

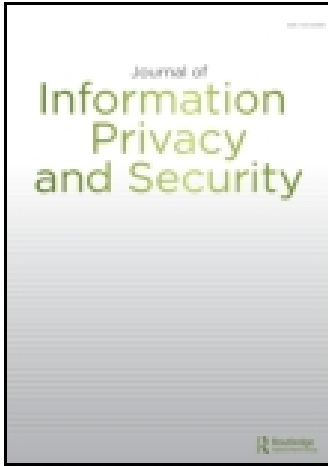
This article was downloaded by: [York University Libraries]

On: 11 November 2014, At: 19:04

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954

Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



## Journal of Information Privacy and Security

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/uips20>

### Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy

Jeffrey D. Wall<sup>a</sup>, Prashant Palvia<sup>b</sup> & Paul Benjamin Lowry<sup>c</sup>

<sup>a</sup> University of North Carolina at Greensboro,

<sup>b</sup> University of North Carolina at Greensboro,

<sup>c</sup> City University of Hong Kong,

Published online: 07 Jul 2014.

To cite this article: Jeffrey D. Wall, Prashant Palvia & Paul Benjamin Lowry (2013) Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy, *Journal of Information Privacy and Security*, 9:4, 52-79, DOI: [10.1080/15536548.2013.10845690](https://doi.org/10.1080/15536548.2013.10845690)

To link to this article: <http://dx.doi.org/10.1080/15536548.2013.10845690>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing,

systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

## Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy

Jeffrey D. Wall, University of North Carolina at Greensboro, jdwall2@uncg.edu

Prashant Palvia, University of North Carolina at Greensboro, pcpalvia@uncg.edu

Paul Benjamin Lowry, City University of Hong Kong, paul.lowry.phd@gmail.com

### ABSTRACT

*Employees' failures to follow information security policy can be costly to organizations, causing organizations to implement security controls to motivate secure behavior. Information security research has explored many control-related motivations (e.g., self-efficacy, response efficacy, and behavioral control) in the context of ISP compliance; however, the behavioral effects of perceptions of autonomous functioning are not well understood in security contexts. This paper examines employee autonomy as a control-related motivation from the lens of self-determination theory and psychological reactance theory. Self-determination theory is widely used in other disciplines to explain intrinsically driven behavior, but has not been applied to security research. Psychological reactance theory is also widely used, but is only beginning to receive attention in security research. Self-determination and psychological reactance offer complementary yet opposite conceptualizations of trait-based autonomy. This paper posits that perceptions of trait-based autonomy influence self-efficacy and response efficacy. Through a survey of government employees, we provide support for several hypotheses. We also discuss important directions for the use of self-determination theory and psychological reactance theory in future research.*

**KEYWORDS** Self-determination, reactance, efficacy, information security policy

### INTRODUCTION

Information system (IS) security is increasingly important to organizations, as security breaches are costly (Richardson 2009; Richardson 2011). Technical security controls are not sufficient to prevent security breaches, particularly breaches by employees (Choobineh et al. 2007; Dhillon et al. 2001). Employees are key to maintaining secure IS (Bulgurcu et al. 2010; Crossler et al. 2013; Posey et al. 2013); however, employees are often a weak link in securing organizational information and IS (Warkentin et al. 2009; Willison et al. 2013). Sabotage by employees, such as data theft and data manipulation, cause direct harms to organizations (Warkentin et al. 2009). Further, negligent behaviors, such as failing to log out of organizational systems or sharing passwords, create vulnerabilities and opportunities for external breaches (Workman et al. 2008). Organizations develop security controls to deter harmful autonomous action

and encourage beneficial autonomous action in employees. Sanctions, for example, are used to deter misbehavior (D'Arcy et al. 2011), while training and education are used to promote positive security behavior (Puhakainen et al. 2010). The importance of information security in organizations has prompted a burgeoning of research on employee compliance and noncompliance with security policies and standards.

Control-related motivations figure prominently in explaining employees' compliance with information security policy (ISP). *Control-related motivations* refer to individuals' perceptions of their ability to execute courses of action given their perceptions of control over themselves and their environment (Biddle 1999; Boss et al. 2009). Self-efficacy, locus of control, perceived behavioral control, and self-determination offer different ways to conceptualize control-related motivation (Biddle 1999). Additionally, psychological reactance (Brehm et al. 1981) represents a form of control-related demotivation. Many of these constructs have been studied in information security research, including: self-efficacy (e.g., Johnston et al. 2010; Warkentin et al. 2011), behavioral control (e.g., Pee et al. 2008), locus of control (e.g., Workman et al. 2008), and psychological reactance (e.g., Lowry et al. 2010; Posey et al. 2011).

Self-determination, however, has not received attention in information security research. Self-determination is studied widely in other disciplines (e.g., Deci et al. 1999; Hodgins et al. 1996; Koestner et al. 1992; Koestner et al. 1996; Olesen 2011; Olesen et al. 2010; Ryan et al. 1985; Ryan et al. 2000), including in areas of IS research (Ke et al. 2012; Ke et al. 2010; Liu et al. 2013). Self-determination is shown to increase intrinsic motivation, initiative, persistence, psychological well-being, and lead to positive behavioral outcomes (e.g., Deci et al. 1994; Deci et al. 1999).

Self-determination theory provides a useful lens for studying intrinsically motivated, well-adjusted behaviors. We posit that such behaviors would naturally include employees' protection motivation behaviors important to security research (Posey et al. 2013). Additionally, self-determination and psychological reactance are viewed as complementary and somewhat opposite views of autonomy (Koestner et al. 1996; Pavey et al. 2009). Together, therefore, self-determination and reactance offer a more complete view of autonomy than either can alone.

*Self-determination* refers to an individual's belief that his/her actions are self-guided through considerate thought, reflection, and choice (Pavey et al. 2009; Ryan et al. 1985; Ryan et al. 2000). Self-determination theory (Ryan et al. 1985; Ryan et al. 2000) states that self-determination leads to increased intrinsic motivation to accomplish tasks. Conversely, *psychological reactance* refers to an individual's belief in his/her right to freedom from external restriction (Brehm 1966; Brehm et al. 1981; Pavey et al. 2009). Reactance theory (Brehm 1966; Brehm et al. 1981) suggests that individuals desire freedom and that they react to encroachments of their autonomy by reasserting their perceived rights. Both conceptualizations of autonomy are trait-based (Brehm 1966; Brehm et al. 1981; Ryan et al. 1985; Ryan et al. 2000). Together, self-determination and reactance offer a holistic and dualistic perspective of trait-based autonomy missing from information security research.

This paper seeks to explore autonomy perceptions in relation to efficacy perceptions. Efficacy perceptions are important to information security research (e.g., Johnston et al. 2010; Warkentin et al. 2011). Further, many studies examine control-related motivations in isolation, particularly within information security research (Herath et al. 2009b; Johnston et al. 2010). This paper examines the effect trait-based autonomy and situation-specific efficacy perceptions have on employees' intentions to comply with security policy in order to better understand autonomy in security settings and the relationships between different control-related motivations. In particular, we ask: *how do autonomy and efficacy relate and how do these control-related motivations affect employee's ISP compliance intentions?*

To answer this question, we developed a conceptual model that counterpoises the key elements of self-determination and reactance, and tested it with an online survey of government employees in the United States (US). The survey was developed from well-established instruments, including an instrument used in self-determination research that consists of several vignettes. Analyses were conducted using partial least squares (PLS). The results provide preliminary evidence that autonomy perceptions influence efficacy perceptions, and thereby, influence intentions to comply with security policy.

This study contributes to IS security research in several ways. First, we introduce self-determination theory to IS security research. Self-determination theory has been important to other fields in explaining intrinsic drive to engage in tasks (Koestner et al. 1996). Information security compliance requires proactive effort to be efficacious (Choobineh et al. 2007); therefore, self-determination may be an important theoretical contribution to information security research. Second, this paper provides a conceptualization of autonomy that captures the duality of autonomy. We offer a more complete conceptual understanding of the effect of autonomy on employees' information security behaviors than has been presented previously. Third, we provide evidence of linkages between different types of control-related motivations in a security setting. Security research has mostly failed to examine relationships between different control-related motivations, particularly autonomy and efficacy. Finally, we highlight potential issues with highly used instruments pertaining to self-determination and psychological reactance. Studies in other fields have mostly failed to examine convergent and discriminant validities, relying solely on reliability to determine the quality of the scales. We provide important insight into the measurement of self-determination and psychological reactance.

