network externalities, competition, and compatibility," *The American economic review* (75:3), pp 424-440.

Kirsch, L., and Boss, S.,2007, The last line of defense: motivating employees to follow corporate security guidelines," International Conference on Information Systems, Montreal, QC, Canada, p. 103.

Krueger, N., and Dickson, P. R. 1994. "How believing in ourselves increases risk taking: Perceived self-efficacy and opportunity recognition," *Decision Sciences* (25:3), pp 385-400.

Lam, T., and Hsu, C. H. 2004. "Theory of planned behavior: Potential travelers from China," *Journal of Hospitality & Tourism Research* (28:4), pp 463-482.

Lapointe, L., and Rivard, S. 2005. "A multilevel model of resistance to information technology implementation," *MIS Quarterly* (29:3), pp 461-491.

Lee, S. M., Lee, S. G., and Yoo, S. 2004. "An integrative model of computer abuse based on social control and general deterrence theories," *Information & Management* (41:6), pp 707-718.

Lee, Y. 2011. "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective," *Decision Support Systems* (50:2), pp 361–369.

Lee, Y., and Larsen, K. R. 2009. "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," *European Journal of Information Systems* (18:2), pp 177-187.

Li, L., Liang, L. J., Lin, C., Wu, Z., and Wen, Y. 2009. "Individual attitudes and perceived social norms: Reports on HIV/AIDS-related stigma among service providers in China," *International Journal of psychology* (44:6), pp 443-450.

Liang, H., and Xue, Y. 2010. "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems* (11:7), pp 394-413.

Limayem, M., Hirt, S. G., and Chin, W. W.,2001, Intention does not always matter: the contingent role of habit on IT usage behavior," ECIS 2001 Proceedings, Bled, Slovenia, pp. 274-286.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp 114-121.

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It," *IEEE Transactions on Professional Communication* (57:2), pp 123-146.

Maddux, J. E., and Rogers, R. W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology* (19:5), pp 469-479.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., and Raghu, T. 2010. "Moving toward black hat research in information systems security: an editorial introduction to the special issue," *Mis Quarterly* (34:3), pp 431-433.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp 1865-1883.

Manning, K. C., Bearden, W. O., and Madden, T. J. 1995. "Consumer innovativeness and the adoption process," *Journal of Consumer Psychology* (4:4), pp 329-345.

Mattord, H. J., Levy, Y., and Furnell, S. 2014. "Factors for Measuring Password-Based Authentication Practices," *Journal of Information Privacy and Security* (10), pp 71-94.

Milne, G. R., Labrecque, L. I., and Cromer, C. 2009. "Toward an understanding of the online consumer's risky behavior and protection practices," *Journal of Consumer Affairs* (43:3), pp 449-473.

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), pp 192-222.

Netemeyer, R. G., Johnston, M. W., and Burton, S. 1990. "Analysis of role conflict and role ambiguity in a structural equations framework," *Journal of Applied Psychology* (75:2), pp 148-157.

Nunnally, J. 1978. *Psychometric Theory*, (McGraw-Hill: New York, NY.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., and Whitty, M.,2014, Understanding Insider Threat: A Framework for Characterising Attacks," IEEE Security and Privacy Workshops, pp. 214-228.

Oppenheimer, D. M., Meyvis, T., and Davidenko, N. 2009. "Instructional manipulation checks: Detecting satisficing to increase statistical power," *Journal of Experimental Social Psychology* (45:4), pp 867-872.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding And Mitigating Uncertainty In Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp 105-136.

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), pp 879-903.

Podsakoff, P. M., and Organ, D. W. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp 531-544.

Ringle, C. M., Wende, S., and Will, A. 2005. "SmartPLS, Release: 2.0 (beta) ", SmartPLS Hamburg, Germany

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

Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology: Interdisciplinary and Applied* (91:1), pp 93-114.

Rubens, P. 2014. "Has the flawed password system finally had its day?," in *BBC*, BBC.

Schlienger, T., and Teufel, S. 2002. "Information Security Culture," in *Security in the Information Society: Visions and Perspectives,* M. A. Ghonaimy, M. T. El-Hadidi and H. K. Aslan (eds.), Springer US: Boston, MA, pp. 191-201.

