Journal of the Association for Information Systems (2021) **22**(1), 246-272
doi: 10.17705/1jais.00660

RESEARCH ARTICLE

ISSN 1536-9323

Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship

Jeffrey L. Jenkins[1], Alexandra Durcikova,[2] Jay F. Nunamaker, Jr.[3]

[1]Brigham Young University, USA, jjenkins@byu.edu
[2]University of Oklahoma, USA, alex@ou.edu
[3]University of Arizona, USA, jnunamaker@cmi.arizona.edu

Abstract

Although users often express strong positive intentions to follow security policies, these positive intentions fail to consistently translate to behavior. In a security setting, the inconsistency between intentions and behavior—termed the intention-behavior gap—is particularly troublesome, as a single failure to enact positive security intentions may make a system vulnerable. We address a need in security compliance literature to better understand the intention-behavior gap by explaining how an omnipresent competing intention—the user's desire to minimize required effort—negatively moderates the relationship between positive intentions and actual security behavior. Moreover, we posit that this moderating effect is not accounted for in extant theories used to explain behavioral information security, introducing an opportunity to broadly impact information security research to more consistently predict behavior. In three experiments, we found that high levels of required effort negatively moderated users' intentions to follow security policies. Controlling for this moderating effect substantially increased the explained variance in security policy compliance. The results suggest that security researchers should be cognizant of the existence of competing intentions, such as the desire to minimize required effort, which may moderate the security intention-behavior relationship. Otherwise, such competing intentions may cause unexpected inconsistencies between users' intentions to behave securely and their actual security behavior.

Keywords: Security, Intention-Behavior Gap, Effort, Passwords, Information Disclosure, Competing Intentions

France Bélanger was the accepting senior editor. This research article was submitted on May 26, 2017 and underwent five revisions.

1 Introduction

Computer users who are not compliant with security policies pose a serious threat to their organizations (Chang & Seow, 2019). Security breaches caused by a lack of compliance with security policies can create significant upheavals, such as credit card number theft (Kolkowska, Karlsson, & Hedström, 2017; Willey & White, 2019) and government data theft (Abelson et al., 2015). Security breaches can have a negative impact on a firm's financial performance, market value, reputation, and may even lead to government sanctions (Avery & Ranganathan, 2016). The damages from security breaches have been estimated to cost hundreds of thousands or even millions of dollars per incident (IBM, 2019). Despite the potential harm from security breaches, employees' disregard of security policies is prevalent (Balozian & Leidner, 2017).

To help encourage compliance, a rich body of literature has examined how to improve users' intentions to comply with organizations' security policies (Moody, Siponen, & Pahnila, 2018). In general, *intentions*, or the readiness to perform a given behavior, impact behavior in a meaningful way

(Sheeran, 2002); however, in a security setting, positive intentions are frequently inconsistent with actual behavior, which may result in serious security vulnerabilities (Crossler et al., 2014). We suggest that one reason for this inconsistency, termed the *intention-behavior gap* (Sheeran, 2002), is that the user encounters different competing intentions when performing security behaviors—one of which is the user's omnipresent desire to minimize the amount of required effort to complete a task. *Required effort* refers to the actual effort needed to behave securely at the moment a user encounters a security decision. We posit that the effect of required effort on behavior is not currently accounted for in constructs (e.g., perceived behavioral control) included in various prevalent theories used to predict security behavior—such as the theory of planned behavior (Ajzen, 1991), protection motivation theory (Rogers, 1975), or deterrence theory (D'Arcy & Herath, 2011). We leverage Zipf's law (Zipf, 1949) to explain how the desire to reduce required effort moderates the intention-behavior relationship in a security setting. In summary, we address the following research question:

RQ: How does required effort moderate the intention-behavior relationship in the context of users' adherence to security policies?

We performed three experiments in two contexts (password creation and information sharing) to answer our research question. By accounting for the moderating effect of required effort on the intention-behavior relationship, the explained variance in actual behavior often doubled in our experiments, and the effect sizes of adding effort were large, medium, and medium for Experiments 1, 2, and 3, respectively.

Our results indicate that IT security managers and researchers must strive to understand competing intentions in a security context—such as the user's desire to minimize required effort—when implementing security controls. Otherwise, this required effort may decrease the influence of one's positive intentions on behavior, mitigating the effect of various organizational efforts to improve intentions and thereby security policy compliance. Likewise, information security researchers could include required effort as an extension to prevalent security theories to help increase explained variance in behavior and mitigate the intention-behavior gap. Finally, our results suggest a need to examine behavior directly, when possible, in a security context or to provide estimates of required effort to follow a security control rather than to rely only on intentions because required effort may inhibit the impact of intentions on actual behavior.

2 Background and Hypotheses

Intentions are studied as a precursor of behavior. However, there is often an inconsistency between people's intentions and their behavior. In a meta-analysis examining the influence of intentions on behavior (n = 82,107), intentions were shown to account for, on average, 28% of the variance in behavior (Sheeran, 2002). In general, explaining 28% of the variance is often considered good. However, 28% of the variance is short of ideal, especially in a security setting where a single failure to follow a security policy can cause a security risk (e.g., creating a single weak password can make a system vulnerable). Research has shown that although people are concerned about their security and may have good intentions to protect it, they often do not take action to protect their information (Acquisti, 2004).

Much research has examined how to strengthen people's intentions to adhere to security policies (Moody et al., 2018). However, little research in information security has examined why these intentions are often inconsistent with people's security behavior, and most of this research focuses on demographic moderators such as gender (e.g., Anwar et al., 2017). Our paper aims to identify a factor—required effort of a security task—that may explain the intention-behavior gap by both directly influencing behavior and also moderating the intention-behavior relationship. In contrast to demographic-related moderators of the intention-behavior relationship, security administrators have control over many system-design features and security controls that influence required effort. If systems are not properly designed to minimize effort, they may "derail a previously formed intention" (Ortiz de Guinea & Markus, 2009, p. 438).

Despite the dearth of research on the intention-behavior gap in the security discipline, the intention-behavior gap has been studied extensively in psychology and related disciplines (e.g., Gollwitzer, 1999; Pieters & Verplanken, 1995; Schifter & Ajzen, 1985; Sheeran, Norman, & Orbell, 1999; Sutton, McVey, & Glanz, 1999). We leverage and extend this research to mitigate the intention-behavior gap in information security. The literature classifies contributors to the intention-behavior gap roughly into four areas: behavior types, intention type, properties of intentions, and cognitive and personality variables (Sheeran, 2002).

First, *behavior type* can influence how well intentions translate to behavior. Behavior type can be differentiated into either single actions or sustained behaviors/goals (i.e., behaviors that require multiple actions over time). Intentions are more likely to influence behavior for single actions than for goals that require multiple actions (Sheeran, 2002). For example,

it is more likely that intentions will influence the behavior of changing one's password tomorrow (one action) than that of changing one's password every month (multiple actions). Second, the *intention type* can influence how well intentions translate to behavior. Intention type can be differentiated into at least two types: general intentions and implementation intentions (Gollwitzer, 1999). General intentions are measured in the form of "I intend to do X." Implementation intentions are measured in the form of, "I intend to do X, *in situation Y*." For example, a general intention might be, "I intend to change my password" whereas an implementation intention might be, "I intend to change my password every first Monday of the month at 8:00 a.m." People are more likely to behave as intended when specifying implementation intentions than when specifying general intentions (Gollwitzer, 1999; Gollwitzer & Brandstätter, 1997).

Third, the *properties of intentions* may influence how well intentions translate into behavior (Sheeran, 2002). One property of intentions includes *temporal stability*—i.e., the degree to which intentions change prior to performing a behavior (Ajzen, 1985, 1991; Ajzen, Brown, & Carvajal, 2004). Although the moderating influence of temporal stability is debated (e.g., Randall & Wolff, 1994), in general, one should measure intentions as closely as possible to the targeted behavior (Ajzen, 1985). Finally, *cognitive* and other personality *characteristics* may influence how well intentions translate to behavior (Sheeran, 2002). From a cognitive perspective, *conflicting intentions* or multiple conflicting goals may moderate the influence of intentions on behavior because they impede the performance of the focal behavior (Abraham et al., 1999). For example, a user may have intentions to adhere to a security policy but may also have intentions to complete a task as quickly as possible. In such a scenario, one's intentions to complete a task quickly may hinder one's intentions to adhere to the security policy (Abraham et al., 1999).

Although each category is helpful for understanding the intention-behavior gap in security literature, our study particularly contributes to the cognitive characteristics category. Specifically, based on Zipf's law, we identify a salient, albeit often subconscious competing intention that may directly influence behavior and may also moderate the influence of security intentions on behavior: namely, required effort. Zipf's law asserts that people have a desire to minimize required effort and normally choose the path of least resistance or the least required effort (Zipf, 1949). Contrary to the cost-benefit paradigm, which suggests that people consciously assess the anticipated costs and benefits of performing a behavior that shapes their beliefs about the behavior (Hardy, 1982), Zipf's law denotes a primitive, automatic process through which required effort influences behavior at the precise time of the behavior. The principle is based on the premise that humans have limited resources (e.g., time, cognitive effort, abilities, etc.) and naturally choose alternatives that minimize required effort, thereby freeing up resources for other tasks (Case, 2012). This natural tendency to free up resources is almost always present (Zipf, 1949); even if other tasks are not currently competing for resources, humans naturally free resources for future use (Case, 2012; Pashler, 1994).

