Control-Related Motivations and Information Security Policy Compliance: The Effect of Reflective and Reactive Autonomy

Research-in-Progress

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

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

ABSTRACT

Employees' failures to follow information security policy can be costly to organizations. Organizations implement security controls in order to motivate employees. Many control-related motivations have been explored in information security research (e.g., self-efficacy and behavioral control); however, self-determination has yet to receive attention. Self-determination theory is widely used in other fields to explain intrinsically driven performance. This paper examines the effect self-determination—conceptualized as reflective autonomy, and psychological reactance—conceptualized as reactive autonomy have on employees' intentions to comply with security policy. Reflective and reactive autonomy offer complementary yet opposite conceptualizations of autonomy, offering a more holistic view of control-related motivation. We find that both reflective and reactive autonomy affect information security policy compliance intentions. Reflective autonomy increases and reactive autonomy decreases compliance intentions. Managers should become aware of the way employees view security controls in order to develop controls that maximize reflective autonomy and minimize reactive autonomy in employees.

Keywords

Autonomy, reactance, self-determination, information security, policy compliance.

INTRODUCTION

Information system (IS) security is increasingly important to organizations, as security breaches are costly (Richardson, 2009; Richardson, 2011). Employees are key to maintaining secure IS (Bulgurcu, Cavusoglu and Benbasat, 2010); however, employees are often a weak link in information security (Warkentin and Willison, 2009). 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 and Herath, 2011), while training and education are used to promote positive security behavior (Puhakainen and Siponen, 2010).

IS security research has examined many control-related motivations to understand how employees react to security controls. *Control-related motivations* refer to individuals' perceptions of their ability to execute courses of action given their perceptions of control (Biddle, 1999). Self-efficacy, locus of control, perceived behavioral control, and self-determination offer different ways to conceptualize control-related motivation (Biddle, 1999). Additionally, psychological reactance captures control-related demotivation (Brehm and Brehm, 1981). Many of these constructs have been studied in information security research, including: self-efficacy (e.g., Warkentin, Johnston and Shropshire, 2011), behavioral control (e.g., Pee, Woon and Kankanhalli, 2008), locus of control (e.g., Workman, Bommer and Straub, 2008), and psychological reactance (e.g., Posey, Bennett, Roberts and Lowry, 2011). Self-determination, however, has not received attention in information security literature. Importantly, self-determination may be a better representation of control-related motivation than other constructs (Biddle, 1999). Additionally, self-determination and psychological reactance—referred to in this study as reflective and reactive autonomy respectively—are viewed as complementary and somewhat opposite views of control-related motivation (Koestner and Losier, 1996; Pavey and Sparks, 2009). Together, therefore, reflective and reactive autonomy offer a more complete view of control-related motivation than other constructs alone.

Reflective autonomy refers to an individual's belief that his/her actions are self-guided through considerate thought and reflection (Pavey et al., 2009). Reflective autonomy is akin to self-determination in self-determination theory. Self-determination theory (Ryan and Deci, 1985; Ryan and Deci, 2000) states that self-determination leads to increased intrinsic

motivation to accomplish tasks. Conversely, *reactive autonomy* refers to an individual's belief in his/her right to freedom from external restriction (Pavey et al., 2009). Reactive autonomy is akin to reactance in psychological reactance theory. 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 (Brehm et al., 1981). Information security studies have failed to capture the dualistic nature of autonomy—as captured by reflective and reactive autonomy. We seek to bridge this gap by examining reactive and reflective autonomy and their effect on employee security behaviors. In particular, we seek to explain and predict the effect that employees' perceptions of autonomy have on their intentions to comply with information security policy. We ask: *do reflective and reactive autonomy affect employee's information security policy compliance intentions?*

This study has the potential to offer several important contributions to IS security research. First, we introduce self-determination theory to IS security research. Self-determination theory has been important to other fields in explaining individual's intrinsic drive to engage in various tasks (Koestner et al., 1996). Information security compliance requires proactive effort to be efficacious (Choobineh, Dhillon, Grimaila and Rees, 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. This paper, therefore, offers a more complete conceptual understanding of the effect of autonomy on employees' information security behaviors than prior studies. IT and security managers can use the findings in this paper to assist in developing security controls that encourage reflective autonomy and discourage reactive autonomy.