The remainder of this paper continues as follows. First, we provide a literature review with a focus on control-related motivations. Second, we present a conceptual model to link perceptions of autonomy with perceptions of efficacy and intentions to comply with security policy. Third, we describe the methodology used to test the model. Fourth, we present the analysis and results. Finally, we discuss the implications of the study.

## THEORETICAL FOUNDATIONS

The study of employees' compliance with ISP is a major focus in behavioral information security research (Crossler et al. 2013). Further, control-related motivations are an important topic in security research (e.g., Herath et al. 2009a; Herath et al. 2009b; Johnston et al. 2010; Vance et al. 2012; Warkentin et al. 2011). Behavioral information security studies examine control-related motivations in two primary ways. First, some studies examine control-related motivations as covariates with other security-related variables. Self-efficacy, for example, is a common covariate in information security research (Bulgurcu et al. 2010; Herath et al. 2009b). Behavioral control (e.g., Pee et al. 2008) and locus of control (e.g., Workman et al. 2008) have also been studied in this manner. Second, a few studies examine control-related motivations as mediating factors. Warkentin et al. (2011), for example, find that self-efficacy mediates the relationship between security controls and compliance. Similarly, Posey et al. (2011) discuss the mediating role of reactance in security settings, though they do not empirically test its mediating role. Vance et al. (2012) suggest self-efficacy and response efficacy mediate habit and intentions to comply with ISP. Additionally, Boss et al. (2009) find that the perceived mandatoriness of security policy mediates compliance. *Mandatoriness* which refers to "the degree to which individuals perceive that compliance... is compulsory or expected" (p. 151) could be considered a control-related motivation as well, as it focuses on perceptions of control.

This paper follows the second model; we examine control-related motivations as mediating factors. However, like Myrny et al. (2009), we do not directly examine security controls, but focus instead on motivational factors that lead to behavior change. In this way, we are able to hypothesize and explore the ways that different control-related motivations relate to one another. Such an attempt has not been made in behavioral information security literature. Examining control-related motivations is particularly interesting in the study of autonomy and efficacy. Autonomy and efficacy provide two different ways to examine perceptions of control (Senecal et al. 2000), but little is known about how they relate. Understanding how autonomy relates to efficacy may help managers develop appropriate controls that increase efficacy and subsequent behavior.

### Self-determination

Self-determination is derived from self-determination theory (Ryan et al. 1985; Ryan et al. 2000). Self-determination is considered a trait-based phenomenon, though some research conceptualize it as a semi-contextualized phenomenon (Koestner et al. 1992; Koestner et al. 1996). Self-determination theory suggests that individuals' behavior is driven by three psychological needs—competence, relatedness, and autonomy. *Competence* refers to individuals' needs and attempts to control the outcomes of their actions and to feel effectance. *Relatedness* refers to individuals' needs and strivings to develop satisfying, authentic social relationships. Finally, *autonomy* refers to individuals' needs and strivings to be agentic; to feel that they direct their own courses of action and can choose their behaviors. Self-determination theory explains the development of perceptions of autonomous functioning. Autonomy is the central

component of self-determination theory. Self-determination theory captures control-related motivations with three orientations—autonomous, control-determined, and impersonal functioning (Ryan et al. 1985). Self-determination is best represented by the autonomous orientation (Koestner et al. 1992). Given that our focus is autonomy, we do not examine the other orientations mentioned in self-determination theory. This should not dissuade researchers from exploring the effect of the other orientations on security behavior.

Research on self-determination suggests that autonomy increases intrinsic motivation, initiative, persistence, psychological well-being, optimism, and behavioral consistency (Deci et al. 1994; Deci et al. 1999; Koestner et al. 1996). Ryan and Deci (1985), for example, found that individuals with high autonomy orientations are more likely to feel intrinsic drive to complete tasks. Koestner et al. (1992) found that individuals' with high self-determination demonstrate more consistency between their attitudes and behaviors. Deci et al. (1994) found that individuals with high autonomous orientations are more likely to internalize behavior. That is, individuals are more likely to "identify with the value of an activity and accept full responsibility for doing it" (p. 121) when they feel high levels of autonomy. Importantly, self-determination does not mean that an individual actively opposes outside influence. To the contrary, individuals with high levels of self-determination may be open to external influence, but feel able to make self-directed decisions regarding external influences (Koestner et al. 1996; Pavey et al. 2009).

In IS research, self-determination has been used to study a number of phenomena. Ke et al. (2012) use self-determination theory to examine the influence of intrinsic motivation on the adoption and exploration of enterprise IS. They find that intrinsic motivation increases users' exploration of systems. Similarly, Ke and Zhang (2010) use self-determination theory to explain how satisfaction of individuals' needs for competence, autonomy, and relatedness moderate the relationship between motivation and task effort in developing open source software (Ke et al. 2010). Finally, Liu et al. (2013) use self-determination theory to explain effort in digital gaming contexts. Many of the IS studies treat self-determination as contextualized rather than trait-based phenomenon. In this study, we examine self-determination as primarily trait-based as described in the original conceptualization of self-determination (Ryan et al. 1985; Ryan et al. 2000).

### **Psychological Reactance**

Psychological reactance is derived from psychological reactance theory (Brehm 1966; Brehm et al. 1981). Reactance theory is based on the premise that individuals desire to be free from the control of others. Reactance theory also asserts that individuals will strive to restore freedoms which they perceive to be threatened by external control. The attempt to restore freedom is referred to as reactance. Reactance is conceptualized as being a stable personality trait (Brehm et al. 1981; Koestner et al. 1996) as well as a behavioral response (Lowry et al. 2010). In this paper, we examine reactance as a personality trait, as we compare it with self-determination which is also a trait-based construct. To be consistent in our treatment of autonomy, we do not examine reactance as a behavioral response. Thus, in the remainder of this paper, reactance

refers to trait-based reactance and not reactance as a behavioral response. When reactance as a trait and reactance as a response are examined in a single study, trait reactance is referred to as reactance proneness, while the behavioral response is called reactance. However, such distinctions are not necessary in this paper. Reactance is manifest by several factors, including: emotional response to restricted choice, reactance to compliance, resisting influence from others, and reactance toward advice and recommendations (Hong et al. 1996).

Reactance is associated with decreased self-esteem, life satisfaction, religiosity, and locus of control, and is associated with increased trait anger and depression (Hong et al. 1996). In addition to these maladapted feelings and perceptions, reactance has been shown to affect behavior. For example, reactance has been shown to affect compliance with health regimens (Dillard et al. 2005) and may lead to noncompliant behavior (Brown et al. 2011). In IS research, psychological reactance is employed to study several phenomena, such as the formation of preferences for IS interfaces (Murray et al. 2011), reactance to online recommendation services (Lee et al. 2009), and decision-makers reactions to feedback (Hosack 2007). In an information security context, Posey et al. (Posey et al. 2011) suggest that computer monitoring may lead to reactance that results in insecure behavior.

### **Efficacy**

In this paper we examine efficacy as self-efficacy and response efficacy. Self-efficacy is derived from Bandura's social cognitive theory (Bandura 1986). *Self-efficacy* refers to individuals' "judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" (Bandura 1986). Self-efficacy is task dependent, and is shown to increase persistence with a task even when faced with opposition (Schunk et al. 2005). As suggested earlier, self-efficacy is used extensively in behavioral information security research as a covariate and mediating variable. In security literature, self-efficacy is often conceptualized as an individual's perception that he/she can comply with ISP or use security technologies in order to secure organizational information and IS. Self-efficacy is shown to increase positive security behaviors (Herath et al. 2009b; Johnston et al. 2010; Vance et al. 2012).

Response efficacy stems from protection motivation theory (Rogers 1975) and is similar to expectations in expectancy theory (Vroom 1964). *Response efficacy* refers to individuals' perceptions that a course of action will result in desirable outcomes (Johnston et al. 2010). Response efficacy is based on cognitive analysis of the potential outcomes of a course of action (Witte 1992). According to protection motivation theory, response efficacy influences individuals' actions (Rogers 1975). Similarly, in expectancy theory, individuals engage in activities based on the perceived likelihood of positive outcomes resulting from the activity (Van Eerde et al. 1996). Thus, response efficacy can be a strong motivator of behavior when response efficacy is high. Response efficacy is also shown to increase positive security behaviors and attitudes (Herath et al. 2009a; Herath et al. 2009b; Johnston et al. 2010; Vance et al. 2012).