Seebauer, S. 2015. "Why early adopters engage in interpersonal diffusion of technological innovations: An empirical study on electric bicycles and electric scooters," *Transportation Research Part A: Policy and Practice* (78), pp 146-160.

Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security* (49), pp 177-191.

Siponen, M., and Iivari, J. 2006. "Six design theories for IS security policies and guidelines," *Journal of the Association for Information Systems* (7:7), pp 445-472.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly* (20:2), p 167.

Son, J. Y. 2011. "Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies," *Information & management* (48:7), pp 296-302.

Straub, D. W. 1989. "Validating instruments in MIS research," *MIS Quarterly* (13:2), pp 147-169.

Straub, D. W. 1990. "Effective IS security: An empirical study," *Information Systems Research* (1:3), pp 255-276.

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

Straub, E. T. 2009. "Understanding technology adoption: Theory and future directions for informal learning," *Review of Educational Research* (79:2), pp 625-649.

Summers, W. C., and Bosworth, E. 2004. "Password policy: the good, the bad, and the ugly," in *Proceedings of the winter international synposium on Information and communication technologies*, Trinity College Dublin: Cancun, Mexico, pp. 1-6.

Tam, L., Glassman, M., and Vandenwauver, M. 2010. "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology* (29:3), pp 233-244.

Trope, Y., and Liberman, N. 2003. "Temporal construal," *Psychological review* (110:3), p 403.

Trustwave 2015. "2015 Trustwave Global Security Report," p. 110.

Turel, O. 2015. "Quitting the use of a habituated hedonic information system: a theoretical model and empirical examination of Facebook users," *European Journal of Information Systems* (24:4), pp 431-446.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp 263-290.

Venkatesh, V., Morris, M., Davis, G. B., and Davis, F. D. 2003. "User acceptance of information technology: Toward a unified view," *MIS Quarterly* (27:3), pp 425-478.

Warkentin, M., Davis, K., and Bekkering, E. 2004. "Introducing the check-off password system (COPS): An advancement in user authentication methods and information security," *Journal of Organizational and End User Computing* (16:3), pp 41-58.

Willison, R., and Warkentin, M. 2013. "Beyond deterrence: an expanded view of employee computer abuse," *Mis Quarterly* (37:1), pp 1-20.

Woon, I. M. Y., Tan, G. W., and Low, R. T.,2005, A Protection Motivation Theory Approach to Home Wireless Security," Twenty-Sixth International Conference on Information Systems (ICIS), pp. 367-380.

Workman, M., Bommer, W. H., and Straub, D. W. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24:6), pp 2799-2816.

Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M.,2012, Measuring Mobile Users' Concerns for Information Privacy," Thirty Third International Conference on Information Systems (ICIS), Orlando.

Biographies

France Bélanger is the R. B. Pamplin Professor and the Tom & Daisy Byrd Senior Faculty Fellow at Virginia Tech Pamplin College of Business. Her research focuses on digital interactions between individuals, businesses, and governments and the related information security and privacy issues. Her award-winning work has been published in leading IS journals. She received the 2008 IEEE Education Society Research Award, the 2008 Hoeber Research Excellence Award, the 2013 INFORMS Design Science Award for Outstanding Research Stream, and the 2014 Best Paper of the Year Award for *Database for Advances in Information Systems*. She is or has been a Senior Editor, a Guest Senior Editor, and an Associate Editor for the *Journal of the Association for Information Systems, MIS Quarterly,* and *Information Systems Research,* and a number of other journals as well as Guest Editor for *Information Systems Journal* and *Database for Advances in Information Systems.* Her work has been funded by several agencies, corporations, and research centers, including the National Science Foundation. She was named Fulbright Distinguished Chair in 2006 (Portugal) and Erskine Visiting Fellow in 2009 (New Zealand). She is a visiting Professor at Addis Ababa University in Ethiopia.

Stéphane E. Collignon, PhD, is a Teaching Assistant Professor at the Department of MIS in the College of Business and Economics at West Virginia University. He received his MBA from Duquesne University and BA in Entrepreneurship from Institut Commercial de Nancy, France. His two main current research interests are transportation procurement issues and privacy issues on social media. These topics are partially inspired from his experience in industry where Collignon worked for 7 years in logistics as an analyst and a project manager in two different French distribution companies. His research has appeared in *Information & Management, Information Technology Management,* and *Expert Systems with Applications*. Collignon is a member of the Decision Sciences Institute and the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).