Literature supports Zipf's law by providing anecdotal evidence that the desire to minimize effort is a competing intention that may impact security. Through interviewing employees from commercial organizations, Adams and Sasse (1999) found that the actual costs (i.e., required effort) and perceived benefits of compliance influence actual compliance with security policies. Similarly, interviews have indicated that increasing required effort by forcing users to frequently change passwords decreases users' motivation to comply with the security policy (Beautement, Sasse, & Wonham, 2008). Further, response costs—or the costs associated with the recommended behavior—have been shown to negatively influence intentions to protect oneself (Herath & Rao, 2009; Lee & Larsen, 2009; Vance, Siponen, & Pahnila, 2012; Workman, Bommer, & Straub, 2008). Perceived barriers, which may include the amount of required effort, may also decrease secure behavior (Ng, Kankanhalli, & Xu, 2009).

In summary, the desire to minimize required effort is an omnipresent, albeit often subconscious intention of users. Intentions can be viewed as someone's self-instructions and motivation to perform a behavior. When actually performing a behavior, people tend to follow their self-instructions to a degree, especially when their motivation is high (i.e., intentions are strong) (Sheeran & Webb, 2016). However, unlike many other intentions, the desire to minimize required effort may not be fully anticipated until one encounters a situation involving high levels of required effort. Sheeran and Webb (2016, p. 503) explain "most behavior is habitual or involves responses that are triggered automatically by situational cues." High required effort is one of those situational cues that can heighten the intention to minimize effort. As such, high levels of required effort will cause people to modify their behaviors to decrease that effort. In summary, we predict:

H1: Required effort negatively influences actual security policy adherence.

In addition to the direct relationship between required effort and compliance behavior, we predict that required effort will also moderate the influence of users' intentions to adhere to a security policy on the

resulting compliance behavior. Moderating effects are common in information systems research. For example, research has studied how IT investment moderates IT returns (Lim, Richardson, & Roberts, 2004), how various factors moderate system success (McKeen, Guimaraes, & Wetherbe, 1994), and even how factors moderate the relationship between intentions and its antecedents (Chen, Ramamurthy, & Wen, 2012). However, very little research has examined what factors moderate the intention-behavior relationship in a security context aside from demographic moderators on self-reported security compliance (Anwar et al., 2017). We extend this research to show that required effort moderates the influence of compliance intentions on security behavior.

Simultaneous competing intentions interact, moderate, and influence each other (Sheeran, 2002). In a security setting, the desire to minimize required effort is shown to be often greater than intentions to achieve an optimal solution (e.g., Bawden & Robinson, 2009; Griffiths & Brophy, 2005). This means that users' natural tendency to minimize required effort may inhibit one from fully enacting positive security intentions because behavior is a function of each competing intention and the relative importance of each intention (Abraham et al., 1999). In a subconscious automatic process, people assess each competing intention and attribute value (or degree of importance) to each intention. In some cases, people may choose a behavior that fulfills all competing intentions. However, in most cases, competing intentions conflict with each other (Abraham et al., 1999; Wigfield & Eccles, 2000). For example, adhering to a security policy and minimizing required effort often conflict with each other (the former often results in additional required effort, while the latter calls for less required effort).

When people have multiple conflicting intentions, the likelihood of any given intention fully translating into behavior decreases, and people engage in an optimization process to maximize overall value. Often, a satisficing approach is taken: people partially implement multiple intentions to maximize value (Simon, 1956). In this case, the relationship between any given intention and behavior weakens. For example, to reduce required effort in a security context, one may sufficiently fulfill both the intention to behave securely and the intention to minimize required effort by adhering to some security policies while ignoring others that have less perceived importance. Thus, in this example, the intention to behave securely would be selectively translated to behavior—i.e., the omnipresent intention to minimize required effort influences how well secure behavior intentions translate to behavior. Furthermore, when effort increases, people generally have a greater desire to decrease effort (i.e., the competing intention to minimize effort becomes more salient) (Zipf, 1949). As such, under circumstances requiring high effort, positive intentions to adhere to the security policy are less likely to translate into behavior than when the required effort is lower. In summary, we hypothesize the following:

H2: Required effort negatively moderates the relationship between the intentions of adhering to a security policy and actual security policy adherence.

Some research suggests that, in prevalent theory, perceived behavioral control (PBC)—i.e., the perceived degree of control a person has over factors that may interfere with the execution of an intended action—entails effort. For example, researchers have described PBC as "people's perception of the ease or difficulty of performing the behavior of interest" (Ajzen, 1991, p. 183), a "person's perception of how easy or difficult it would be to carry out a behavior" (Pavlou & Fygenson, 2006, p. 119), and "a set of control beliefs" (Pavlou & Fygenson, 2006, p. 117). However, all of these definitions refer to a perception or belief of control, while the required (or actual) effort of completing a task is largely ignored in theoretical models. In reality, several factors make it difficult, if not impossible, to accurately perceive or estimate the amount of control and effort required to complete security tasks, meriting separate treatment of PBC and required effort. We summarize these factors next.

First, people are inherently unskilled at estimating their own abilities and the amount of required effort needed to complete a task (Kruger & Dunning, 1999). Hence, users' efforts in a security context are often fraught with failure caused by overestimating abilities and underestimating required effort. Inaccurately estimating abilities and required effort is often caused by people lacking the appropriate expertise or metacognition to assess a scenario. Particularly in a security setting, this is problematic because most computer users are nonexperts who lack even basic privacy and cybersecurity knowledge (e.g., Smith, 2016; Ur et al., 2016; Wash & Rader, 2015). Ur et al. (2015) explained that attaining accurate knowledge of computer security is very hard for everyday users because their decisions can be difficult to execute correctly and the outcomes of their behaviors are not always visible.

Second, when considering the amount of required effort that something might involve, people often underestimate or do not fully anticipate what other competing intentions are present in a security context (e.g., work demands and time pressures). Security is often a secondary task of using computers. In other words, people do not normally use a computer for the sake of being secure. Rather, people use computers to complete their everyday jobs, socialize, and be

entertained. Even when security is a high priority, it often interferes and is interfered with by these other tasks (Jenkins et al., 2016). Normally, people are not aware of demands interfering with each other unless these demands are highly difficult or physically incompatible. Hence, it might seem that only high-cognitive demands decrease security policy adherence; however, studies have demonstrated that the opposite is true. Demands can interfere with each other quite drastically, even when they are neither highly challenging nor physically incompatible (Pashler, 1994). This finding is especially true in a security setting (e.g., Anwar et al., 2017; Bravo-Lillo et al., 2011; Jenkins et al., 2016).

Accurately assessing control and effort is very difficult because users lack security knowledge and often do not anticipate competing demands when performing security behaviors. This difficulty in assessing control and effort exemplifies the need to separately measure required effort and PBC when predicting security behavior. In summary, we predict that required effort is still a meaningful significant factor when predicting behavior, even after controlling for PBC. H3 is summarized below and all the hypotheses are graphically summarized in Figure 1.

H3: After controlling for the effect of PBC on actual security policy adherence, the **(a)** main effect of required effort and **(b)** the moderating effect of required effort on intentions will still be significant predictors of actual security policy adherence.

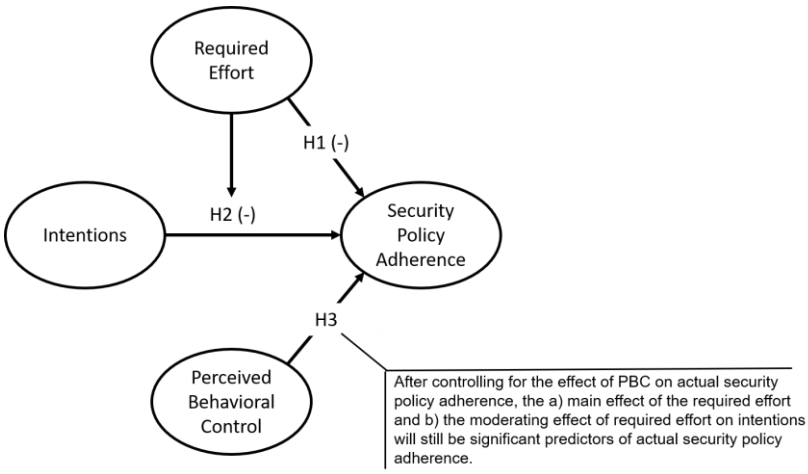

Figure 1. Summary of Hypotheses

3 Methodology

To test our hypotheses, we conducted three experiments. The first two experiments measured users' adherence to a password security policy. In Experiment 1, we manipulated effort using a single sign-on versus a multiple sign-on scenario. In Experiment 2, we manipulated effort using a single-factor authentication versus a multifactor authentication scenario. Experiment 3 measured users' adherence to an information disclosure policy. In this experiment, we manipulated effort by either (1) requiring participants to memorize the information disclosure policy (the high-effort treatment) or (2) using just-in-time information to remind participants about relevant policy information as it was needed (the low-effort treatment). The experiments are described in the following sections.

3.1 Experiment 1

In Experiment 1, we examined the influence of required effort—manipulated as a single sign-on versus a multiple sign-on scenario—on users' compliance with their organizations' password security policy. *Single sign-on* refers to the ability to access all resources in an organization through a single set of credentials (one username and password). *Multiple sign-on* refers to a situation in which each subsystem within an organization requires its own set of credentials. Because multiple sign-on requires users to create several passwords, it requires greater effort.

We designed the experiment so that participants interacted with a typical organizational environment that required them to work with several systems to complete a given task. We asked the participants to act as new employees at a company. Upon arriving at the experiment site, they participated in a new-employee orientation and were introduced to their first task:

completing a financial summary report. All participants watched a training video (a five-minute narrated PowerPoint presentation) that explained the importance of security for the organization and instructed participants on how to create strong passwords. We adapted the training materials for creating passwords based on a password policy from the SANS Institute,[1] a recognized authority on security training and standards. We also provided participants with a written copy of the company's security policy (summarized in Table 1). After they watched the training video and reviewed the security policy (further described in Appendix C), the participants completed a short assessment to determine comprehension and to capture the measures described in Section 3.1.1 of the current paper.