**CONCEPTUAL MODEL**

Our proposed conceptual model links several conceptualizations of control-related motivation in order to better understand why employees comply with security policy. At a high level, the model suggests that individuals' trait-based perceptions of autonomy influence situational efficacy perceptions, and thereby influence their compliance intentions. Figure 1 presents the conceptual model.

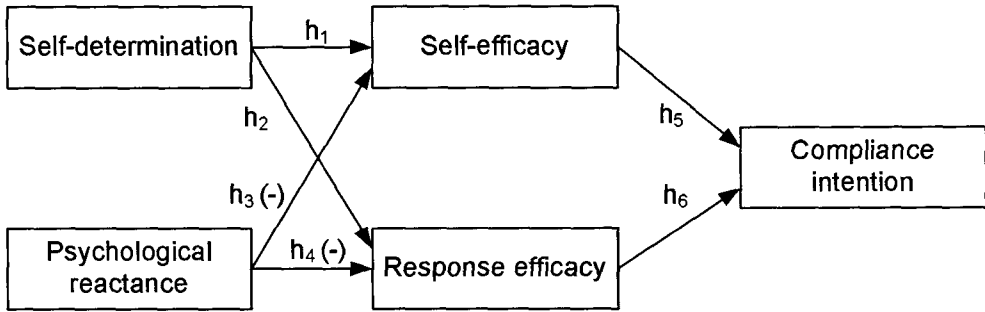


Figure 1 - Conceptual Model

**Autonomy and Efficacy**

Self-determination helps to promote positive cognitions and emotions (Ryan et al. 2000) which can promote consistent behavior (Koestner et al. 1992). Engaging in consistent behavior is essential to the development of task-specific mastery. Continued personal experience with a task helps individuals to master the task, thereby increasing individuals' perceptions of their ability to successfully engage with the task (Bandura 1977a; Bandura 1986; Bandura 1997). In this way, self-determination may influence the development of task-specific self-efficacy. That is, self-determination creates the intrinsic motivation to promote consistent task-related behavior, which influences mastery of the task and subsequent feelings of efficacy. In a security setting, high levels of self-determination could influence consistent security behavior and the subsequent development of compliance self-efficacy through continued experience with security tasks. In this paper, we define *self-efficacy* as an individual's perception of his/her ability to comply with security policies in order to ensure the security of organizational information and IS. As a trait characteristic, self-determination has the potential to influence attitudes toward specific tasks (Ryan et al. 1985; Ryan et al. 2000). That is, self-determination has the potential to enhance performance across many tasks. Therefore, an increase in self-determination could increase security-related self-efficacy. Based on this discussion, we propose:

*Hypothesis 1: An increase in perceptions of self-determination pertaining to policy compliance will increase perceptions of self-efficacy to comply with security policy.*

In similar fashion, the positive emotions and general well-being experienced by individuals with high levels of self-determination is likely to affect perceptions of response efficacy as well. In this paper, *response efficacy* refers to individuals' perceptions that complying with ISP will help to secure organizational information

and IS. Individuals who experience positive emotions tend to view the world through “rose-colored glasses.” For example, positive emotions and general contentment may increase the perceived desirability of objects (Griskevicius et al. 2010). Further, at the neurological level, optimism is shown to influence individuals’ perceptions of outcomes (Izuma et al. 2011). Therefore, a positive outlook on life could influence perceptions of the outcomes of a particular response. In the case of information security, high levels of self-determination should lead to strong perceptions of response efficacy pertaining to policy compliance by positively altering the mood of an employee. Therefore, we suggest:

*Hypothesis 2: An increase in perceptions of self-determination pertaining to policy compliance will increase perceptions of the response efficacy of security policy compliance.*

Like self-determination, psychological reactance is considered trait-based rather than situation dependent (Brehm 1966; Dillard et al. 2005). As such, general emotions and cognitions can affect individuals’ perceptions and attitudes across tasks. Psychological reactance is associated with depression and anger, and may negatively influence perceptions of control and general well-being (Hong et al. 1996). By increasing negative perceptions and feelings, psychological reactance may affect self-efficacy by influencing emotional arousal. Emotional arousal affects performance efficacy perceptions (Bandura 1977a; Bandura 1977b; Bandura 1997). Further, negative emotions and cognitions related to high levels of psychological reactance may influence job performance (Ford et al. 2011). Failure to successfully complete job tasks could lead to perceptions of low self-efficacy pertaining to those tasks. Where reactance influences security-related job performance, it could subsequently influence efficacy perceptions. Further, low self-esteem, a symptom of individuals that experience high level of psychological reactance, can affect general perceptions of competence (Lewinsohn et al. 1980), thereby decreasing perceptions of self-efficacy. Based on this discussion, we suggest:

*Hypothesis 3: An increase in psychological reactance proneness will decrease perceptions of self-efficacy to comply with security policy.*

Psychological reactance may negatively affect response efficacy as well. An important dimension of reactance is reactance to compliance. Individuals with high levels of psychological reactance are likely to experience negative emotions and cognitions toward efforts to garner compliance with some rule or policy (Hong et al. 1996) and may even lead to noncompliant behaviors in an attempt to reassert autonomy (Brown et al. 2011; Posey et al. 2011). Therefore, ISPs are not likely to be viewed in a positive manner by individuals with high levels of psychological reactance. We argue that these negative thoughts and emotions influence perceptions of the outcomes of security policy compliance. Individuals with high levels of psychological reactance also resist persuasion and influence. Thus, managerial interventions that attempt to influence ISP compliance may further decrease perceptions of response efficacy by increasing the likelihood of negative emotional responses to the control environment. Given this discussion, we propose:

*Hypothesis 4: An increase in psychological reactance proneness will decrease perceptions of the response efficacy of security policy.*

### **Efficacy and Compliance**

Self-efficacy and response efficacy are used widely in information security research to explain and predict employee security behavior. Self-efficacy influences ISP policy compliance intentions (Bulgurcu et al. 2010), protective technology usage (Rhee et al. 2009), and secure email behavior (Vishwanath et al. 2011). Similarly, response efficacy is shown to influence positive security attitude and behavior (Herath et al. 2009a; Herath et al. 2009b; Johnston et al. 2010). Self-efficacy influences sustained effort in the performance of tasks, even when confronted with opposition (Schunk et al. 2005). Thus, we propose that self-efficacy will increase ISP compliance intentions. We define the *behavioral intention to comply with ISP* as the degree to which individuals plan to follow and feel motivated to follow the official, organizational ISP. Studying behavioral intention is common in security research (Crossler et al. 2013) and is based on the premise that intentions to engage in behavior lead to actual behavior (Ajzen 1985; Fishbein et al. 1975). Based on this discussion, we propose:

*Hypothesis 5: An increase in perceptions of self-efficacy will increase intentions to comply with security policy.*

Beyond feeling capable of completing a task, individuals desire to know that their efforts in completing tasks will lead to desirable outcomes (Rogers 1975; Van Eerde et al. 1996). When individuals know that a course of action will lead to positive outcomes, they feel motivated to engage in the action and are more likely to do so. Conversely, demotivation occurs when courses of action are perceived as unlikely to produce desirable outcomes. Response efficacy is shown to affect both attitudes and behaviors toward information security and policy compliance (Herath et al. 2009a; Herath et al. 2009b; Johnston et al. 2010; Vance et al. 2012). In summary, we propose:

*Hypothesis 6: An increase in perceptions of the response efficacy of security policy compliance will increase intentions to comply with security policy.*

### **METHODOLOGY**

To test the model, an online survey was distributed to employees of municipal governments in the US. Governments tend to develop rigid hierarchical structures and bureaucratic controls. Thus, governments offer an ideal setting for the study of autonomy and control. The municipalities for this study were randomly selected from the International City Management Association's (ICMA) list of municipalities. Only municipalities with a population greater than 5,000 citizens were randomly sampled to increase the likelihood that respondents would have regular access to computers at work. After the random selection process, publicly available employee emails were taken from the websites of the randomly selected municipalities. Where multiple emails were found on a municipal website, employee emails were randomly selected. The survey instrument was pre-tested by seeking the opinions of content experts and a

pilot study was conducted on undergraduate students in a business school in the Eastern US.