The remainder of this paper will continue as follows. First, a review of IS security literature is given with a focus on control-related motivations. Second, a conceptual model is presented. Third, the survey methodology used to test the model is described. Fourth, the results of the survey are analyzed. Lastly, a discussion of the results and their implications for researchers and managers is offered.

LITERATURE REVIEW

Behavioral information security research seeks to explain and predict employees' compliance with information security policy. Many studies explore the direct effect of security controls on employees' compliance or compliance intentions. Herath and Rao (2009a), for example, examine the direct effect of penalties on employees policy compliance intentions. Siponen and Vance (2010) explore the direct effect of formal and informal sanctions on intentions to violate information security policy. Similarly, Vance et al. (2012) examine the effect that sanctions and rewards have on compliance intentions. Although these studies offer value, mediated models may offer better tests of theoretical explanations linking security controls with compliance. Many studies examine control-related motivations as covariates. Self-efficacy is a common covariate in information security research (e.g., Boss, Kirsch, Angermeier, Shingler and Boss, 2009; Bulgurcu et al., 2010; Herath and Rao, 2009b). Behavioral control (e.g., Pee et al., 2008) and locus of control (e.g., Workman et al., 2008) have also been studied.

Other studies examine mediated models that directly test explanations of why security controls affect compliance. Few studies, however, examine control-related motivations as mediating factors. Mediating factors include attitude (e.g., Bulgurcu et al., 2010; Herath et al., 2009b), persuasion (Puhakainen et al., 2010) and punishment expectancy (Xue, Liang and Wu, 2011). Warkentin et al. (2011) is one of the few studies to examine control-related motivations as a mediator. They find that self-efficacy mediates the relationship between security controls and compliance. Posey et al. (2011) discuss the mediating role of reactance in security settings, though they do not empirically test its mediating role. Additionally, Boss et al. (2009) find that the perceived mandatoriness of security policy mediating factor. Mandatoriness—"the degree to which individuals perceive that compliance… is compulsory or expected" (p. 151)—could be considered a control-related motivation as it focuses on perceptions of organizational control. It is likely, however, that mandatoriness is mediated further by reactive autonomy, as individuals with high reactive autonomy experience reactance to compulsion and expectations (Brehm et al., 1981; Dillard and Shen, 2005; Hong and Faedda, 1996). Importantly, control-related motivations have provided important explanations for the link between controls and compliance in other fields (e.g, Dillard et al., 2005).

Finally, some security studies do not directly examine security controls. Rather, these studies provide rationale for individuals' security behaviors. For example, Myyry et al. (2009) examine the effect that moral reasoning and values have on hypothetical and actual policy compliance. Given that reflective and reactive autonomy are conceptualized as relatively stable personality traits (Brehm et al., 1981; Ryan et al., 1985), we adopt the approach of Myyry et al. (2009). The purpose of this paper, therefore, is to establish the salience of autonomy and its duality, and to introduce self-determination theory to information security research.

AUTONOMY AND INFORMATION SECURITY COMPLIANCE

Reflective and reactive autonomy have been studied extensively in other fields. Although reactive autonomy has recently received attention in security research (e.g., Posey et al., 2011), reflective autonomy has yet to be explored. The model in this paper seeks to combine these two conceptualizations of autonomy to explain and predict information security policy compliance intentions. Figure 1 presents the model examined in this paper. The primary purpose of this paper is to introduce reflective and reactive autonomy to IS security research.