After the new employee orientation, participants began compiling their financial reports by following a printed set of instructions. The task required participants to access several internal systems in the organization (e.g., a Wiki, email, and a document repository). In the single sign-on group, participants created one password for their Windows workstation, which gave them access to all other subsystems. In the multiple sign-on group, users had to create a unique password for each subsystem in the organization, resulting in the need for three different passwords to complete their financial reports. Once participants finished compiling their financial reports, they emailed the reports to their manager. The duration of the entire task was about 30 minutes. The systems captured, anonymized, and automatically analyzed the degree to which users adhered to the password policy by following the procedures described in Section 3.1.2.

3.1.1 Independent Variables

We coded required effort as a binary variable based on the treatment group ("1" for the high-required effort treatment group and "0" for the low-required effort treatment group). We measured intentions and PBC (as a control variable) through a pre-survey that used validated instruments in an information-systems context originally from Ajzen (1991) and further refined by Taylor and Todd (1995) and Bulgurcu, Cavusoglu, and Benbasat (2010). Prior to answering these items, participants again reviewed the security policy. Appendix A lists the instruments. We adapted the measures specifically to our context, as recommended by D'Arcy and Herath (2011) and measurement and security experts reviewed them to ensure face and content validity. Furthermore, we tested the items in a pilot study and we made minor adjustments to improve clarity. We also collected several other control variables that represent the salient differences among the participants, including age, gender, years of education, nationality, and major.

3.1.2 Dependent Variable

The dependent variable we used was compliance with the password policy. The security policy contained five criteria for strong passwords. For each criterion, users received a score that ranged between 0 and 1, with a score of 5 indicating total compliance across the five criteria (see Table 1). The score for the single sign-on group was the score for the single password created. The score for the multiple sign-on group was the average score for the three different passwords created.

Table 1. Scoring Criteria for Compliance with Security Policy

#	Criteria	Score
1	Passwords should contain at least 15 characters.	$\frac{\#\ of\ characters\ in\ password}{15} = 0 \ldots 1$
2	Passwords should contain both upper- and lowercase letters.	1 if password contains upper- and lowercase letters; 0 if it does not
3	Passwords should contain at least one special character.	1 if password contains at least one special character; 0 if it does not
4	Passwords should contain at least one number.	1 if password contains at least one number; 0 if it does not
5	Passwords should not contain words found in a dictionary.	1 if password does not contain words found in a dictionary; 0 if it does We used the following dictionaries: English, Spanish, French, German, Russian, Urban, Common Names, Movie Characters
	Total possible score	**5**

[1] https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

3.1.3 Participants

We recruited students to participate in the experiment and offered extra credit for participating in the study. A total of 86 students (60% male) participated in Experiment 1. The three most represented majors were management information systems (MIS) (56%), MIS/operations management (17%), and pre-business (15%). Approximately 58% of participants were 18-22 years old. The two most represented nationalities were American (64%) and Chinese (13%). Six of the participants did not pass the security policy comprehension assessment and were removed from the dataset, resulting in 80 usable data points.

3.1.4 Data Analysis and Results

Prior to our analysis, we assessed the validity and reliability of the instruments, which are reported in Appendix B. PBC and intentions served as reflective measures; therefore, we validated the convergent and discriminant validity and reliability of the measurement scales through a factor analysis as well as through construct correlations and cross-correlations for both experiments. All the loadings for each item on its latent construct exceeded 0.6. The average variance extracted from all constructs was much larger than 0.5; therefore, good convergent validity was demonstrated (Anderson & Gerbing, 1988). In addition, all square roots of the average variance extracted exceeded the correlation coefficients between constructs, thereby demonstrating good discriminant validity (Fornell & Larcker, 1981). Correlations among the independent variables were less than 0.65 (Billings & Wroten, 1978), and the VIF was below 5 (Kutner, Nachtsheim, & Neter, 2004); hence, multicollinearity was not deemed to be a problem. Finally, all of the Cronbach's alpha scores were above 0.7, suggesting good internal consistency (Billings & Wroten, 1978).

Next, we performed a manipulation check on our treatment using a self-reported measure of effort that was collected in the post-survey (measure adapted from Wang & Benbasat, 2009). We conducted an independent sample *t*-test to verify that the two different conditions successfully manipulated effort. We found that the high-required effort group (the multiple sign-on group) reported significantly higher effort than the low-required effort group: $t(73.402) = 3.362$, $p < 0.01$. Table 2 displays the means and standard deviations for compliance and self-reported effort for each treatment.

The next step was a regression analysis. First, we specified a model with all independent, dependent, and control variables. Required effort was included as a factor of whether someone had multiple sign-on or a single sign-on. None of the control variables were significant ($p > 0.05$ for all paths from the control variables to compliance). Therefore, we specified a second model, omitting the control variables (Kenny, 2011) other than PBC so that we could test H3. Table 3 shows the results of the regression and Figure 2 summarizes them. For comparison, we also specified a competing model without the effect of required effort. Table 4 displays the *R*-squared for our hypothesized model and the competing model. We conducted a Wald test to examine whether the hypothesized model explained more variance than the competing model. The test indicated a significant difference between the two models: $\chi^2(2) = 94.74$, $p < 0.0001$.

The significant interactions are plotted in Figure 3. This graph displays the compliance with the security policy at each intention level for both the high-required effort treatment and the low-required effort treatment with error bars. As the graph shows, people in the high-required effort treatment displayed lower compliance as intentions increased.

Table 2. Experiment 1 Password Compliance Means and Standard Deviations

Group	# of participants	Compliance mean (*sd*)	Self-reported effort (*sd*)
Multiple sign-on (high required effort)	42	1.701 (1.091)	5.645 (0.880)
Single sign-on (low required effort)	38	3.361 (0.721)	4.833 (1.262)

Table 3. Experiment 1 Regression Analysis Results

	Estimate	*SE*	*T*-Value	*P*-Value
(Intercept)	(1.374)	0.855	(1.608)	0.112
Perceived behavioral control	0.085	0.071	1.200	0.234
Intentions	0.743	0.143	5.208	0.000
Required effort	1.148	0.986	1.164	0.248
Required effort*Intentions	(0.478)	0.170	(2.811)	0.006
Note: Adjusted *R*-squared: 0.625				

Table 4. Experiment 1 Model *R*-Squared

	Proposed model	**Model without required effort**	**Effect size of adding required effort relationships***
Adjusted *R*-squared compliance	0.625	0.374	0.669 (large)

Note: * Effect size (f^2) is calculated by the formula ($R^2_{full} - R^2_{partial}$) / ($1 - R^2_{full}$). Cohen (1988) suggested 0.02, 0.15, and 0.35 as operational definitions of small, medium, and large effect sizes, respectively.

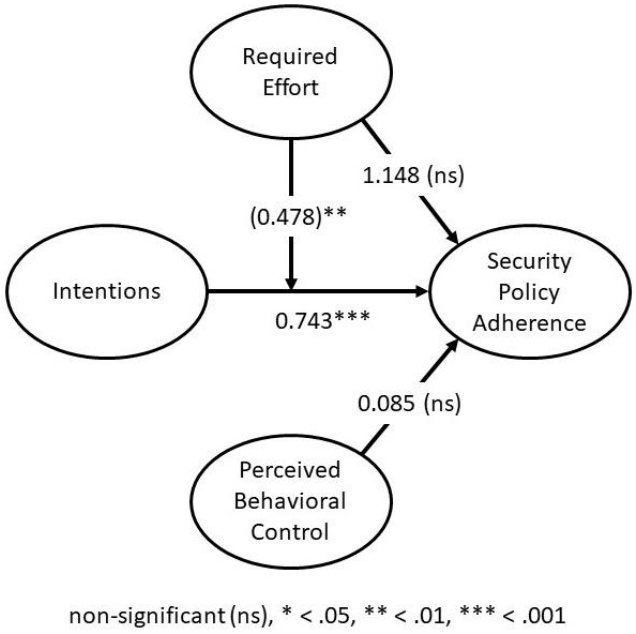

Figure 2. Experiment 1 Summary Model Results

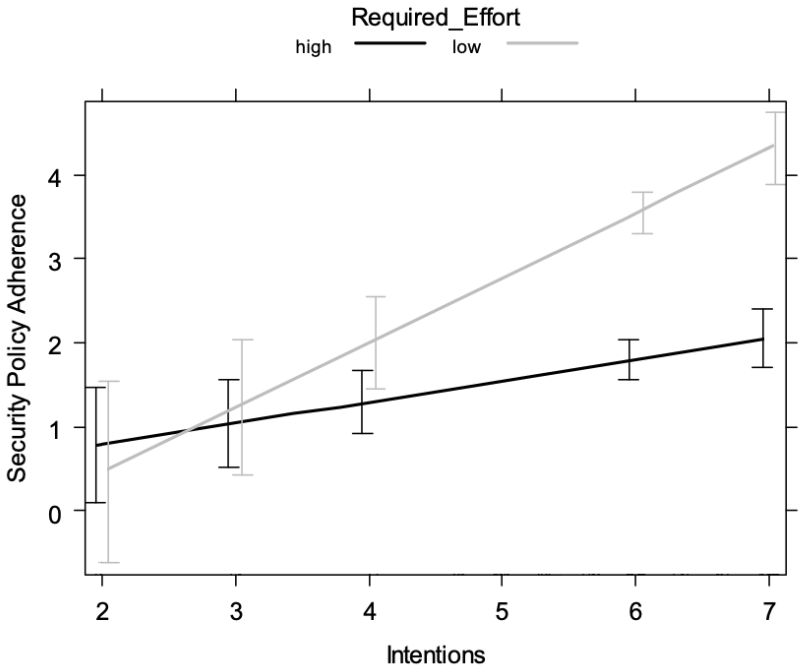

Figure 3. Experiment 1 Interaction Plot

3.2 Experiment 2 Task and Procedure

To increase the generalizability to other authentication contexts, Experiment 2 manipulated required effort through single- versus multifactor authentication. In Experiment 2, participants were asked to engage in a consulting task for an e-commerce organization. All participants watched a training video (the same five-minute narrated PowerPoint presentation as in Experiment 1 [see Appendix C], which was viewed 0-26 days prior to the experiment) that explained the importance of security for the organization and taught participants how to create strong passwords. Participants were also given a written copy of the company's security policy (see Table 1 for a summary). After they watched the training video and reviewed the security policy, the participants were required to complete a short assessment to determine comprehension and to measure intentions, PBC, and required effort, which are outlined in Section 3.2.1. Then, we asked participants to schedule a session in the computer lab to complete their consulting tasks, which involved assessing online inventory and ordering supplies for the company through an online vendor. The entire task lasted approximately 45 minutes.