Kathy Enget, PhD, CPA, CFE, is an Assistant Professor at the Department of Accounting and Law, University at Albany, SUNY. Her research and teaching focuses on forensic accounting. In particular, she concentrates her research on auditing procedures, including nature, timing and extent, particularly as it relates to the detection of fraud, continuous auditing, and continuous monitoring. She is a behavioral researcher, who utilizes experimental, qualitative, survey, and interview techniques in her research and incorporates insights from auditing, information systems, and other disciplines to investigate these research questions. She uses her research, skills, and experiences gained as a former Big 4 forensic accounting manager to provide students with a hands on academic education that will prepare them to be ready on day one of their careers as auditors and forensic accounting professionals.

Eric Negangard is an Assistant Accounting Professor at the University of Virginia's McIntire School of Commerce. His research primarily focuses on financial reporting fraud, internal controls, and the involvement of forensic specialists in the auditing environment. More specifically, he uses a combination of psychology theory and innovative measurement techniques to examine the decision processes and subsequent attributions of those involved in and, affected by, fraudulent financial reporting. His work has been published in *Auditing: A Journal of Practice and Theory* and presented at national conferences sponsored by the American Accounting Association, as well as other conferences and university research workshops. Professor Negangard also has an extensive professional experience as a Forensic Accountant and has provided advisory and assurance services to numerous domestic and international organizations. Before pursuing a career in academia, he was a Manager in KPMG's Forensic Services practice and served as a National Instructor. He is a licensed CPA in the state of Indiana and a Certified Fraud Examiner. He has taught various accounting and business related courses to undergraduate, graduate, and professional students, and is the recipient of several research and teaching awards. He currently teaches an undergraduate auditing course and a graduate course in forensic accounting.

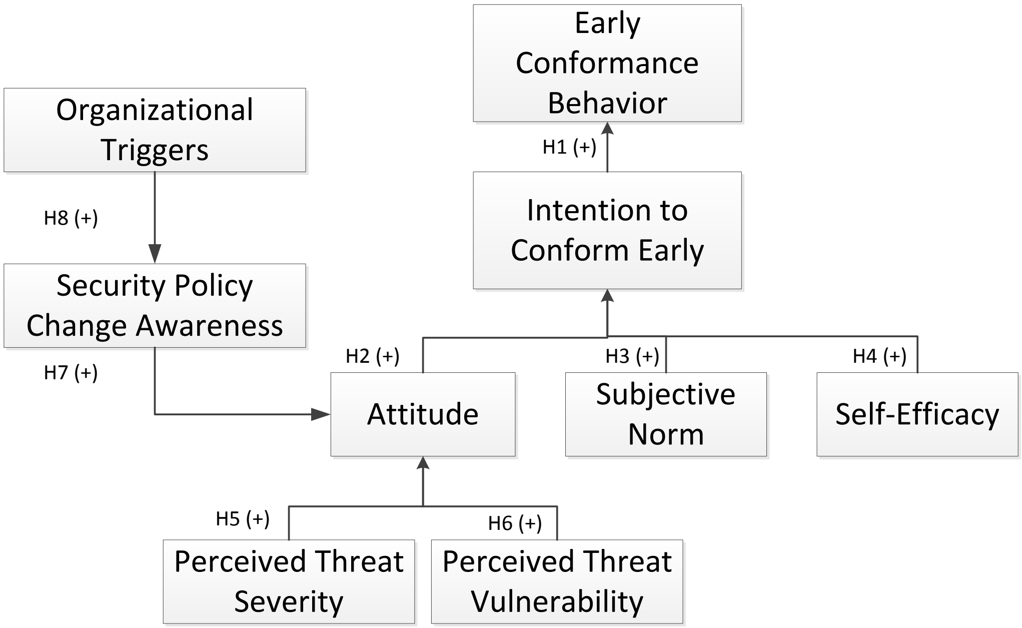

Early Conformance Behavior
H1 (+)
Organizational Triggers
H8 (+)
Intention to Conform Early
Security Policy Change Awareness
H2 (+)
H3 (+)
H4 (+)
H7 (+)
Attitude
Subjective Norm
Self-Efficacy
H5 (+)
H6 (+)
Perceived Threat Severity
Perceived Threat Vulnerability