### Measures

The survey consisted of measures for self-efficacy, response efficacy, self-determination, psychological reactance, ISP compliance intentions, and demographic factors, including: age, level of education, gender, work experience, and perceptions of the certainty and severity of sanctions. Measures of self-efficacy and response efficacy were borrowed from (Johnston et al. 2010). Measures of self-determination were borrowed from the 17 vignette version of the General Causality Orientations Scale (GCOS) (Hodgins et al. 1996). Only the autonomy orientation measures were used from the GCOS scale to match the focus of the paper. Measures of reactive autonomy were borrowed from (Hong et al. 1996). Measures of compliance intention were borrowed from (Bulgurcu et al. 2010). All items were measured on a 7 point Likert scale. The items for key constructs are presented in Appendix A.

### Participants

The survey response rate was less than 5 percent. 238 government employees responded to the survey. Low response rates are common when surveys are distributed to unsolicited groups and are common even in highly reputed journals (Sivo et al. 2006). The emails were also sent shortly after a major US holiday. Therefore, recipients may have been particularly overwhelmed with a buildup of high priority emails.

**Table 1. Results from Comparison of Early and Late Responders**

Variable	p-value
Age	0.3080
Education	0.7868
Emotional response to restricted choice	0.9143
Gender	0.3163
ISP compliance intention	0.1093
Job position	1.0000
Reactance to compliance	0.4067
Response efficacy	0.1228
Resistance to influence from others	0.4031
Reactance toward advice and recommendations	0.8616
Self-determination	0.2282
Self-efficacy	0.1724
Work experience	0.6563

Attrition rates were also high. Many respondents failed to answer a significant number of the survey questions. 95 responses were used to test the model after dropping the incomplete responses and removing two responses with values of compliance intentions that were strong outliers. Due to the low response rate and high attrition rate, differences between early and late responders were tested for all variables. Tests

for differences between responses from early and late responders offer a reasonable test for response bias (Sivo et al. 2006). To control for family-wise error rates, we conducted an analysis of variance (ANOVA) in SAS (version 9.2) to determine if responses to key and control variables differed for early and late responders. All p-values in the ANOVA analysis were greater than 0.05, providing some evidence that response bias is not an issue. Table 1 provides the p-values for each key and control variable. The respondents were mostly well-educated, non-IT employees who have extensive work experience and long tenures at the municipalities where they work. More than 40 percent of the respondents had earned at least a Master's Degree. 96 percent of the respondents worked in non-IT positions. Additionally, 97 percent of the respondents had more than 10 years of work experience, and 55 percent had job tenure greater than 10 years.

**Table 2. Demographic Data of Respondents**

Demographic Item	Count	Percent	
Age	18-25	1	1%
	26-35	5	5%
	36-45	11	12%
	46-55	29	31%
	56-65	42	45%
	65+	6	6%
Gender	Male	54	58%
	Female	39	42%
Education	High school	10	11%
	Associate's Degree	8	9%
	Bachelor's Degree	32	34%
	Master's Degree	38	40%
	Doctoral Degree	6	6%
Job position	IT	4	4%
	Non-IT	68	96%
Work experience	1-3 years	0	0%
	4-6 years	1	1%
	7-9 years	2	2%
	10+ years	92	97%
Tenure at the organization	1-3 years	10	11%
	4-6 years	22	23%
	7-9 years	10	11%
	10+ years	52	55%

Nearly an equal number of males and females responded to the survey, 58 and 42 percent respectively. Most of the respondents, more than 75 percent, were over the age of 45. Table 2 presents a more detailed breakdown of the respondents by demographic information. The high number of well-educated and well-tenured respondents is likely a remnant of the email selection process. Emails posted on municipal government websites seem to represent senior employees.

## **RESULTS**

Data was analyzed with partial least squares (PLS) using SmartPLS (version 2.0) (Ringle et al. 2005).

### **Measurement Model**

In both the pilot and full studies, the measures for self-determination displayed high composite reliability (above 0.80); however, they also displayed levels of average variance extracted (AVE) well below the 0.50 cutoff, suggesting a lack of convergent validity (Chin 1998; Fornell et al. 1981). Loadings were extremely low for several of the items. Items with low loadings were systematically dropped until the remaining set of items displayed AVE values above the 0.50 cutoff. A subset of 5 items from the GCOS scale was used to measure self-determination. Many studies that use the GCOS scale treat the measures as a single combined score (e.g., Koestner et al. 1992; Koestner et al. 1996; Ryan et al. 1985) or only examine reliability such as Cronbach's Alpha (e.g., Olesen 2011; Olesen et al. 2010; Ryan et al. 1985). This is not surprising, as the instructions for the use of the GCOS scale call for summations of scores for each of the three orientations (Hodgins et al. 1996; Koestner et al. 1996; Ryan et al. 1985). Convergent validity was not examined in the initial development of the instrument; only reliability was assessed. The convergent validity of the scale is not well understood in the literature. Our study employed PLS to test for convergent validity using AVE and provides an important analysis of the GCOS scale. Our findings suggest that further development of the GCOS scale may be necessary. Addressing the possible issues with the scale is important, as the GCOS scale is widely used. Due to low loadings, three measures were also dropped from the psychological reactance scale. One item was dropped from the reactance to compliance sub-dimension, one was dropped from resistance to influence sub-dimension, and one was dropped from the emotional response to restricted choice sub-dimension. Each sub-dimension remained with two measures.

Reactance is commonly measured as a second-order reflective construct (Hong et al. 1996). To assess the measurement model, we first examined first-order constructs and then examined the psychometric properties of second-order constructs (Wetzels et al. 2009). Overall, the measurement model showed high reliability. Composite reliabilities were high, suggesting internal consistency (Fornell et al. 1981). Additionally, AVE for each latent construct was above the 0.5 cutoff (Chin 1998; Fornell et al. 1981), suggesting convergent validity. Values for AVE and composite reliability are presented in Table 3.

Table 3. AVE and Composite Reliability for First Order Constructs

Construct	AVE	Composite reliability
Emotional response to restricted choice (ERTR)	0.6384	0.7754
ISP compliance intention (ISPC)	0.8600	0.9485
Reactance to compliance (RECO)	0.6653	0.7984
Response efficacy (REFF)	0.8890	0.9412
Resistance to influence from others (RIFO)	0.6894	0.8155
Reactance toward advice and recommendations (RTAR)	0.8453	0.9161
Self-determination (SDET)	0.8667	0.8667
Self-efficacy (SEFF)	0.9550	0.9550

Discriminant validity was tested by ensuring that all item loadings were greater than cross loadings and that the square root of AVE was larger than interconstruct correlations (Chin 1998). Most indicators loaded highly on their associated factors; all but one loading exceeded the common 0.70 cutoff (Fornell et al. 1981). ERTR2 loaded the lowest at 0.6718; however, we retained the measure to maintain a minimum of two items per construct.

Table 4. Factor Loadings and Cross Loadings

	ERTR	ISPC	RECO	REFF	RIFO	RTAR	SDET	SEFF
ERTR1	<b>0.9085</b>	-0.2539	0.2156	-0.2428	0.0802	-0.0756	0.1535	-0.1488
ERTR2	<b>0.6718</b>	-0.1432	0.2844	-0.0817	0.0615	0.1778	-0.0194	-0.1049
ISPC1	-0.2565	<b>0.8995</b>	-0.4660	0.5427	-0.3356	-0.1472	0.2656	0.4837
ISPC2	-0.2248	<b>0.9299</b>	-0.4152	0.4824	-0.3327	-0.0740	0.1942	0.3530
ISPC3	-0.2393	<b>0.9520</b>	-0.4378	0.4673	-0.2844	0.0080	0.2209	0.4297
RECO1	0.3993	-0.3339	<b>0.7613</b>	-0.2807	0.2552	0.2422	-0.0342	-0.2735
RECO2	0.1169	-0.4339	<b>0.8667</b>	-0.3102	0.3532	0.2685	-0.2029	-0.1400
REFF1	-0.1154	0.4858	-0.3727	<b>0.9380</b>	-0.1900	-0.1657	0.3408	0.6592
REFF2	-0.3001	0.5276	-0.3130	<b>0.9477</b>	-0.2260	-0.1407	0.1953	0.5856
RIFO1	0.0688	-0.3232	0.2874	-0.2438	<b>0.8843</b>	0.2306	-0.0209	-0.1143
RIFO2	0.0826	-0.2377	0.3565	-0.1057	<b>0.7725</b>	0.3929	-0.0011	-0.0268
RTAR1	0.0212	-0.0659	0.2240	-0.1266	0.2815	<b>0.9058</b>	-0.2662	-0.0677
RTAR2	0.0146	-0.0774	0.3429	-0.1680	0.3698	<b>0.9328</b>	-0.2915	-0.0335
SDET1	0.0943	0.1524	-0.1010	0.1686	0.0043	-0.2620	<b>0.7024</b>	0.2217
SDET2	0.0946	0.1579	-0.1418	0.1877	0.0414	-0.2152	<b>0.7247</b>	0.2249
SDET3	0.1451	0.1796	-0.1308	0.2649	0.1104	-0.1103	<b>0.8206</b>	0.2357
SDET4	0.0890	0.1745	-0.1087	0.2408	-0.0039	-0.2021	<b>0.8061</b>	0.2521
SDET5	0.0160	0.2352	-0.1111	0.1896	-0.1548	-0.3235	<b>0.7005</b>	0.1869
SEFF1	-0.1410	0.3892	-0.2388	0.5835	-0.0431	-0.0608	0.2876	<b>0.9467</b>
SEFF2	-0.1656	0.4787	-0.2245	0.6677	-0.1250	-0.0433	0.2797	<b>0.9651</b>