Upon arriving at the computer lab, participants were randomly assigned to either a single-factor authentication treatment or a multifactor authentication treatment. During the task, participants were required to create an account at a vendor's website and then order new inventory. The single-factor authentication treatment allowed users to create one username and password to access the vendor website; however, the multifactor authentication treatment required participants to configure a token and then create a password. In the first step, users had to configure their token for the authentication context. This included entering at least two of the token's codes on a configuration page (the code changed every 60 seconds) and then saving backup codes. In the second step, users had to create a password to accompany the token. Each time they logged into the vendor's website thereafter (which users had to do multiple times during the experiment regardless of their treatment group), they entered both their password and a PIN number from the token. The PIN number changed every 60 seconds and was synchronized with the vendor's website. Because the multifactor authentication treatment required an extra step to create passwords and authenticate, it required greater effort.

3.2.1 Independent Variables

Required effort was coded as a binary variable in the model based on the treatment group ("1" for the high-required effort treatment group and "0" for the low-required effort treatment group). The same instruments from Experiment 1 were used to measure intentions, PBC, and the other control variables. We also controlled for the length between participants' security training and the actual experiment, which was a duration of 0-26 days.

3.2.2 Dependent Variable

Because the participants in both treatments created their own passwords, password information was extracted and anonymized to protect user privacy. Compliance with the security policy was calculated using the same procedure outlined in Experiment 1.

3.2.3 Participants

A total of 157 subjects participated in the experiment. Students from a large US public university were recruited to complete the experiment for class credit. The students averaged 3.8 years of college education, 54% of the participants were male, and the average age was 23. The four most represented majors for the participants were accounting (15%), management information systems (15%), marketing (13%), and finance (11%); 61% of the participants were American, 12% Indian, 8% Mexican, 8% Chinese, and 11% other. Ten of the participants did not pass the security policy comprehension assessment and were removed from the dataset, resulting in 147 usable data points.

3.2.4 Data Analysis and Results

Consistent with Experiment 1, we assessed the validity and reliability of our survey measures and found them to be both valid and reliable (see Appendix B). Again, to ensure that the treatments achieved their desired effects, we conducted manipulation checks. All participants rated the perceived effort of authenticating during the post-survey (measure adapted from Wang & Benbasat, 2009). Participants in the multifactor treatment ranked the self-reported effort significantly higher than participants in the single-factor treatment: $t(138) = 3.092$, $p < 0.01$. Table 5 displays the means and standard deviations for compliance for each group.

Next, we conducted a regression analysis to test our hypotheses. We specified a model with all independent, dependent, and control variables. Required effort was included as a factor whether participants used multiple-factor authentication or single-factor authentication. Like in Experiment 1, none of the control variables were found to be significant ($p > 0.05$ for all paths from the control variables to compliance), except for the length of time between participants' security training and the actual experiment. Therefore, we specified a second model, omitting all the control variables except for days since training and PBC so that we could test H3. Table 6 and Figure 4 show the results of this model. For comparison, we also specified a competing model without required effort included. Table 7 displays the

R-squared for our hypothesized model and the competing model. We conducted a Wald test to examine whether the hypothesized model explained more variance than the competing model. The test indicated a significant difference between the two models: $\chi^2(2) = 43.524$, $p < 0.0001$

The significant interactions are plotted in Figure 5. This graph displays compliance with the security policy at each intention level for both the high-required effort treatment and the low-required effort treatment using error bars. As shown by the graph, individuals in the high-required effort treatment group displayed lower compliance as intentions increased.

Table 5. Experiment 2 Password Compliance Means and Standard Deviations

Group	# of participants	Compliance mean (sd)	Self-reported effort (sd)
Multifactor authentication (high required effort)	74	2.775 (0.744)	5.710 (0.907)
Single-factor authentication (low required effort)	73	3.603 (0.799	5.180 (1.157)

Table 6. Experiment 2 Regression Analysis Results

	Estimate	*SE*	*T*-Value	*P*-Value
(Intercept)	1.609	0.562	2.865	0.005
Days since training	(0.032)	0.008	(3.998)	0.000
Perceived behavioral control	(0.021)	0.057	(0.374)	0.709
Intentions	0.402	0.094	4.290	0.000
Required effort	1.120	0.611	1.834	0.069
Intentions*Required effort	(0.317)	0.105	(3.015)	0.003
Note: Adjusted *R*-squared: 0.379				

Table 7. Experiment 2 Model *R*-Squared

	Proposed Model	Model without Required effort	Effect size of adding required effort relationships*
Adjusted R-squared compliance	**0.379**	0.178	0.324 (medium)
Note: * Effect size (f^2) is calculated by the formula ($R^2_{full} - R^2_{partial}$) / ($1 - R^2_{full}$). Cohen (1988) suggested 0.02, 0.15, and 0.35 as operational definitions of small, medium, and large effect sizes, respectively.			

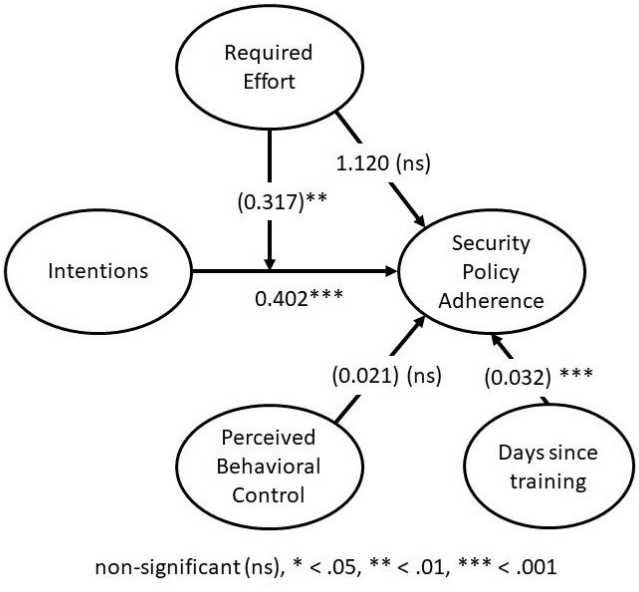

Figure 4. Experiment 2 Summary Model Results

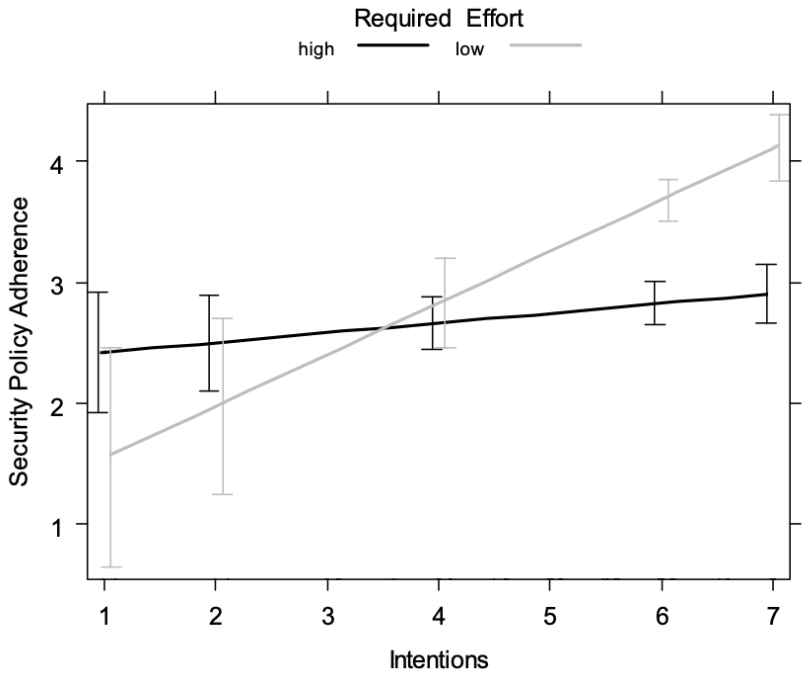

Figure 5. Experiment 2 Interaction Plot

3.3 Experiment 3 Task and Procedure

The purpose of Experiment 3 was to determine whether the results of the prior experiments could be generalized to a context outside of password compliance—namely users' compliance with the organization's information disclosure policy. Participants were told that they were completing a remote consulting project for clients. They could complete the task on their own time and on their own computers. The entire task required approximately 30 minutes.