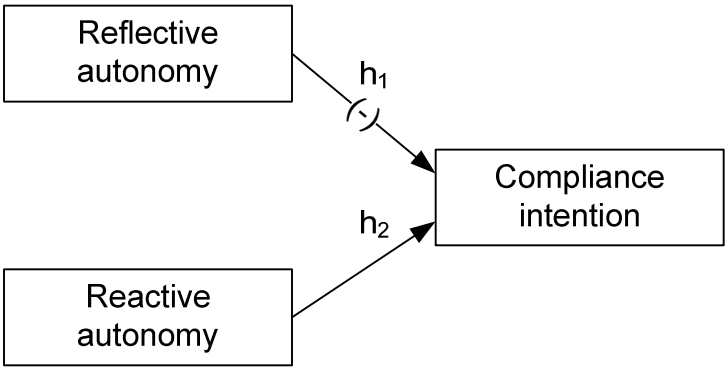

Figure 1. Conceptual Model

Reflective Autonomy

Reflective autonomy is derived from self-determination theory (Koestner et al., 1996; Pavey et al., 2009). Self-determination theory (Ryan et al., 1985; Ryan et al., 2000) suggests that individuals behavior is driven by three psychological needs—competence, relatedness, and autonomy. Competence refers to individuals' needs and attempts "to control outcomes and experience effectance" (p. 243). Relatedness refers to individuals' needs and strivings to "relate to and care for others, to feel that those others are relating authentically to oneself, and to feel a satisfying and coherent involvement with the social world more generally" (p. 243). And autonomy refers to individuals' needs and strivings "to be agentic, to feel like the origin of their actions, and to have a voice or input into determining their own behavior" (p. 243). Self-determination theory captures control-related motivations with three orientations—autonomous, control-determined, and impersonal functioning (Ryan et al., 1985). Reflective autonomy is best represented by the autonomous orientation. Given that the focus of this paper is autonomy, the other two orientations are not important to the discussion in this paper.

Research on reflective autonomy suggests that autonomy increases initiative, persistence, psychological well-being, optimism, and behavioral consistency (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 reflective autonomy 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) rather than complete the activity to avoid sanctions. Based on the above discussion, we propose:

Hypothesis 1: An increase in reflective autonomy will increase information security policy compliance.

Reactive Autonomy

Reactive autonomy is derived from psychological reactance theory (Brehm, 1966; Brehm et al., 1981) and other theories that conceptualize autonomy as freedom from governance (Koestner et al., 1996; Pavey et al., 2009). Reactance theory is based on the premise that individuals desire to be free from the control of others. It also asserts that individuals will strive to restore freedoms which they perceive as threatened by external control. The attempt to restore freedom is referred to as reactance. Reactive autonomy is conceptualized as being a stable personality trait (Brehm et al., 1981; Koestner et al., 1996). Reactive autonomy as conceptualized by psychological 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 to compliance refers to negative reactions toward complying with other's demands. Given that the focus of this study is security compliance intentions, we are most interested in reactance to compliance.

Reactance is associated with decreased self-esteem, life satisfaction, religiosity, and locus of control and increased trait anger and depression (Hong et al., 1996). In addition to these maladapted feelings, reactive autonomy has been shown to affect behavior. Reactance has also been shown to affect compliance with health regimens (Dillard et al., 2005) and may be related to noncompliance in other situations (Brown, Finney and France, 2011). 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. Based on the above discussion, we propose:

Hypothesis 2: An increase in reactive autonomy will decrease information security policy compliance.

METHODOLOGY

To test the model, an online survey was distributed to municipal government employees in the United States (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. Municipalities with a population greater than 5,000 citizens were randomly sampled. After the random selection process, employee emails were taken from the websites of the 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 U.S.

Measures

The survey consisted of measures for reflective and reactive autonomy, information security policy compliance intentions, and demographic factors, including: age, level of education, gender, job tenure, and the size of the organization where the employee worked. Measures of reflective autonomy were borrowed from the General Causality Orientations Scale (GCOS) (Hodgins, Koestner and Duncan, 1996). Only the autonomy orientation measures were used from the GCOS scale, as they measure reflective autonomy. Measures of reactive autonomy were borrowed from (Hong et al., 1996). Since the outcome variable of this paper is compliance, we only used measures of reactive autonomy that capture reactance to compliance. We were not concerned with resistance to influence and persuasion, other manifestations of reactive autonomy (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.

In the pilot and full studies, the measures for reflective autonomy displayed acceptable levels of Cronbach's alpha; however, they also displayed levels of average variance extracted (AVE) well below the 0.50 cutoff (Chin, 1998; Fornell and Larcker, 1981). Loadings were extremely low for several of the items. Items with low loadings were 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 reflective autonomy. Many studies that use the GCOS scale treat the measures as a single combined score; therefore, the convergent validity of the scale is not well tested. This study employed partial least squares (PLS) with SmartPLS (version 2.0); therefore, we were able to test for convergent validity using AVE. Our findings about the low AVE values suggest that further development of the GCOS scale may be necessary. This is important as the GCOS scale is widely used.