Figure 1. Research Model

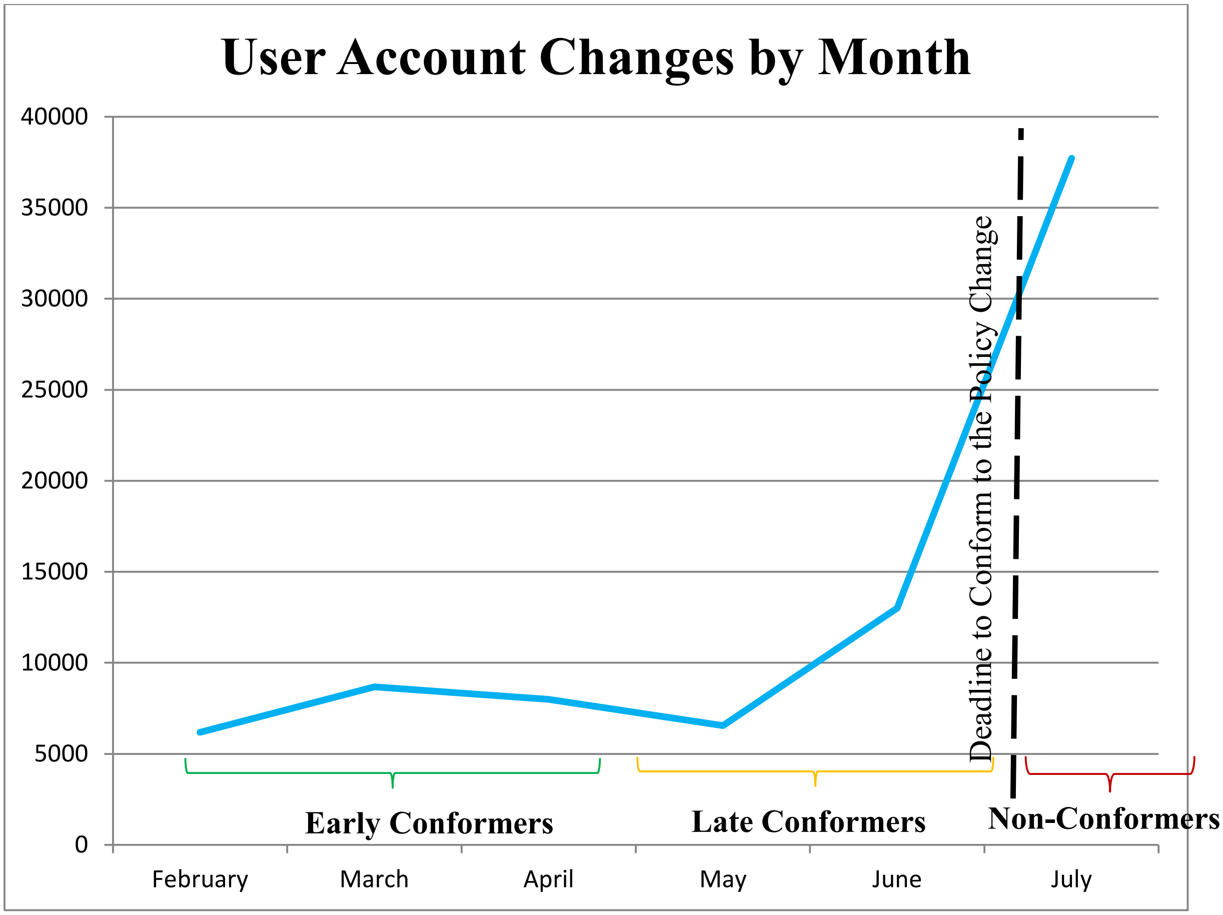
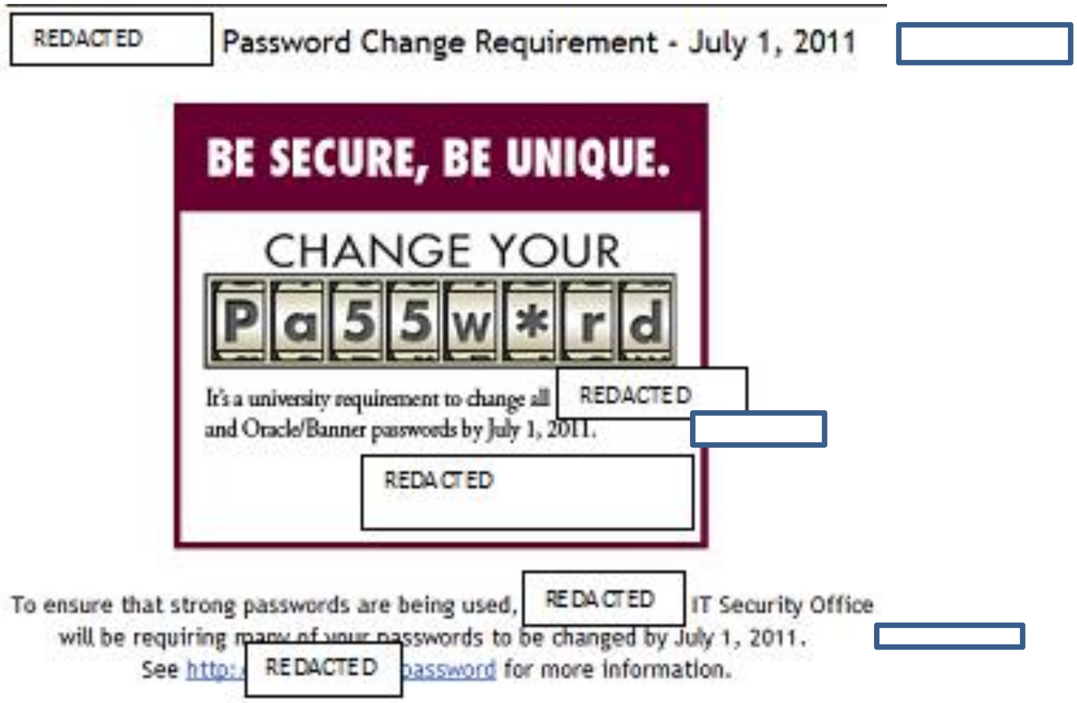