In the experiment, each participant consulted for a client and was required to adhere to an information disclosure policy from the client. All participants were given the policy at the beginning of the study and were asked to report their intentions and PBC regarding adherence to the policy. The policy explained why information disclosure about clients was prohibited, what their responsibility was to protect client information, and why they should never disclose client information (e.g., names, contact information, etc.) to third parties (see Appendix C). Required effort was manipulated by either (1) requiring participants to memorize the information policy at that time (the high-required effort treatment) or (2) using just-in-time prompts during the experiment to remind participants about relevant policy information as it was needed (the low-required effort treatment). The participants were then given a short quiz on the material to ensure comprehension and were then allowed to download a copy of the policy for future reference.

After receiving the information disclosure policy, participants were given their first consulting task: to evaluate and recommend a printer for their client. They were given instructions regarding how to evaluate printers and to make a recommendation for their client. All participants were then given the contact information about their first client (e.g., name, phone number, contact person, etc.) and instructed to complete the task.

During one part of the task, participants visited two printer vendor websites to complete their evaluations. Both websites were created by the research team but participants were unaware of this. If the participants were in the low-required effort condition, they were shown a prompt just before visiting each vendors' website, reminding them to not disclose information about clients to third parties. Participants in the high-required effort condition did not receive this prompt. On each website, the users interacted with a sales representative using a chat window to obtain information about the printer (e.g., price, service options). Unbeknownst to the participants, the sales representative was an automated bot. The bot first asked participants: "Hi, my name is Kelly. What product would you like information for?" After the participants entered the product description, the sales representative asked: "I would be happy to help. First, may I ask who you are buying the printer for?" Irrespective of the participants' answers to this question, the sales representative then provided them with the printer information they requested. Participants' interactions with the sales representative were logged and,

afterward, two research assistants manually reviewed each interaction to determine whether client information was disclosed. Given the simplicity of the coding, we observed no discrepancies in coding.

3.3.1 Independent Variables

Required effort was coded as a binary variable in the model based on the treatment group ("1" for the high-required effort treatment group and "0" for the low-required effort treatment group). When participants were shown the information on the disclosure policy, they also reported their PBC and intentions (as a control variable) to obey the information disclosure policy (see Appendix A for instruments). We also captured additional control variables related to participant demographics as done in Experiment 1.

3.3.2 Dependent Variable

Security policy adherence was operationalized as unauthorized information disclosure—that is, whether participants disclosed sensitive client information. Information disclosure was coded as "1" if participants disclosed sensitive information to the automated chatbot and "0" if they did not.

3.3.3 Participants

A total of 156 students participated in the experiment and were given extra credit for participating. The four most represented majors for participants were accounting (11%), energy management (8%), finance (7%), and marketing (6%). The average age of participants was 22, 63% of the participants were male, and participants had an average of 2.2 years of higher education. Nationalities represented were 80% American, 4% Mexican, and 16% other. All participants passed the security policy comprehension assessment.

3.3.4 Data Analysis and Results

Consistent with Experiments 1 and 2, we assessed the validity and reliability of our survey measures and found them to be both valid and reliable (see Appendix B). Again, to ensure that the treatments achieved their desired effects, we conducted manipulation checks. During the post-survey, all participants ranked their self-reported effort of adhering to the security policy during the post-survey (measure adapted from Wang & Benbasat, 2009). Participants in the just-in-time reminder treatment ranked their self-reported effort significantly lower than participants in the no just-in-time reminders treatment: $t(128.85) = 2.210$, $p < 0.05$. See Table 8 for a summary of the statistics.

Next, we conducted a logistic regression analysis to test our hypotheses. First, we specified a model with all independent, dependent, and control variables. Required effort was included as a factor indicating whether a participant had a reminder or did not have a reminder and had to memorize the policy. As in the previous experiments, none of the control variables were found to be significant ($p > 0.05$ for all paths from the control variables to compliance). Therefore, we specified a second model, omitting all of the control variables except for *PBC* so that we could test H3. Table 9 and Figure 6 show the results of this model. For comparison, we also specified a competing model without the effect of required effort. Table 10 displays the *R*-squared for our hypothesized model and the competing model. We conducted a Wald test to examine whether the hypothesized model explained more variance than the competing model. The test indicated a significant difference between the two models: $\chi^2(2) = 24.115$, $p < 0.0001$.

The significant interactions are plotted in Figure 7. This graph displays the compliance with the information disclosure policy at each intention level for both the high-required effort treatment and the low-required effort treatment using error bars. As the graph shows, individuals in the high-required effort treatment group displayed lower compliance as intentions increased.

Table 8. Experiment 3 Disclosure Compliance Means and Standard Deviations

Group	# of participants	# compliant (percentage)	Self-reported required effort (sd)
No just-in-time reminders (high required effort)	77	40 (50.649%)	5.300 (0.863)
Just-in-time reminders (low required effort)	79	71 (89.873%)	4.898 (1.347)

Table 9. Experiment 3 Logistic Regression Analysis Results

	Estimate	*SE*	*T*-Value	*P*-Value
(Intercept)	(4.488)	2.069	(2.169)	0.030
Perceived behavioral control	0.420	0.244	1.720	0.085
Intentions	0.712	0.295	2.414	0.016
Required effort	2.462	2.357	1.045	0.296
Required effort*Intentions	(0.794)	0.394	(2.017)	0.043
Note: Pseudo *R*-squared: 0.254				

Table 10. Experiment 3 Model Fit Indices

	Proposed Model	Model without Effect	Effect size of adding required effort relationships*
Pseudo *R*-squared compliance	0.254	0.072	0.244 (medium)

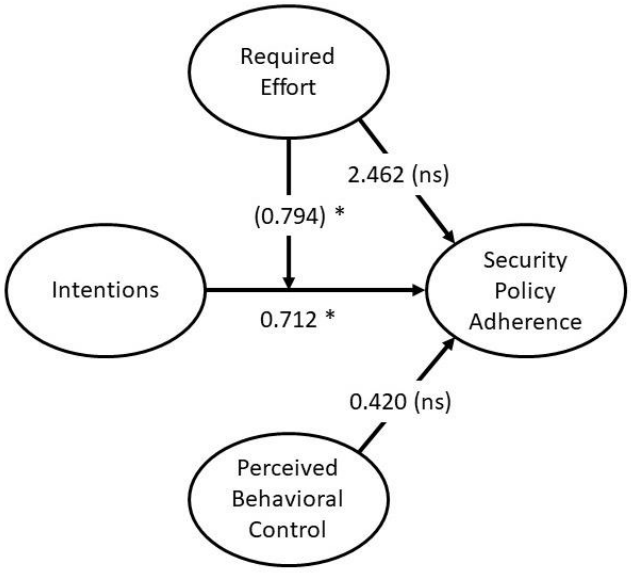

Figure 6. Experiment 3 Summary Model Results

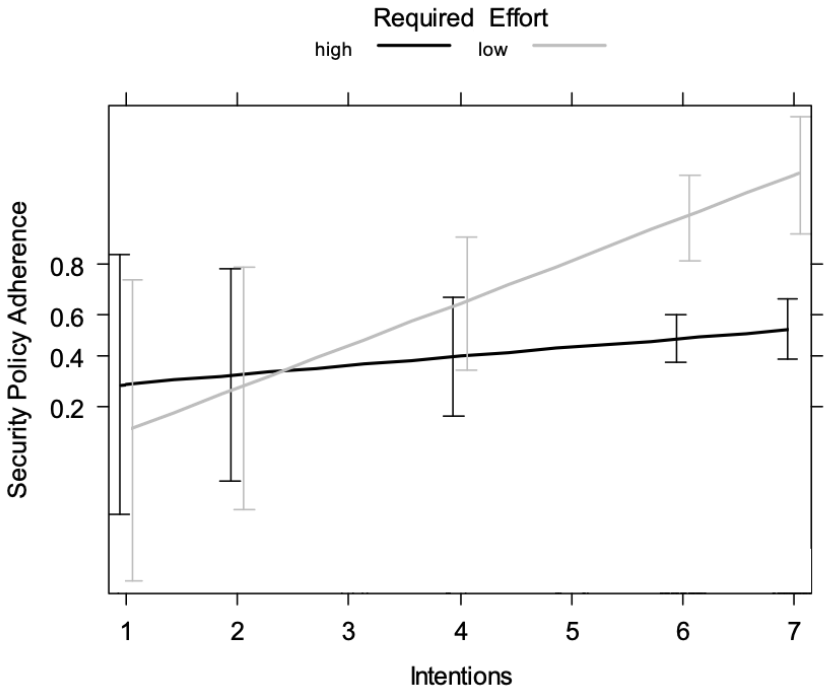

Figure 7. Experiment 3 Interaction Plot

Table 11. Summary of Results

Hypothesis	Experiment 1	Experiment 2	Experiment 3
H1: Required effort negatively influences actual security policy adherence.	Not supported	Not supported	Not supported
H2: Required effort negatively moderates the relationship between the intentions of adhering to a security policy and actual security policy adherence.	Supported	Supported	Supported
H3a: After controlling for the effect of PBC on actual security policy adherence, the main effect of required effort will still be a significant predictor of actual security policy adherence.	Not supported	Not supported	Not supported
H3b: After controlling for the effect of PBC on actual security policy adherence, the moderating effect of required effort on intentions will still be a significant predictor of actual security policy adherence.	Supported	Supported	Supported

4 Discussion

The purpose of the current research was to investigate how required effort moderates the intention-behavior relationship in the context of users' adherence to security policies. We developed hypotheses based on Zipf's law, asserting that users have a competing intention to minimize effort, and then tested them in three experiments. The results of the three experiments confirm that intentions influence behavior. Although required effort does not significantly influence behavior directly (H1 was not supported), it negatively moderates the influence of intentions on behavior (H2 was supported). In addition, after controlling for the effect of PBC on actual security policy adherence, the moderating effect of required effort on intentions was a strong predictor of actual security policy adherence (H3a was not supported, but H3b was supported). The nonsignificant effect of effort directly on behavior (H1 and H3a) should be interpreted within the context of the moderating effect; effort significantly moderated the influence of intentions on behavior and, through this mechanism, influenced behavior. The results of the hypotheses in all three experiments are summarized in Table 11. In the following sections, we discuss the implications of these results for research and practice.