Participants

The survey response rate was less than 5 percent. 72 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, Saunders, Chang and Jiang, 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. Attrition rates were high. Many respondents failed to answer a significant number of the survey questions; therefore, we dropped them from further analysis. 31 responses were used in the final test. Due to the low response rate and high attrition rate, differences between early and late responders were tested for all variables. t-tests of early and late responders offer a reasonable test for response bias (Sivo et al., 2006). A difference was found between one of the measures for security policy compliance intention ($p = 0.039$). However, given that no difference existed in 2 of the 3 measures of compliance and the difference was not of practical significance (early responder average = 6.0 and late responder average = 6.8), we conclude that response bias is not a major issue.

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 50 percent of the respondents had earned at least a Master's Degree. 93.5 percent of the respondents worked in non-IT positions. Additionally, 96.8 percent of the respondents had more than 10 years of work experience, and 51.6 percent had a tenure greater than 10 years. Nearly an equal number of males and females responded to the survey, 51.6 and 48.4 percent respectively. Most of the respondents, nearly 75 percent, were over the age of 45. Table 1

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. It appears that emails posted on municipal government websites may be for senior employees.

Demographic Item		Count	Percent
Age	18-25	0	0.0
	26-35	3	10.0
	36-45	5	16.7
	46-55	9	30.0
	56-65	12	40.0
	65+	1	3.3
Gender	Male	16	51.6
	Female	15	48.4
Education	High school	3	9.7
	Associate's Degree	2	6.5
	Bachelor's Degree	9	29.0
	Master's Degree	15	48.4
	Doctoral/Professional Degree	1	3.2
Position	IT	2	6.5
	Non-IT	29	93.5
Total work experience	1-3 years	0	0.0
	4-6 years	0	0.0
	7-9 years	1	3.2
	10+ years	30	96.8
Tenure at organization	1-3 years	5	16.1
	4-6 years	8	25.8
	7-9 years	2	6.5
	10+ years	16	51.6

Table 1. Demographic Data of Respondents

RESULTS

Data was analyzed with PLS using SmartPLS (version 2.0). PLS was used for its ability to handle small sample sizes (Wetzels, Odekerken-Schöder and Oppen, 2009). Despite the small sample size, we found strong support for a link between autonomy and policy compliance.

Measurement Model

Overall, the measurement model showed high reliability. Composite reliabilities were greater than 0.85, 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 2.

	AVE	Composite reliability
ISPC (information security policy compliance intention)	0.882	0.957

REAA (reactive autonomy)	0.657	0.851
REFA (reflective autonomy)	0.659	0.905

Table 2. AVE and Composite Reliability for First Order Constructs

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). Indicators loaded highly on their associated factors; all but one loading exceeded the 0.70 cutoff (Fornell et al., 1981). REFA3 loaded at 0.694. In all cases, item loadings were higher than cross loadings. Table 3 shows the factor loadings and cross loadings.

	ISPC	REAA	REFA
ISPC1	**0.953**	-0.609	0.512
ISPC2	**0.892**	-0.591	0.216
ISPC3	**0.971**	-0.561	0.468
REAA1	-0.462	**0.717**	-0.136
REAA2	-0.453	**0.807**	-0.213
REAA3	-0.589	**0.898**	-0.333
REFA1	0.332	-0.170	**0.793**
REFA2	0.401	-0.277	**0.823**
REFA3	0.189	-0.118	**0.694**
REFA4	0.265	-0.210	**0.791**
REFA5	0.471	-0.326	**0.938**

Table 3. 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 4 shows latent variable correlations with the square root of AVE on the diagonals. Based on the above 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, Liang and Xue, 2007). The highest correlation was 0.625. Therefore, there is some evidence that common method bias is not an issue.

	ISPC	REAA	REFA
ISPC	**0.939**		
REAA	-0.625	**0.811**	
REFA	0.435	-0.290	**0.812**

Table 4. Latent Variable Correlations with Square Root of AVE on Diagonals

Structural Model

Support was found for the relationships proposed in the model. Figure 2 presents the results of the PLS analysis. Controlling for demographic factors, convincing evidence exists to suggest that an increase in reflective autonomy increases information security policy compliance intentions ($\beta = 0.429$; p-value < 0.01). Thus, we found support for hypothesis 1. Controlling for demographic factors, convincing evidence also exists to suggest that an increase in reactive autonomy decreases information security policy compliance intentions ($\beta = -0.549$; p-value < 0.01). Therefore, we found support for hypothesis 2. In total the model accounts for 55 percent of the variance in compliance intentions. Excluding demographic factors, reflective and

reactive autonomy accounted for 46.1 percent of the variance in compliance intentions. All control variables were statistically insignificant.