Figure 2. User Change Data Provided by the University IT Office – All Users



REDACTED Password Change Requirement - July 1, 2011

BE SECURE, BE UNIQUE.

CHANGE YOUR Pa55w*rd

It's a university requirement to change all REDACTED and Oracle/Banner passwords by July 1, 2011.

REDACTED

To ensure that strong passwords are being used, REDACTED IT Security Office will be requiring many of your passwords to be changed by July 1, 2011.
See http:/ REDACTED password for more information.

Figure 3. Sample Online Course Management Site Announcement (Anonymized)

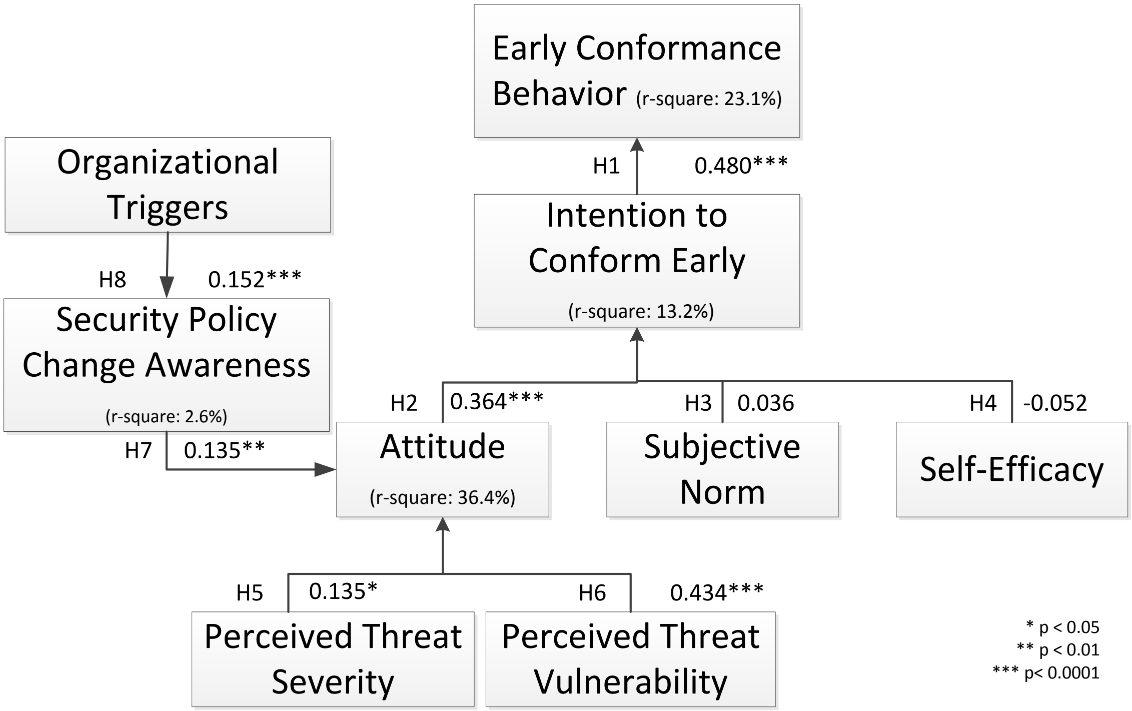


Figure 4. Structural Model Testing

Table 1. Organizational Costs and Benefits of Early, Late, and Nonconformers

Behavior Type	**Definition**	**Costs**	**Benefits**
Early Conformers	Users who proactively conform well in advance of the implementation deadline. Early conformers are less influenced by the timing of the deadline and more influenced by their desire to conform.	• Possible negative reactions if change system not well implemented for early users	• Early problem identification • Individual buy-in into the change process • Avoid overwhelming support staff • May promote awareness of change to others
Late Conformers	Users who procrastinate but ultimately end up conforming at or near the implementation deadline. Late conformers are heavily influenced by a deadline.	• No mechanisms for early problem identification • Can trigger undesired user behaviors • Overwhelms support desk (more personnel needed) if problems occur	• Although late, change minimizes support help if successful • Eventual change as opposed to complete nonconformance • Avoidance of productivity losses
Nonconformers	Users who procrastinate and/or resist and fail to conform prior to the implementation deadline.	• Decreased productivity (users unable to access the system) • Increased support staff workload (help desk) • Decreased moral (user resentment toward the change) • Increased undesired user behaviors (e.g., writing down passwords)	• Can help identify dormant or expired user accounts