4.1 Implications for Research

This research provides several novel insights into the intention-behavior gap in the context of users' adherence to security policies. Given the importance of positive intentions translating to security compliance, it is critical that research looks beyond predicting intentions to better understand behavior and, specifically, what factors influence whether intentions predict security compliance. We address this gap in the literature by extending theory in psychology on the intention-behavior gap and Zipf's law to theoretically and empirically show how required effort moderates the relationship between intentions and behavior. Also, we contribute to the broader intention-behavior gap literature by identifying a salient competing intention in the security context: namely, required effort.

Importantly, our findings have broad impacts on understanding security compliance. The use of intentions to understand security compliance is prevalent in theory and literature. Intentions are used as a dependent variable in many behavioral theories utilized in security research, including but not limited to the theory of planned behavior (Ajzen, 1991), protection motivation theory (Rogers, 1975), and several variants of deterrence theory (D'Arcy & Herath, 2011). Our research potentially extends all of these different theories in a security context. Namely, relevant to all of these theories, we show that the influence of required effort is not captured in people's intentions to adhere to security policies. Rather, the amount of required effort negatively moderates the influence of intentions on behavior and can be included in these various theories to improve consistency between intentions and behavior. The effect of required effort is distinct from competing constructs such as PBC. As a result, even when people know of a given security control and have good intentions of adhering to best security practices related to the control, their actual behavior may deviate from their intentions due to their innate desire to minimize effort.

One important implication of our findings is that they suggest that researchers should consider competing intentions, where possible, to better understand security behaviors. In our study, in addition to measuring participants' intentions to adhere to a security policy, we measured actual effort as a surrogate for an omnipresent competing intention to minimize effort in a security context. By accounting for the moderating effect of effort on adherence intentions, the *R*-squared increased from 0.374 to

0.625 (an increase of 0.251, or 67%) in Experiment 1. Furthermore, security compliance decreased by approximately 49% (from 3.361 to 1.701) when the required effort was higher. Likewise, in Experiment 2, the *R*-squared increased from 0.178 to 0.379 (an increase of 0.201, or 113%). In this experiment, security compliance decreased by approximately 23% when the required effort was higher (from 3.603 to 2.775). In Experiment 3, the *R*-squared increased from 0.072 to 0.254 (an increase of 0.182, or 253%). Despite these encouraging results, the majority of theories utilized in behavioral information security measure a *single* intention when trying to predict an outcome. Our results suggest that when trying to understand a behavioral phenomenon, it would be helpful to identify and account for various competing intentions to predict security-related behavior. Also, given that our experiment had only two levels of effort (high and low), future research should investigate whether there are any breakpoints or, potentially, a curvilinear relationship between security compliance and required effort.

We recommend that future research identify which other competing intentions (conscious or subconscious) may also moderate the intention-behavior relationship in security settings—e.g., the intention to complete a task quickly, turnover intention, or intention to help a colleague. Karjalainen, Sarker, and Siponen (2019) have argued that competing intentions (labeled as tensions) can stem from four different areas: environmental confidence (openness/trust vs. suspicion), level of goals and interests prioritized (individual vs. institutional), motivational drivers (instrumental vs. socioemotional), and time horizon (immediate vs. long-term focus). We empirically examined a variable in one of these areas (level of goals and interests prioritized) and found that it had a significant impact on security policy compliance. Future research should empirically investigate variables in these other areas to identify the relevant competing intentions that may affect security policy compliance and thus better predict actual security behavior.

Our empirical findings provide some interesting observations regarding how effort moderates intentions. Specifically, the main effect of required effort was not significant in any of the experiments; only the interaction was significant. Upon examination of the interaction plots for each experiment (Figure 3, Figure 5, and Figure 7), it became clear that effort had the largest effect on people with positive intentions, whereas individuals with lower intentions were not influenced to the same degree. Future research is needed to better understand this. One potential explanation supported by our results is that people with low intentions anticipate the extra work of adhering to the security policy and thus admit they do not intend to strictly follow it, whereas people with high intentions have a positively biased view of security compliance and do not consider other side effects of behaving securely when reporting intentions (e.g., required effort). In a future study, researchers could confirm whether this is the case by explaining the pros and cons (e.g., effort) of adhering to security policies prior to asking people about their intentions; researchers could then determine whether reported intentions were better aligned with behavior.

Finally, we stress the need for researchers to measure actual security behavior when possible because measuring intentions to behave securely may not adequately predict actual security behavior in the presence of other competing intentions. Consistent with much past research, the results of our controlled studies support that intentions generally improve behavior (e.g., Shropshire, Warkentin, & Sharma, 2015). However, even in our studies, intentions alone were far from a perfect predictor of security behavior. Thus, we echo the observations in non-controlled settings that attitudes and intentions are often inconsistent with behavior (Acquisti, 2004). Hence, measuring behavior directly is often desirable in order to understand the state of security in an organization. The need to measure actual security behavior is valid even in scenarios where users are quite familiar with the security behavior in question. For example, both of our studies were conducted using very common scenarios—password creation and information disclosure. It is likely that every participant had prior experience creating passwords and keeping information confidential (Kaur & Mustafa, 2019). Despite people's familiarity with these two tasks, intentions alone only predicted a minority of variance in behavior. Hence, for many security scenarios, relying on intentions alone to understand behavior is likely inadequate. Rather, a measure of actual behavior is often needed in addition to a measure of intentions.

4.2 Implications for Practice

Practitioners as well as researchers frequently consider users to be the weakest link in security (e.g., Boss et al., 2009). Security managers often attempt to strengthen this weakest link by implementing a variety of security controls. In the current study, we investigated three frequently applied security controls. We found that if companies try to solve the "weakest link" problem by using controls that have high levels of required effort, they may actually weaken the weakest link rather than strengthen it. Our results indicate that even employees who have positive intentions toward behaving securely do not always act on these beliefs due to burdensome technology policies or mechanisms. Thus, IT security managers should carefully consider the proposed benefits of security

controls and the potential side effects caused by high levels of required effort.

Our research has shown that there is a differential effect of required effort, in addition to self-reported PBC, that a user can express via a survey. We suggest that although employees are likely not skilled at estimating their behavioral control for a security task, the required effort it takes to perform a task can be roughly estimated and thus can be much better managed. At a minimum, one could perform a comparative analysis that indicates which controls require more effort than other controls if a precise estimate of required effort is not available. The role of the actual measurement of required effort cannot be underestimated because this required effort moderates the relationship between end users' intentions to behave securely and their actual behavior.

4.3 Limitations

Our research is subject to several limitations. First, Experiments 1 and 2 studied adherence to password policies without technology enforcement of the password policies. This might have created an environment that does not mimic best practices for password policy enforcement; however, current industry research has shown that although most organizations have password policies, half of them do not enforce them (Henderson, 2017). According to OneLogin, less than half (49%) of respondents required their internal users to follow a basic password complexity policy (Henderson, 2017). To minimize this potential limitation, we also performed an experiment using a different type of security policy adherence, namely information disclosure. We found that our results were consistent across these two security policy types and thus believe that this limitation did not significantly influence the validity of Experiments 1 and 2. We recommend that future research explore the scope of the current study's generalizability (e.g., backing up data, installing virus protection software, etc.).

Second, we employed an experimental design. When a balance between generalizability, realism, and precision is required, it is not possible to maximize one without compromising the other two (McGrath, 1981). In the context of laboratory experiments, precision is strong, but the experiments may often lack generalizability and realism. Field studies tend to maximize realism at the expense of generalizability and precision. Thus, "no one method is better or worse than any other; they are simply better at some aspects and worse at others" (Dennis & Valacich, 2001, p. 5). To accomplish the objective of the current study—to understand the moderating influence of required effort on the relationship between intentions and security policy adherence—precision and a laboratory experiment were arguably the most appropriate methodologies for an initial investigation; however, we suggest that future research improve the realism factor by testing our hypotheses in a field study.

Finally, the results of the present study are only generalizable to college-age student samples. Although student subjects are often viewed as an accurate representation of newly hired employees (Greenburg, 1987), a more diverse sample that includes industry professionals should be used to allow generalization to a larger population of new employees.

5 Conclusion

The objective of the current paper was to explore the intention-behavior gap in the context of users' adherence to security policies—specifically, how required effort moderates the relationship between intentions and actual security behavior. Based on Zipf's law, we contribute to the literature by explaining how users' desires to minimize required effort is a salient competing intention in a security setting and by empirically testing how required effort moderates the influence of intentions on actual security policy adherence. Our results indicate that required effort is a very meaningful moderator of the intention-behavior relationship in a security setting, and practitioners should carefully consider the trade-off between increased control and high levels of required effort. Failure to do so has the potential to make the weakest link in an organization's tech-security realm even weaker.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Neumann, P. G. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69-79.

Abraham, C., Sheeran, P., Norman, P., Conner, M., Otten, W., & de Vries, N. (1999). When good intentions are not enough: Modeling post-intention cognitive correlates of condom use. *Journal of Applied Social Psychology*, *29*(12), 2591-2612.