Despite the minor issue with ERTR2, all other items loaded well. In all cases, item loadings were higher than cross loadings. Table 4 shows factor loadings and cross loadings.

Additionally, the square root of AVE for each latent variable was higher than the correlations for corresponding latent variables. Table 5 shows latent variable correlations with the square root of AVE on the diagonals. Based on these analyses, there is evidence that the measurement model demonstrates discriminant validity. Common method bias was examined by ensuring that all latent variable correlations were below 0.90 (Pavlou et al. 2007). The highest correlation was 0.6583. Therefore, some evidence exists to suggest that common method bias is not an issue.

**Table 5. Latent Variable Correlations with Square Root of AVE on Diagonals**

	ERTR	ISPC	RECO	REFF	RIFO	RTAR	SDET	SEFF
ERTR	<b>0.7990</b>							
ISPC	-0.2599	<b>0.9274</b>						
RECO	0.2920	-0.4756	<b>0.8157</b>					
REFF	-0.2244	0.5382	-0.3623	<b>0.9429</b>				
RIFO	0.0892	-0.3429	0.3784	-0.2214	<b>0.8303</b>			
RTAR	0.0191	-0.0783	0.3132	-0.1619	0.3577	<b>0.9194</b>		
SDET	0.1107	0.2464	-0.1578	0.2811	-0.0149	-0.3041	<b>0.7526</b>	
SEFF	-0.1615	0.4584	-0.2413	0.6583	-0.0923	-0.0535	0.2960	<b>0.9560</b>

After examining the first-order constructs, we examined the second-order relationships in the reactance scale (Wetzels et al. 2009). Composite reliability was reasonable for the relationships between the first- and second-order constructs (0.7878). However, AVE was below the 0.50 cutoff at 0.3304. This was caused by the loadings of the first-order constructs on the second-order construct. Again, we removed the items to improve AVE. We removed emotional response to restricted choice, which loaded at 0.453, and the reactance to influence from others, which loaded at 0.720. After removing the items, AVE increased to 0.5004. All loadings were significant. Similar to the GCOS scale, the convergent validity of the highly used reactance scale has not been previously assessed. The low levels of AVE are an important finding, as Hong and Faedda (1996) did not test the measurement properties of the second-order structure of the psychological reactance scale. After removing the items, the change to composite reliability was negligible (from 0.7878 to 0.7980). Loadings of the remaining first-order constructs on the second-order construct improved as well; the loading for RECO increased from 0.763 to 0.765 and the loading for RTAR increased from 0.728 to 0.848. Both loadings remained significant. We continued the analysis of the structural model without the ERTR and RTAR sub-dimensions. A post-hoc analysis shows that there are no differences in statistical significance between the models with and without the ERTR and RTAR sub-dimension, and only negligible differences in path coefficients and R-square values. Table 6 presents measurement properties of the second-order psychological reactance construct.

Downloaded by [York University Libraries] at 19:04 11 November 2014

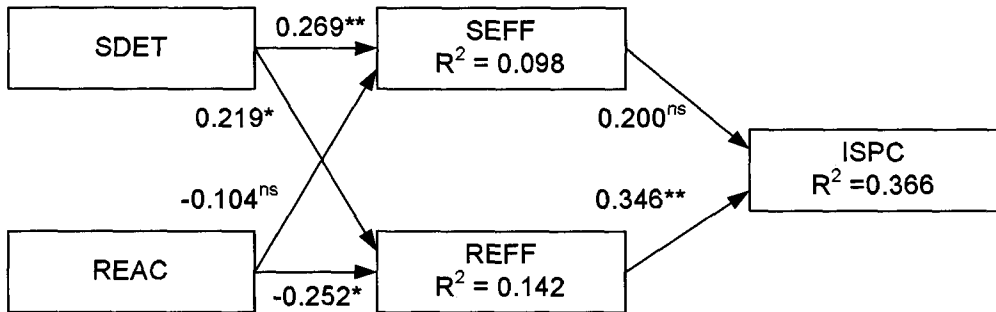


Table 6. Measurement Properties of the Second-Order Psychological Reactance Construct

	Psychological reactance (REAC)	REAC after dropping ERTR and RIFO
Composite reliability	0.7878	0.7980
AVE	0.3304	0.5004
Loadings:		
ERTR	0.453*	N/A
RECO	0.763*	0.765*
RIFO	0.720*	N/A
RTAR	0.728*	0.848*
* Statistical significance at $p < 0.01$		

**Structural Model**

SmartPLS (version 2.0) was used to examine the structural model. We used non-parametric bootstrapping with 500 samples and mean replacement to obtain standard error estimates. Support was found for several of the relationships proposed in the model. Figure 2 presents the results of the PLS analysis. Because a majority of the respondents answered the same for both job position and work experience, these control variables were not included in the PLS model. The limited variability in the responses prevented matrices from being calculated. However, all other control variables were included in the structural analysis.



\* significance at  $p < 0.05$   
 \* significance at  $p < 0.01$

Figure 2. Results of PLS Analysis

Statistical evidence exists to suggest that an increase in self-determination increases perceptions of self-efficacy ( $\beta = 0.269$ ;  $p < 0.01$ ). Thus, we found support for hypothesis 1. Statistical evidence also exists to suggest that self-determination increases perceptions of response efficacy ( $\beta = 0.219$ ;  $p < 0.05$ ). Thus, hypothesis 2 was supported as well. Statistical evidence does not exist to suggest that psychological reactance increases perceptions of self-efficacy ( $\beta = -0.104$ ;  $p > 0.05$ ). Although the sign was negative as proposed, hypothesis 3 was not supported. Statistical evidence does exist to suggest that psychological reactance increases perceptions of response

efficacy ( $\beta = -0.252$ ;  $p < 0.01$ ). Thus, we found support for hypothesis 4. In total, self-determination and psychological reactance accounted for 9.8 percent of the variance in self-efficacy and 14.2 percent of the variance in response efficacy. Since this is a social science study, these values represent a small effect size for self-efficacy and a medium effect size for response efficacy (Cohen 1988).

Accounting for control variables, statistical evidence does not exist to suggest that self-efficacy increases intentions to comply with ISP ( $\beta = 0.200$ ;  $p > 0.05$ ). Although the sign was positive as proposed, hypothesis 5 was not supported. However, accounting for control variables, evidence exists to suggest that an increase in response efficacy increases intentions to comply with ISP ( $\beta = 0.346$ ;  $p < 0.01$ ). Therefore, we found support for hypothesis 6. In total, self-efficacy and response efficacy account for 36.6 percent of the variance in ISP compliance intentions. Age also had a statistically significant effect on compliance intentions ( $\beta = 0.172$ ;  $p < 0.05$ ), showing that an increase in age increases compliance intentions. All other control variables were statistically insignificant, including the certainty and severity of sanctions.