Table 2. Sample Distribution by Classification

University Classification	Count	Gender	Count	Ethnicity	Count
Graduate student	247	Female	266	Caucasian	416
Undergraduate student	220	Male	259	Asian	66
Faculty	41	Unreported	10	Hispanic	14
Administrator, staff, employee	14			African American	11
Other/Unreported	13			Other/Unreported	28
Total	**535**		**535**		**535**

Table 3. Early Conformers Ratio per Category of Respondent

Type of User	Early Conformers	Late and Nonconformers	Total	Ratio of Early Conformers (%)
Undergraduate students	15	205	220	6.8
Graduate students	35	212	247	14.2
Faculty	10	31	41	24.4
Administrators	5	9	14	35.7
Unknown	2	11	13	15.4
	67	468	535	12.5

Table 4. Organizational Triggers

Trigger (Seven-point scale)	**% of Total**	**Total**	**Early Conformers**	**Late/Non Conformers**
Online course management site banner	51.2	274	29	245
Survey (this study)	11.9	64	0	63
Friend or colleague	7.5	41	11	30
Articles on the University news website (general new; weekly reminders)	7.5	40	13	27
University newspaper article (print)	3.6	19	1	18
IT Security website (password site)	2.6	14	0	14
Others (table cards, PDF announcements, individual email, etc.)	15.7	84	13	71
Total	**100%**	**535**	**67**	**468**

Table 5. Correlations and Squared Roots of AVEs for Reflective Constructs

Construct	**AW**	**PS**	**PV**	**SSE**	**SN**	**ATT**
Awareness (AW)	**0.894**					
Perceived severity (PS)	0.305	**0.880**				
Perceived vulnerability (PV)	0.325	0.769	**0.861**			
Security self-efficacy (SSE)	0.441	0.223	0.244	**0.772**		
Subjective norm (SN)	0.290	0.372	0.451	0.169	**0.897**	
Attitude (ATT)	0.317	0.510	0.582	0.354	0.518	**0.867**

** Bolded diagonal values are square root of the average variance extracted.