Acquisti, G. (2004). Privacy attitudes and privacy behavior. *Economics of Information Security*, *12*(1), 165-178.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action-Control: From Cognition to Behavior* (pp. 11-39). Heidelberg: Springer.

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

Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, *30*(9), 1108-1121.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411-423.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*(4), 437-443.

Avery, A., & Ranganathan, C. (2016). *Financial performance impacts of information security breaches.* Paper presented at the Pre-ICIS Workshop on Information Security and Privacy.

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 11-43.

Bawden, D., & Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*, *35*(2), 180-191.

Beautement, A., Sasse, M. A., & Wonham, M. (2008)). *The compliance budget: Managing security behaviour in organisations.* Paper presented at the Workshop on New Security Paradigms.

Billings, R. S., & Wroten, S. P. (1978). Use of path analysis in industrial/organizational psychology: Criticisms and suggestions. *Journal of Applied Psychology*, *63*(3), 677-688.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Bravo-Lillo, C., Cranor, L. F., Downs, J., Komanduri, S., & Sleeper, M. (2011). *Improving computer security dialogs.* Paper presented at the 13th IFIP TC 13 International Conference on Human-Computer Interaction, Lisbon, Portugal.

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

Case, D. (2012). *Looking for information: A survey of research on information seeking, needs and behavior* (3rd ed.). Emerald Group Publishing.

Chang, K.-C., & Seow, Y. M. (2019). Protective measures and security policy non-compliance intention: IT vision conflict as a moderator. *Journal of Organizational and End User Computing*, *31*(1), 1-21.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209-226.

D'Arcy, J., & Herath, T. (2011). A Review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

Dennis, A. R., & Valacich, J. S. (2001). Conducting experimental research in information systems.

Communications of Association for information systems, 7, Article 5.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist, 54*(7), 493-503.

Gollwitzer, P. M., & Brandstätter, V. (1997). Implementation intentions and effective goal pursuit. *Journal of Personality and Social Psychology, 73*(1), 186-199.

Greenburg, J. (1987). The college sophomore as a guinea pig: Setting the record straight. *Academy of Management Review, 12*(1), 157-159.

Griffiths, J. R., & Brophy, P. (2005). Student searching behavior and the web: Use of academic resources and Google. *Library Trends, 53*(4), 539-554.

Hardy, A. P. (1982). The selection of channels when seeking information: Cost/benefit vs. least-effort. *Information Processing & Management, 18*(6), 289-293.

Henderson, N. (2017). Most organizations have password policies, but half don't enforce them. http://www.itprotoday.com/identity-access-management/most-organizations-have-password-policies-half-dont-enforce-them

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

IBM. (2019). Cost of a data breach study by Ponemon. https://www.ibm.com/security/data-breach

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More harm than good? How messages that interrupt can make us vulnerable. *Information Systems Research, 27*(4), 880-896.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research, 30*(2), 687-704.

Kaur, A. A., & Mustafa, K. K. (2019). A critical appraisal on password based authentication. *International Journal of Computer Network and Information Security, 11*(1), 47-61.

Kenny, D. (2011). Path analysis. http://davidakenny.net/cm/pathanal.htm

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *The Journal of Strategic Information Systems, 26*(1), 39-57.

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology, 77*(6), 1121-1134.

Kutner, M. H., Nachtsheim, C. J., & Neter, J. (2004). *Applied linear regression models* (4th ed.). McGraw-Hill.

Lee, Y., & 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), 177-187.

Lim, J., Richardson, V. J., & Roberts, T. L. (2004). *Information technology investment and firm performance: A meta-analysis.* Paper presented at the 37th Annual Hawaii International Conference on System Sciences.

McGrath, J. E. (1981). Delimmatics: The study of research choices and dilemmas. *American Behavioral Scientist, 25*(2), 179-210.

McKeen, J. D., Guimaraes, T., & Wetherbe, J. C. (1994). The relationship between user participation and user satisfaction: An investigation of four contingency factors. *MIS Quarterly, 18*(4), 427-451.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-322.

Ng, B. Y., Kankanhalli, A., & Xu, Y. J. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Ortiz de Guinea, A., & Markus, M. L. (2009). Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quarterly, 33*(3), 433-444.

Pashler, H. (1994). Dual-task interference in simple tasks: Data and theory. *Psychological Bulletin, 116*(2), 220-244.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115-143.

Pieters, R. G., & Verplanken, B. (1995). Intention-Behaviour Consistency: Effects of consideration set size, involvement and need for cognition. *European Journal of Social Psychology, 25*(5), 531-543.

Randall, D. M., & Wolff, J. A. (1994). The time interval in the intention-behaviour relationship: Meta-analysis. *British Journal of Social Psychology, 33*(4), 405-418.

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

Schifter, D. E., & Ajzen, I. (1985). Intention, perceived control, and weight loss: An application of the theory of planned behavior. *Journal of Personality and Social Psychology, 49*(3), 843-851.

Sheeran, P. (2002). Intention-behavior relations: A conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1-36.

Sheeran, P., Norman, P., & Orbell, S. (1999). Evidence that intentions based on attitudes better predict behaviour than intentions based on subjective norms. *European Journal of Social Psychology, 29*(2-3), 403-406.

Sheeran, P., & Webb, T. L. (2016). The intention-behavior gap. *Social and Personality Psychology Compass, 10*(9), 503-518.

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

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological Review, 63*(2), 129-138.

Smith, M. (2016). 88 percent of workers "lack basic privacy and cyber security knowledge." https://business-reporter.co.uk/2016/10/28/88-per-cent-workers-lack-basic-privacy-cyber-security-knowledge/

Sutton, S., McVey, D., & Glanz, A. (1999). A comparative test of the theory of reasoned action and the theory of planned behavior in the prediction of condom use intentions in a national sample of english young people. *Health Psychology, 18*(1), 72-81.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). *Do users' perceptions of password security match reality?* Paper presented at the CHI Conference on Human Factors in Computing Systems.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., . . . Cranor, L. F. (2015). *I added "!"at the end to make it secure: Observing password creation in the lab.* Paper presented at the Symposium on Usable Privacy and Security.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

Wang, W., & Benbasat, I. (2009). Interactive decision aids for consumer decision making in e-commerce: The influence of perceived strategy restrictiveness. *MIS Quarterly, 33*(2), 293-320.

Wash, R., & Rader, E. J. (2015). *Too much knowledge? Security beliefs and protective behaviors among United States internet users*. Paper presented at the Symposium on Usable Privacy and Security.

Wigfield, A., & Eccles, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemporary Educational Psychology, 25*(1), 68-81.

Willey, L., & White, B. J. (2019). Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education, 24*(3), 181-188.

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

Zipf, G. K. (1949). *Human behavior and the principle of least effort*. Addison-Wesley.

Appendix A: Survey Instruments

For Experiments 1 and 2, participants were given a summary of the password policy and were then asked questions about their beliefs and intentions to follow the policy (Table A1).

Table A1. Item Description for Experiments 1 and 2

Items	Dimensions	Scale	Source
Intro	This corporation's password policy requires that all of your passwords adhere to the following guidelines: Should be 15 or more characters Contain both upper- and lowercase letters (e.g., a-z, A-Z) Have at least one digit (0-9) Have at least one special character (e.g., !@#$%^&*()_+|~-) Are not words found in a dictionary (e.g., normal words, common names, or a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc.)		
INT	**Intentions to comply with the password policy**		
	I intend to comply with the requirements of the password policy for this organization.	a	(Bulgurcu et al., 2010)
	I intend to create passwords according to the requirements of the password policy of this organization.		
	I intend to carry out my responsibilities prescribed in the password policy for this organization when I create passwords.		
PBC	**Perceived behavioral control**		
	I would be able to create strong passwords per the password policy on my own.	c	(Taylor & Todd, 1995)
	Creating strong passwords per the password policy is entirely within my control.		
	I have the resources and the knowledge and the ability to create strong passwords per the password policy.		
E	**Manipulation check: self-reported effort**		
	Authenticating was very frustrating.	b	(adapted from Wang & Benbasat, 2009)
	Using this system, I could easily authenticate. (R)		
	Authenticating took too much time.		
	Authenticating was easy. (R)		
	Authenticating required too much effort.		
	Authenticating was too complex.		

Note: * reversed coded items (noted with an R in the item text) were recoded to be consistent with the other items.

Scales:
a. 1 = *Strongly Disagree;* 7 = *Strongly Agree*
b. 0 = *Strongly Disagree;* 10 = *Strongly Agree*
c. 1 = *Almost Never;* 2 = *Very Rarely;* 3 = *Rarely;* 4 = *Occasionally;* 5 = *Frequently;* 6 = *Very Frequently;* 7 = *Almost Always*

For Experiment 3, participants were given a summary of the information disclosure policy and were then asked questions about their beliefs and intentions to follow the policy (Table A2).

Table A2. Item Description for Experiment 3

Items	Dimensions	Scale	Source
INT	**Intentions to adhere to the information disclosure policy**		
	I intend to comply with the requirements of the information disclosure policy for this organization.	a	(Bulgurcu et al., 2010)
	I intend to share information only according to the requirements of the information disclosure policy of this organization.		
	I intend to carry out my responsibilities prescribed in the information disclosure policy for this organization.		
PBC	**Perceived behavioral control**		
	I would be able to adhere to the information disclosure policy on my own.	c	(Taylor & Todd, 1995)
	Adhering to the information disclosure policy is entirely within my control.		
	I have the resources and the knowledge and the ability to adhere to the information disclosure policy.		
E*	**Manipulation check: self-reported effort**		
	Adhering to the information disclosure policy was very frustrating.	b	(adapted from Wang & Benbasat, 2009)
	I could easily adhere to the information disclosure policy. (R)		
	Adhering to the information disclosure policy took too much time.		
	Adhering to the information disclosure policy was easy. (R)		
	Adhering to the information disclosure policy required too much effort.		
	Adhering to the information disclosure policy was too complex.		