An adequate goodness of fit (GoF) index does not currently exist for PLS models; however, Tenenhaus et al. (2005) proposed a GoF as a diagnostic tool to assess PLS models. The GoF index averages the  $R^2$  values for all endogenous variables in the model and calculates the average communality for model constructs with more than one indicator. Then, the geometric mean of the average  $R^2$  and average communality is calculated (Tenenhaus et al. 2005). The average  $R^2$  for the model is 0.202. The calculations of average communality are presented in Table 7. The average communality is 0.7550. The GoF was calculated by taking the geometric mean of 0.202 and 0.7550. GoF for the model is 0.3905. Wetzels et al. (2009) suggests the GoF value should exceed 0.1 for small effect sizes (effect sizes greater than 0.02), 0.25 for medium effect sizes (effect sizes greater than 0.13), and 0.36 for large effect sizes (effect sizes greater than 0.26). The calculated GoF exceeds these cut-offs; therefore, the model performs better than the baseline values.

**Table 7. Calculating Average Communality**

	<i>Communality</i>	<i>p<sub>j</sub></i>	<i>Weighted communality</i>
ISPC	0.8597	3	2.5791
RECO	0.6681	2	1.3362
REFF	0.8891	2	1.7782
RTAR	0.8457	2	1.6914
SDET	0.5733	5	2.8665
SEFF	0.9144	2	1.8288
	<b>p (total)</b>	<b>16</b>	<b>12.0802</b>
<b>Average communality (<math>\Sigma</math>weighted communalities/p)</b>			<b>0.7550</b>

**POST HOC ANALYSIS**

Given that the relationship between self-efficacy and ISP policy compliance intentions was not statistically significant, we examined the link between self-efficacy and

response efficacy. In conducting this test, we used the same structural model used to test the other hypotheses. However, we included a link from self-efficacy to response efficacy. Statistical evidence exists to suggest that self-efficacy affects response efficacy ( $\beta = 0.610$ ;  $p\text{-value} < 0.01$ ). The additional relationship increased the variance explained in response efficacy from 0.142 to 0.477. All other relationships that were statistically significant in the original analysis maintained significance in the ad hoc analysis, except the relationship between self-determination and response efficacy. It may be that self-efficacy is fully or partially mediated by response efficacy for at least some populations.

## DISCUSSION

This study examines control-related motivations and their effect on intentions to comply with ISP. Employee compliance with ISP is an important organizational concern, as employees' security behaviors can negatively affect organizations performance and reputation, and put clients' information at risk (Crossler et al. 2013; Richardson 2009). Control-related motivations are important to the study of behavioral information security research, as they help to explain the internal motivations of employees as they engage with organizational information and IS. In this study, we examine four distinct control-related motivations and their relationships to one another. In particular, we study the effect that self-determination and psychological reactance—two unique and complementary perspectives of autonomy—have on self-efficacy and response efficacy. Though heavily used in other fields, self-determination theory has not been adopted in information security research. Self-determination theory provides an important explanation for internalized behavior and intrinsic motivation. Importantly, researchers and practitioners may need to further explore intrinsically oriented controls, as they may have a greater influence on behavior and behavioral outcomes (Choobineh et al. 2007; Wall et al. 2013a; Wall et al. 2013b). Self-determination theory may provide a useful lens for the future study of intrinsically motivated security behavior. In this study, we show the pertinence of self-determination in security settings.

Through a study of government employees, we find evidence that self-determination increases perceptions of self-efficacy and response efficacy and that psychological reactance decreases perceptions of response efficacy. These are unique findings, as relationships between control-related motivations are not examined in the security research. Understanding how autonomy perceptions affect efficacy perceptions can help managers develop controls that not only attempt to manipulate efficacy directly, but that also improve efficacy by supporting autonomous functioning. Similarly, the findings point to the importance of creating a security environment in which reactive episodes are minimized in order to prevent negative feelings toward security policies and controls. Our study supports prior research on psychological reactance which has found that reactance has negative effects on security behaviors (e.g., Lowry et al. 2010; Posey et al. 2011). However, rather than examining the effect of trait-based reactance on situational conceptualizations of reactance as in Lowry et al. (2010), we show that trait-based reactance influences compliance through other perceptions,

namely efficacy perceptions. Our study helps to extend the nomological network of trait-based reactance.

We did not find strong evidence to suggest that psychological reactance decreases self-efficacy. However, the sign of the path coefficient was as predicted. One explanation is the measurement issues we experienced with the self-determination and psychological reactance scales. Convergent validity was not fully established when the original scales were developed and the scales call for the use of sum scores. However, sum scores should only be used when a scale is shown to have reliability and convergent and discriminant validity. We make an important discovery that both scales suffer from measurement issues that have been hidden due to the nature of their prior assessment and use. Future research should reexamine these scales and consider alternative scales. Interestingly, although originally asserted to be a trait-based phenomenon (Ryan et al. 1985; Ryan et al. 2000), some research suggests that self-determination is only partially trait-based. That is, self-determination is semi-contextualized (Koestner et al. 1996). It may be possible to develop an instrument to measure self-determination that is particular to the study of information security and security contexts. Additionally, other measures of general, trait-based self-determination exist (Pavey et al. 2009).

As in other security studies, we find that response efficacy is an important predictor of security behavior. Evidence continues to suggest that employees are more likely to comply with security policy or security-related messages to the degree they believe compliance will lead to positive outcomes. Response efficacy is shown to increase intrinsic motivation to engage in secure and compliant behavior (Herath et al. 2009a; Vance et al. 2012), increase adoption of security technologies (Johnston et al. 2010), and improve security attitudes (Herath et al. 2009b). This study further confirms the importance of response efficacy in security settings. However, we do not find support to suggest that self-efficacy affects ISP compliance. The sign and general magnitude of the path coefficient was similar to those found in previous research (Herath et al. 2009b; Johnston et al. 2010); however, the t-value in our study was extremely low compared to prior research. Similarly, our findings about the relative influence of self-efficacy and response efficacy match those found by Johnston and Warkentin (2010). That is, the relative strength of the coefficient for response efficacy is greater than that of self-efficacy.

One possibility for our findings about self-efficacy is the nature of the population sampled. Our population consisted of highly educated individuals with a great deal of work experience and long tenure at their organization. Johnston and Warkentin (2010) studied students, faculty, and staff at a university. Thus, demographic factors varied more than in this study. Herath and Rao (Herath et al. 2009b) studied employees and also had a more diverse set of respondents. It is also possible that the participants in our study were so comfortable with their work that self-efficacy was no longer an important differentiating factor. Additionally, we surveyed government employees where other studies have studied students and university and business employees. It may be that the highly procedural and bureaucratic work in government organizations decreases the relative need for self-efficacy. Further, our post hoc analysis suggests

that self-efficacy has a strong relationship with response efficacy. It may be that for certain populations, self-efficacy does not have a direct effect on compliance intentions. These ideas should be explored in future research.

Finally, we find that the certainty of severity of sanctions had no effect on intentions to comply with security policy. In a review of the use of general deterrence theory (GDT) by D'Arcy et al. (2011), they argue that GDT constructs (e.g., certainty and severity of sanctions) may not be useful in exploring positive outcome variables such as compliance. They suggest that GDT is a theory to explain deterrence of rule violations and not to explain motivation to conform to rules. Our results further confirm this assertion.

### **Managerial Implications**

Our findings suggest that managers should be aware of the way employees perceive security-related activities. Further, our results suggest that managers should be concerned not only with employees' perceptions of efficacy, but also with their perceptions of autonomy. Managers who can successfully develop policies and controls that increase self-determination may experience better compliance outcomes. This assertion agrees with security research that suggests that involving employees in the development of security controls improves compliance (Spears et al. 2010). Further, managers should understand that their attempt to control employee's security behaviors may result in reactance which could decrease intentions to engage in secure behaviors. Additionally, this study provides further evidence that attempts to encourage proactive security behaviors may be more influential than punishing noncompliance. We found no support to suggest that perceptions of the certainty and severity of sanctions influence compliance. Managers should develop security controls that promote the internalization of security behaviors. According to self-determination theory, managers may be able to influence the internalization of security behaviors by allowing employees autonomy over their security behaviors.

### **Limitations and Future Research**

Our study has clear limitations. First, the sample size we used to test the hypothesized relationships is not large and response rates were low while attrition rates were high. Although our sample size wasn't large, we were still able to find several interesting relationships. Importantly, our sample size is sufficient for PLS to function properly and smaller sample sizes exist even in the disciplines highest quality journals (Goodhue et al. 2012). Further, despite the low response rate and high attrition rate, responses of early and late responders did not differ statistically. This offers some evidence that the response and attrition rates may not have affected the analysis substantially (Sivo et al. 2006).