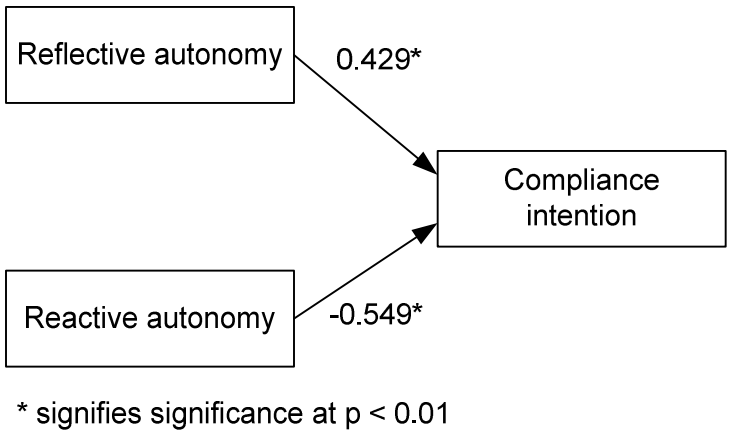

Figure 2. Results of PLS Analysis

Post-hoc Analysis

In addition to controlling for demographic factors as described above, we also examined the effect of demographic factors on reflective and reactive autonomy. Convincing evidence exists to suggest that job tenure is related to reflective autonomy (β = -0.492; p-value < 0.01). An increase in job tenure is associated with a decrease in reflective autonomy. No other significant effects were found amongst the demographic control variables.

DISCUSSION

This study examines the duality of autonomy in an information security setting. In particular, we examine the effect that reflective and reactive autonomy—two complementary and opposite conceptualizations of autonomy—have on government employees' intentions to comply with information security policy. We find evidence that both reflective and reactive autonomy affect employees' compliance intentions. As predicted, reflective autonomy has a positive relationship with compliance intentions and reactive autonomy has a negative relationship. The model provides evidence that autonomy may be an important factor in behavioral information security research. It is important to note that the study consisted of mostly well-educated senior government employees. The generalizability of these findings should be corroborated, therefore, through further study.

Path coefficients provide simplistic evidence that reactive autonomy may be a more powerful predictor of compliance intentions than reflective autonomy. Koestner and Losier (1996) find similar results for requests issued by authority figures. Pavey and Sparks (2009) also find higher coefficients for reactive autonomy. However, Koestner and Losier (1996) find that reflective autonomy is more influential than reactive autonomy when considering peers requests. Future security studies could further examine this phenomenon by comparing the effect of informal and formal security controls on autonomy.

Finally, we find certain deficiencies in the GCOS scale. The GCOS scale is a widely used and accepted measurement instrument (Koestner et al., 1996). In this study, the GCOS scale demonstrated low levels of AVE. Although we only used measures of the autonomy orientation, we collected responses based on the full GCOS instrument. We conducted a small post-hoc analysis and found that the competence and relatedness dimension also display values of AVE well below the 0.50 cutoff. This suggests that further refinement of the scale may be necessary.

Managerial Implications

These findings suggest that managers should be aware of the way employees perceive security-related activities. 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. Managers should develop security controls that promote the internalization of security behaviors and allow employees the autonomy to secure their systems.

Limitations and Future Research

Future research should examine the antecedents of autonomy, particularly reflective autonomy. Reflective autonomy, though conceptualized as a fairly stable trait (Ryan et al., 1985), may be affected by situational factors (Koestner et al., 1996). Given the semi-contextual nature of reflective autonomy, future studies might also seek to develop an instrument that measures reflective autonomy in a security setting. The GCOS instrument is designed to capture responses to a variety of activities. Additionally, in future research we will examine the way different security controls might influence reflective and reactive autonomy. Based on reactance theory and self-determination theory, coercive controls may elicit higher levels of reactive autonomy and lower levels of reflective autonomy, while controls that focus on education and informed action may elicit higher levels of reflective autonomy. This should be studied in future research. Thus, autonomy would act as a mediating variable between perceptions of controls and compliance.