Note: * reversed coded items (noted with an R in the item text) were recoded to be consistent with the other items.

Scales:
a. 1 = *Strongly Disagree;* 7 = *Strongly Agree*
b. 0 = *Strong Disagree;* 10 = *Strong Agree*
c. 1 = *Almost Never;* 2 = *Very Rarely;* 3 = *Rarely;* 4 = *Occasionally;* 5 = *Frequently;* 6 = *Very Frequently;* 7 = *Almost Always*

Appendix B: Instrument Validation

Table B1. Measurement Model, Validity, and Reliability Experiment 1

#	Construct	Mean	SD	VIF	Composite reliability	Cronbach's alpha	AVE	1	2	3
1	Intentions	5.683	1.125	1.001	0.893	0.864	0.712	**0.844**		
2	PBC	5.263	1.222	1.006	0.944	0.937	0.877	0.006	**0.936**	
3	Self-reported effort	5.259	1.164	1.007	0.954	0.956	0.766	(0.026)	(0.77)	**0.875**
Note: SQRT of AVE on Diagonals of the Correlation Matrix										

Table B2. Measurement Model, Validity, and Reliability Experiment 2

#	Construct	Mean	SD	VIF	Composite reliability	Cronbach's alpha	AVE	1	2	3
1	Intentions	5.595	1.297	13.700*	0.977	0.977	0.935	**0.967**		
2	PBC	5.244	1.067	1.124	0.844	0.840	0.638	0.292	**0.799**	
3	Self-reported effort	5.447	1.071	13.999*	0.938	0.937	0.714	(0.462)	(0.324)	**0.845**
Note: *If including self-reported effort in the model, the VIF indicates that multicollinearity is too high; however, the self-reported effort variable was only used for manipulation checks and was not included in the actual model. When excluding self-reported effort (as done in our models to test the hypotheses), the VIF is acceptable: 1.094 for intentions. We, therefore, deem multicollinearity to be a nonissue in our model. SQRT of AVE on diagonals of the correlation matrix										

Table B3. Measurement Model, Validity, and Reliability Experiment 3

#	Construct	Mean	SD	VIF	Composite reliability	Cronbach's alpha	AVE	1	2	3
1	Intentions	6.224	1.007	1.334	0.979	0.979	0.940	**0.970**		
2	PBC	6.051	1.002	1.375	0.917	0.917	0.788	0.475	**0.888**	
3	Self-reported effort	5.096	1.143	1.036	0.874	0.869	0.554	(0.081)	(0.052)	**0.744**
Note: SQRT of AVE on diagonals of the correlation matrix										

Table B4. Experiment 1 Exploratory Factor Analysis

	Component		
	Effort	**PBC**	**Intentions**
int1	-0.01	-0.08	0.79
int2	-0.02	0.05	0.91
int3	-0.12	0.05	0.96
pbc1	-0.36	0.86	0
pbc2	-0.43	0.87	-0.07
pbc3	-0.4	0.82	0.02
effort1	0.72	-0.55	-0.13
effort2	0.76	-0.44	-0.23
effort3	0.79	-0.45	-0.13
effort4	0.86	-0.2	-0.03
effort5	0.9	-0.32	0.01
effort6	0.89	-0.32	0.05

Note: Extraction method: Principal component analysis
Rotation method: Varimax with Kaiser normalization

Table B5. Experiment 2 Exploratory Factor Analysis

	Component		
	Effort	**Intentions**	**PBC**
int1	-0.15	**0.97**	0.08
int2	-0.18	**0.94**	0.1
int3	-0.16	**0.96**	0.07
pbc1	-0.33	0.15	**0.8**
pbc2	-0.28	0.03	**0.82**
pbc3	-0.28	0.08	**0.82**
effort1	**0.83**	-0.15	-0.28
effort2	**0.84**	-0.1	-0.2
effort3	**0.85**	-0.19	-0.23
effort4	**0.76**	-0.08	-0.26
effort5	**0.82**	-0.16	-0.27
effort6	**0.85**	-0.19	-0.24

Note: Extraction method: Principal component analysis.
Rotation method: Varimax with Kaiser normalization.

Table B6. Experiment 3 Exploratory Factor Analysis

	Component		
	Effort	**Intentions**	**PBC**
int1	-0.07	**0.93**	0.29
int2	-0.08	**0.95**	0.24
int3	-0.08	**0.95**	0.24
pbc1	-0.15	0.3	**0.85**
pbc2	-0.13	0.27	**0.87**
pbc3	-0.14	0.21	**0.9**
effort1	**0.79**	-0.04	0.1
effort2	**0.65**	-0.04	-0.11

effort3	**0.85**	-0.07	-0.08
effort4	**0.65**	0.02	-0.13
effort5	**0.83**	-0.12	-0.16
effort6	**0.85**	-0.09	-0.18
Note: Extraction method: Principal component analysis Rotation method: Varimax with Kaiser normalization			

Appendix C: Training Material

In all three studies, we provided a security policy and associated online training to help ensure participants understand the security expectations. In addition, we asked participants to complete a questionnaire to verify comprehension. For Studies 1 and 2, Figure C1 shows a screenshot of part of the security policy, and Figure C2 shows a segment of the video. For Study 3, Figure C3 shows part of the security policy, Figure C4 shows the security policy reminder (shown just-in-time), and Figure C5 shows a segment of the security training video.

General Password Construction Guidelines
All users should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least fifteen alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The word "NetworkSolutions.com" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Figure C1. Security Policy for Studies 1 and 2

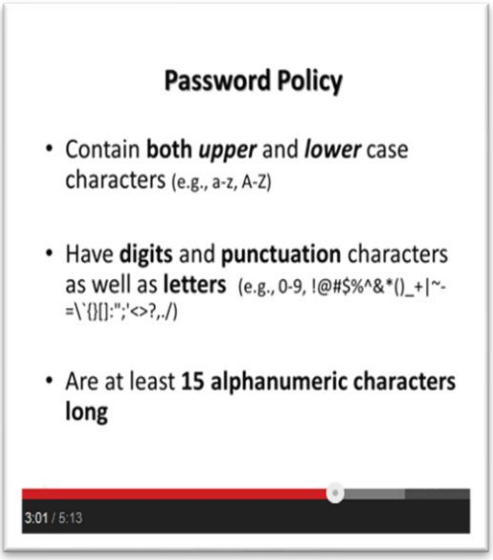

Figure C2. Screenshot of Video Segment Training for Studies 1 and 2 (5-Minute Narrated Slide Show)

A. General Client Disclosure Information

You should never disclose information about clients to others, including suppliers, vendors, co-workers, and other people. Only with written permission are you allow to disclose information about clients. Information about clients include: a) names of clients, b) contact information about clients, c) names of people working for our clients, or d) any other information about clients.

Figure C3. Security Policy for Study 3

REMEMBER: Do not disclose customer information (name, contact, etc.) to anyone.

Figure C4. Security Policy Reminder for Study 3

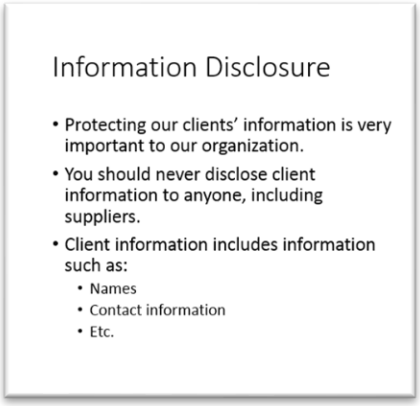

Figure C5. Short Training Video (Narrated Slide Show) for Study 3.

About the Authors

Jeffrey L. Jenkins is an associate professor of information systems at the Marriott School of Business, Brigham Young University. His research focuses on behavioral information security and using human-computer input devices (e.g., the computer mouse, touchscreen, keyboard) to better understand users' cognitive and emotional states. He has applied his expertise to a variety of settings to improve fraud detection, risk assessments, system usability, and online learning. He is an active entrepreneur and his research has been patented and successfully commercialized, in addition to being extensively published in leading business and technology journals. He graduated with a PhD in management with a major in management information systems and a minor in computational linguistics from the University of Arizona. He earned a master's degree in information systems management and a bachelor's degree in information systems from Brigham Young University, and an associate degree in information systems from Brigham Young University-Idaho.

Alexandra Durcikova is an associate professor at the Price College of Business at the University of Oklahoma. She has two research streams. The first stream focuses on the adoption of electronic knowledge repositories (EKR) by individuals in organizational settings. The second stream focuses on end-user security behavior; specifically, the goal is to develop a deeper understanding of how different types of technical controls and educational controls influence employees' compliance with security policies. Her work has been published in premium journals such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *European Journal of Information Systems*, as well as other journals and international conference proceedings.

Jay F. Nunamaker, Jr. is a Regents and Soldwedel Professor of MIS, computer science and communication and director of the Center for the Management of Information and the National Center for Border Security and Immigration at the University of Arizona. He received his PhD in operations research and systems engineering from Case Institute of Technology. He has held a professional engineer's license since 1965. He was inducted into the Design Science Hall of Fame and received the LEO Award for Lifetime Achievement from the Association for Information Systems. He was featured in the July 1997 issue of *Forbes* magazine on technology as one of eight key innovators in information technology. His specialization is in the fields of system analysis and design, collaboration technology, and deception detection. The commercial product GroupSystems ThinkTank, based on his research, is often referred to as the gold standard for structured collaboration systems. He founded the MIS Department at the University of Arizona in 1974 and served as department head for 18 years.