Second, we experienced several measurement issues with the instruments for self-determination and psychological reactance. Because of the adjustments we made to the measurement model, namely dropping measurement items, our study is more exploratory than confirmatory. However, the measurement issues are a welcome finding. We are able to highlight potential issues that exist with widely used and influential measurement instruments. Finding measurement issues that have been

taken for granted is important to the progress of research. Future research should seek to better understand the weaknesses in the GCOS and Hong psychological reactance scales. As suggested earlier, there may be an opportunity to develop a contextualized measure of self-determination for the security context or at least for organizational settings.

Third, our model did not link characteristics of security controls with perceptions of autonomy. Although our model provides a better understanding of the relationships between different types of control-related motivations, future research should examine the antecedents of autonomy perceptions. In particular, future studies should examine the autonomy catalyzing aspects of security controls. Such efforts should focus on the dualistic nature of autonomy provided by self-determination theory and psychological reactance theory.

## **CONCLUSION**

Control-related motivations such as autonomy and efficacy are important to information security research. They help to describe why employees engage in secure behaviors. Researchers should continue to examine control-related motivations in security contexts. In particular, researchers should look to self-determination theory to provide insight into intrinsically driven and internalized security behaviors. Research should also continue to study the dualistic nature of autonomy. Managers should be engaged in developing security controls that encourage self-determination while minimizing reactance.

## REFERENCES

- Ajzen, I. 1985. "From intentions to actions: A theory of planned behavior," in *Action control: From cognition to behavior*, J. Kuhl and J. Beckman (eds.), Springer: Heidelberg.
- Bandura, A. 1977a. "Self-efficacy: Toward a unifying theory of behavioral change," *Psychological Review* (84:2), pp 191-215.
- Bandura, A. 1977b. *Social learning theory*, (Prentice Hall: Englewood Cliffs, NJ).
- Bandura, A. 1986. *Social foundations of thought and action: A social cognitive theory*, (Prentice Hall: Englewood Cliffs, NJ).
- Bandura, A. 1997. *Self-efficacy: The Exercise of Control*, (Freeman: New York, NY).
- Biddle, S. J. H. 1999. "Motivation and perceptions of control: Tracing its development and plotting its future in exercise and sport psychology," *Journal of Sport & Exercise Psychology* (21:1), pp 1-23.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, W. R. 2009. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems* (18), pp 151-164.
- Brehm, J. W. 1966. *A theory of psychological reactance*, (Academic Press: London, England).
- Brehm, S. S., and Brehm, J. W. 1981. *Psychological Reactance: A theory of freedom and control*, (Academic Press: London, England).
- Brown, A. R., Finney, S. J., and France, M. K. 2011. "Using the bifactor model to assess the dimensionality of the Hong Psychological Reactance Scale," *Educational and Psychological Measurement* (71:1), pp 170-185.
- 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), pp 523-548.
- Chin, W. W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Business Research Methods*, G. A. Marcoulides (ed.), Lawrence Erlbaum Associates: Mahwah, NJ, pp. 295-336.
- Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. 2007. "Management of information security: Challenges and research directions," *Communication of the Association for Information Systems* (20:1), pp 958-971.
- Cohen, J. 1988. *Statistical power analysis for the behavioral sciences*, (Lawrence Erlbaum Associates: Hillsdale, NJ).
- 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), pp 90-101.
- D'Arcy, J., and 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), pp 643-658.
- Deci, E. L., Eghrari, H., Patrick, B. C., and Leone, D. R. 1994. "Facilitating internalization: The self-determination theory perspective," *Journal of Personality* (62:1), pp 119-142.

- Deci, E. L., Koestner, R., and Ryan, R. M. 1999. "A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation," *Psychological Bulletin* (125:6), pp 627-668.
- Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research: Towards socio-organizational perspectives," *Information Systems Journal* (11:2), pp 127-153.
- Dillard, J. P., and Shen, L. 2005. "On the nature of reactance and its role in persuasive health communication," *Communication Monographs* (72:2), pp 144-168.
- Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*, (Addison-Wesley: Reading, MA).
- Ford, M. T., Cerasoli, C. P., Higgins, J. A., and Decesare, A. L. 2011. "Relationships between psychological, physical, and behavioural health and work performance: A review and meta-analysis," *Work & Stress* (25:3), pp 185-204.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating structural equations models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1), pp 39-50.
- Goodhue, D. L., Lewis, W., and Thompson, R. 2012. "Does PLS have advantages for small sample size or non-normal data?," *MIS Quarterly* (36:3), pp 981-1001.
- Griskevicius, V., Shiota, M. N., and Nowlis, S. M. 2010. "The many shades of rose colored glasses: An evolutionary approach to the influence of different positive emotions," *Journal of Consumer Research* (37:2), pp 238-250.
- Herath, T., and Rao, H. R. 2009a. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:2), pp 154-165.
- Herath, T., and Rao, H. R. 2009b. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18), pp 106-125.
- Hodgins, H. S., Koestner, R., and Duncan, N. 1996. "On the compatibility of autonomy and relatedness," *Personality and Social Psychology Bulletin* (22), pp 227-237.
- Hong, S.-M., and Faedda, S. 1996. "Refinement of the Hong Psychological Reactance Scale," *Educational and Psychological Measurement* (56:1), pp 173-182.
- Hosack, B. 2007. "The effect of system feedback and decision context on value-based decision-making behavior," *Decision Support Systems* (43:4), pp 1605-1614.
- Izuma, K., and Adolphs, R. 2011. "The brain's rose-colored glasses," *Nature Neuroscience* (14:11), pp 1355-1356.
- Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: an empirical study," *MIS Quarterly* (34:3), pp 549-566.
- Ke, W., Tan, C.-H., Sia, C.-L., and Wei, K. K. 2012. "Inducing intrinsic motivation to explore the enterprise system: The supremacy of organizational levers," *Journal of Management Information Systems* (29:3), pp 257-289.
- Ke, W., and Zhang, P. 2010. "The effects of extrinsic motivation and satisfaction in open source software development," *Journal of the Association for Information Systems* (11:12), pp 784-808.



- Koestner, R., Bernieri, F., and Zuckerman, M. 1992. "Self-regulation and between attitudes, traits, and behaviors," *Personality and Social Psychology Bulletin* (18:1), pp 52-59.
- Koestner, R., and Losier, G. F. 1996. "Distinguishing reactive versus reflective autonomy," *Journal of Personality* (64:2), pp 465-494.
- Lee, G., and Lee, W. J. 2009. "Psychological reactance to online recommendation services," *Information & Management* (46:8), pp 448-452.
- Lewinsohn, P. M., Mischel, W., Chaplin, W., and Barton, R. 1980. "Social competence and depression: The role of illusory self-perceptions," *Journal of Abnormal Psychology* (89:2), pp 203-212.
- Liu, D., Li, X., and Santhanam, R. 2013. "Digital games and beyond: What happens when players compete?," *MIS Quarterly* (37:1), pp 111-124.
- Lowry, P. B., Teh, N., Molyneux, B., and Bui, S. N. Year. "Using theories of formal control, mandatoriness, and reactance to explain working professionals' intent to comply with new it security policies," Dewald Roode Workshop on IS Security Research, IFIP WG 8.11 / 11.13, Waltham, MA, 2010, pp. 278-316.
- Murray, K. B., and Häubl, G. 2011. "Freedom of choice, ease of use, and the formation of interface preferences," *MIS Quarterly* (35:4), pp 955-976.
- Myry, L., Siponen, M., Pahlila, S., Vartiainen, T., and Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems* (18:2), pp 126-139.
- Olesen, M. H. 2011. "General causality orientations are distinct from but related to dispositional traits," *Personality and Individual Differences* (51), pp 40-465.
- Olesen, M. H., Thomsen, D. K., Schnieber, A., and Tønnesvang, J. 2010. "Distinguishing general causality orientations from personality traits," *Personality and Individual Differences* (48), pp 538-543.
- Pavey, L., and Sparks, P. 2009. "Reactance, autonomy and paths to persuasion: Examining perceptions of threats to freedom and informational value," *Motivation and Emotion* (33:3), pp 277-290.
- Pavlou, P., 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.
- Pee, L. G., Woon, I. M. Y., and Kankanhalli, A. 2008. "Explaining non-work-related computing in the workplace: A comparison of alternative models," *Information & Management* (45:2), pp 120-130.
- Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. "When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse," *Journal of Information Systems Security* (7:1), pp 24-47.
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. 2013. "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," *MIS Quarterly*).

- Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly* (34:4), pp 757-778.
- Rhee, H., Kim, C., and Ryu, Y. 2009. "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security* (28:8), pp 816-826.
- Richardson, R. 2009. "14th annual CSI computer crime and security survey," Computer Security Institute, pp. 1-14.
- Richardson, R. 2011. "15th Annual 2010/2011 Computer Crime and Security Survey," Computer Security Institute, pp. 1-44.
- Ringle, C. M., Wende, S., and Will, A. 2005. *SmartPLS*, (SmartPLS: Hamburg, Germany).
- Rogers, R. W. 1975. "Protection motivation theory of fear appeals and attitude change," *The Journal of Psychology* (91:1), pp 93-114.
- Ryan, R. M., and Deci, E. L. 1985. *Intrinsic motivation and self-determination in human behavior*, (Plenum Press: New York, NY).
- Ryan, R. M., and Deci, E. L. 2000. "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being," *American Psychologist* (55:1), pp 68-78.
- Schunk, D. H., and Pajares, F. 2005. "Competence Perceptions and Academic Functioning " in *Handbook of Competence and Motivation* A. J. Elliot and C. C. Dweck (eds.), Guilford Press: New York, NY, pp. 85-104.
- Senecal, C., Nouwen, A., and White, D. 2000. "Motivation and dietary self-care in adults with diabetes: Are self-efficacy and autonomous self-regulation complementary or competing constructs?," *Health Psychology* (19:5), pp 452-457.
- Sivo, S. A., Saunders, C., Chang, Q., and Jiang, J. J. 2006. "How low should you go? Low response rates and the validity of inference in IS questionnaire research," *Journal of the Association for Information Systems* (7:6), pp 351-414.
- Spears, J. L., and Barki, H. 2010. "User participation in information systems security risk management," *MIS Quarterly* (34:3), pp 503-522.
- Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., and Lauro, C. 2005. "PLS path modeling," *Computational Statistics & Data Analysis* (48:1), pp 159-205.
- Van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81:5), pp 575-586.
- Vance, A., Siponen, M., and Pahlila, S. 2012. "Motivating IS security compliance: Insights from habit and protection motivation theory," *Information & Management* (49), pp 190-198.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems* (51), pp 576-856.
- Vroom, V. H. 1964. *Work and Motivation*, (Wiley: Oxford, UK).
- Wall, J. D., Iyer, L., Salam, A. F., and Siponen, M. Year. "Conceptualizing employee compliance and noncompliance in information security research: A review

and research agenda. ," Dewald Roode Workshop on IS Security Research, IFIP WG 8.11 / 11.13, Niagara Falls, NY, 2013a.

- Wall, J. D., Palvia, P., and D'Arcy, J. Year. "A review and typology of security-related corruption controls: Setting an agenda for studying the behavioral effects of security countermeasures. ," Dewald Roode Workshop on IS Security Research, IFIP WG 8.11 / 11.13, Niagara Falls, NY, 2013b.
- Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20), pp 267-284.
- Warkentin, M., and Willison, R. 2009. "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems* (18), pp 101-105.
- Wetzels, M., Odekerken-Schöder, G., and Oppen, C. V. 2009. "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration," *MIS Quarterly* (33:1), pp 177-195.
- Willison, R., and Warkentin, M. 2013. "Beyond deterrence: An expanded view of employee computer abuse," *MIS Quarterly* (37:1), pp 1-20.
- Witte, K. 1992. "Putting the fear back into fear appeals: The extended parallel process model," *Communication Monographs* (59), pp 329-349.
- Workman, M., Bommer, W. H., and Straub, D. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24), pp 2799-2816.

## **AUTHOR BIOGRAPHY**

**Jeffrey Wall** is a PhD student in the Bryan School of Business & Economics at the University of North Carolina at Greensboro, USA. Jeff received his MPA from Brigham Young University with a minor in Information Systems and a BA in Speech Communication at the University of Utah. His research interests include IT-related deviance at both the individual and organizational levels and in various contexts, such as employee computer abuse, organizational HIPAA violations, information poaching in supply chains, and cybercrime. He has published research in several IS conferences and workshops, including ICIS and AMCIS.

**Prashant Palvia** is Joe Rosenthal Excellence Professor in the Bryan School of Business & Economics at the University of North Carolina at Greensboro, USA. Dr. Palvia received his Ph.D., MBA and MS from the University of Minnesota and BS from the University of Delhi, India. Professor Palvia is the Editor-in-Chief of *the Journal of Global Information Technology Management*, and is an associate editor for *Information & Management*. His research interests include global information technology management, healthcare IT, organizational issues in IS, inter-organizational systems. He has published 100 journal articles in such outlets as the *MIS Quarterly*, *Decision Sciences*, *Communications of the ACM*, *Communications of the AIS*, *Information & Management*, *Decision Support Systems*, and *ACM Transactions on Database Systems*, and 194 conference articles. Prof. Palvia has co-edited four books on Global Information Technology Management and is the general chair of the annual Global Information Technology Management Association (GITMA) World Conference.

**Dr. Paul Benjamin Lowry** is an Associate Professor of IS at the City University of Hong Kong. He received his Ph.D. in MIS from the University of Arizona. He has published articles in MISQ, JMIS, JAIS, IJHCS, JASIST, ISJ, EJIS, CACM, Information Sciences, DSS, IEEEETSMC, IEEEETPC, SGR, Expert Systems with Applications, Computers & Security, and others. He serves as an AE at MISQ (regular guest), EJIS, I&M, ECRA, CAIS, AIS-THCI, and ISEJ. He has also served as an ICIS track co-chair. His research interests include behavioral information security (e.g., protection motivation, accountability, whistle-blowing, compliance, deception, privacy), human-computer interaction (e.g., trust, culture, intrinsic motivations), e-commerce, and scientometrics of IS research.

**APPENDIX A. RESEARCH INSTRUMENT**

The items for all key constructs, excepting self-determination (SDET), are presented in Table A1. The vignettes and items for the GCOS scale which measures self-determination are available for free at <http://selfdeterminationtheory.org> after registration with the site.

**Table A1. Items For Key Constructs (excepting self-determination)**

Construct	Item	Item statement	Type	Source
Intention to comply with information security policy	ISPC-1	I intend to comply with the requirements of the information security policy of my organization in the future.	First order construct with reflective items.	(Bulgurcu et al. 2010)
	ISPC -2	I intend to protect information and technology resources according to the requirements of the information security policy of my organization in the future.		
	ISPC -3	I intend to carry out my responsibilities prescribed in the information security policy of my organization when I use information and technology in the future.		
Response efficacy	REFF-1	My organization's information security policy works for protection?	First order construct with reflective items.	(Johnston et al. 2010)
	REFF-2	My organization's information security policy is effective for protection?		
Self-efficacy	SEFF-1	I believe that complying with my organization's information security policy will be ease to do?	First order construct with reflective items.	(Johnston et al. 2010)
	SEFF-2	I am able to comply with my organization's information security policy without much effort?		
Reactive autonomy (REAC) emotional response toward	ERTR-1	I become frustrated when I am unable to make free and independent decisions.	Second order construct consisting of first	(Hong et al. 1996)
	ERTR-2	I become angry when my freedom of choice is		

*Issues in Information Security Policy Compliance*

restricted choice (ERTR)		restricted.	order constructs with reflective items.
	ERTR-3	It irritates me when someone points out things which are obvious to me.	
Reactive autonomy (REAC) reactance to compliance (RECO)	RECO-1	Regulations trigger a sense of resistance in me.	
	RECO-2	I find contradicting others stimulating.	
	RECO-3	When something is prohibited, I usually think "that's exactly what I am going to do."	
Reactive autonomy (REAC) resisting influence from others (RIFO)	RIFO-1	I resist the attempts of others to influence me.	
	RIFO-2	It makes me angry when another person is held up as a model for me to follow.	
	RIFO-3	When someone forces me to do something, I feel like doing the opposite.	
Reactive autonomy (REAC) reactance toward advice and recommendations (RTAR)	RTAR-1	I consider advice from others to be an intrusion.	
	RTAR-2	Advice and recommendations induce me to do just the opposite.	