Future research should also seek to reexamine the psychometric properties of the GCOS instrument (Ryan et al., 1985). By treating the instrument as a scale, previous studies have ignored convergent and discriminant validity. In this study we find that the instrument demonstrates low AVE scores, suggesting that convergent validity may be weak. It may be that each orientation in the GCOS has sub-dimensions. We acknowledge, however, that our sample size is small and that PLS has certain measurement deficiencies as compared to covariance-based structural equation modeling (Goodhue, Lewis and Thompson, 2012). Still, these findings cast doubt into the use of the GCOS instrument as a set of averaged scores. With the advances in statistical tools, it is important to test scales that are assumed to possess convergent and discriminant validity.

CONCLUSION

Control-related motivations such as autonomy 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 continue to examine self-determination theory and the duality that exists between reflective and reactive autonomy. Developing security controls that encourage reflective autonomy while minimizing reactance is an important endeavor for managers.

REFERENCES

1. 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, 1-23.
2. 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: manditoriness, control, and information security, *European Journal of Information Systems* 18, 151-164.
3. Brehm, J. W. (1966) *A theory of psychological reactance*, (Academic Press: London, England.
4. Brehm, S. S., and Brehm, J. W. (1981) *Psychological Reactance: A theory of freedom and control*, (Academic Press: London, England.
5. 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, 170-185.
6. 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, 523-548.
7. 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, 295-336.
8. 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, 958-971.
9. 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, 643-658.
10. 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, 119-142.
11. Dillard, J. P., and Shen, L. (2005) On the nature of reactance and its role in persuasive health communication, *Communication Monographs* 72, 2, 144-168.
12. Fornell, C., and Larcker, D. F. (1981) Evaluating structural equations models with unobservable variables and measurement error, *Journal of Marketing Research* 18, 1, 39-50.
13. 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, 981-1001.

14. 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, 154-165.
15. 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, 106-125.
16. Hodgins, H. S., Koestner, R., and Duncan, N. (1996) On the compatibility of autonomy and relatedness, *Personality and Social Psychology Bulletin* 22, 227-237.
17. Hong, S.-M., and Faedda, S. (1996) Refinement of the Hong Psychological Reactance Scale, *Educational and Psychological Measurement* 56, 1, 173-182.
18. Koestner, R., Bernieri, F., and Zuckerman, M. (1992) Self-regulation and between attitudes, traits, and behaviors, *Personality and Social Psychology Bulletin* 18, 1, 52-59.
19. Koestner, R., and Losier, G. F. (1996) Distinguishing reactive versus reflective autonomy, *Journal of Personality* 64, 2, 465-494.
20. Myyry, L., Siponen, M., Pahnila, 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, 126–139.
21. 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, 277-290.
22. Pavlou, P., Liang, H., and Xue, Y. (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective, *MIS Quarterly* 31, 1, 105-136.
23. 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, 120-130.
24. 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, 24-47.
25. Puhakainen, P., and Siponen, M. (2010) Improving employees' compliance through information systems security training: an action research study, *MIS Quarterly* 34, 4, 757-778.
26. Richardson, R. (2009) 14th annual CSI computer crime and security survey, Computer Security Institute, 1-14.
27. Richardson, R. (2011) 15th Annual 2010/2011 Computer Crime and Security Survey, Computer Security Institute, 1-44.
28. Ryan, R. M., and Deci, E. L. (1985) *Intrinsic motivation and self-determination in human behavior*, (Plenum Press: New York, NY.
29. 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, 68-78.
30. Siponen, M., and Vance, A. (2010) Neutralization: new insights into the problem of employee information systems security policy violations, *MIS Quarterly* 34, 3, 487-502.
31. 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, 351-414.
32. Vance, A., Siponen, M., and Pahnila, S. (2012) Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management* 49, 190-198.
33. 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, 267-284.
34. Warkentin, M., and Willison, R. (2009) Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems* 18, 101-105.
35. 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, 177-195.
36. 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, 2799-2816.
37. Xue, Y., Liang, H., and Wu, L. (2011) Punishment, justice, and compliance in mandatory IT settings, *Information Systems Research* 22, 2, 400-414.