



Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness

Alex Koohang, Alojzy Nowak, Joanna Paliszkievicz & Jeretta Horn Nord

To cite this article: Alex Koohang, Alojzy Nowak, Joanna Paliszkievicz & Jeretta Horn Nord (2020) Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness, Journal of Computer Information Systems, 60:1, 1-8, DOI: [10.1080/08874417.2019.1668738](https://doi.org/10.1080/08874417.2019.1668738)

To link to this article: <https://doi.org/10.1080/08874417.2019.1668738>



Published online: 19 Dec 2019.



Submit your article to this journal [↗](#)




View related articles [↗](#)



View Crossmark data [↗](#)



Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness

Alex Koohang^a, Alojzy Nowak^b, Joanna Paliszkievicz^c, and Jeretta Horn Nord ^d

^aMiddle Georgia State University, Macon, GA, USA; ^bUniversity of Warsaw, Warsaw, Poland; ^cWarsaw University of Life Sciences – SGGW, Warsaw, Poland; ^dUniversity of Oklahoma, Stillwater, OK, USA

ABSTRACT

The purpose of this study was to find out which one of the four selected predictor variables, i.e., leadership, trusting beliefs, role values, and information security policy awareness are most influential in predicting employees' intention to comply with organizational information security policy. An instrument with five constructs was administered to subjects from a higher-education university in the USA. Collected data were methodically examined through multiple regression analysis. Results indicated that all four predictor variables were influential in predicting employees' intention to comply with organizational information security policy requirements. Implications of the findings are discussed and recommendations for future research are made.

KEYWORDS

Information security policy; compliance; leadership; trust; role values; awareness

Introduction

Information system vulnerability (i.e., OS command injection, SQL injection, buffer overflow, missing authorization, unrestricted upload of dangerous file types, reliance on untrusted inputs in a security decision, download of codes without integrity checks, weak passwords, and software infected with the virus among others) is the “... weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (see ref. 1, p. 87).” Information security threats are malware, phishing, proxies, spyware, adware, botnets, and spam among others. Information security threats are defined as “... any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (see ref. 1, pp. 85–86).”

Information system vulnerability is present when employees do not comply with the organizations' information security policy (ISP) requirements, therefore, placing organizational resources at risk.² ISP is described as “... a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations (see ref. 3, p. 434).” Furthermore, ISP is defined as the “... aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information (see ref. 1, p. 26).” Ifinedo⁴ referred to ISP as guidelines, requirements, and rules prescribed by organizations to aim at employees' behaviors, thus improving information security

policy compliance. User behavior, i.e., activities that employees perform to ensure the protection of an organization's assets against threats becomes vital in ISP compliance.⁵

The literature has documented that ISP compliance protects and safeguard organizations' resources from potential security threats and breaches.^{2,6,7} Kim and Yong⁸ referred to compliance as the employee's willingness to execute the ISP requirements of the organization.

ISP compliance models have been the focus of numerous studies.^{2,8–15} These studies draw from various theories, for example, the theory of planned behavior¹⁶, the theory of protection motivation¹⁷, formal/informal theories that include severity and certainty¹⁸ among others to study variables that influence ISP compliance. For example, drawing from the planned behavior theory, the variables of self-efficacy, attitude, benefit of compliance, cost of compliance/noncompliance, vulnerability of resources, sanctions, awareness, etc. were explored to find out about employees' ISP compliance related to rationality-based beliefs and information security awareness.²

Other variables that have shown to explain employees' intention to comply with ISP are attitude², avoidance¹⁹, fear¹³, habits¹³, reactance³, and self-efficacy^{2,20}. In the meanwhile, there are variables such as organizational leadership, employees' trusting beliefs, and role values that have been given little attention in the literature when explaining employees' intention to comply with ISP. In the present study, we build a prediction model and choose these variables as the predictor variables. We chose organizational leadership and trusting beliefs variables because little research has been conducted relating to these variables and employees' information security compliance.²¹ We chose role values because this is the newest proposed construct¹³ as a part of a unified model of

ISP compliance which integrated variables from across eleven theories presented in previous research. The authors indicated that this new construct may be the most significant variable in explaining ISP compliance within organizations. In the model, we also include IS awareness as a predictor variable because of its importance as a determinant factor of ISP compliance.^{10,22} We will then seek to find out which four predictor variables are influential in predicting employees' ISP compliance – intention to comply with organizational ISP. Therefore, we ask the following research questions:

Which of the four predictor variables (leadership, trusting beliefs, role values, and ISP awareness) are most influential in predicting employees' intention to comply with organizational ISP?

Are there any predictor variables (leadership, trusting beliefs, role values, and ISP awareness) that do not contribute significantly to the prediction model?

Review of literature

Leadership

Leadership is defined as “... the process of interactive influence that occurs when, in a given context, some people accept someone as their leader to achieve common goals” (see ref. 23, p. 3). Northouse²⁴ stated that leadership is about bringing people together to carry out common goals. Yukl (see ref. 25, p. 2) described leadership as “... a group process that involves interaction between at least two persons in pursuit of a goal.” In the context of ISP, researchers have confirmed that leadership is one of the most critical elements that positively influence employees' compliance with ISP requirements and in turn protects the organizational resources.^{2,18,21,26–32}

Scholars agree that information security should be viewed as a top strategic priority in organizations and that commitment from top management supports the effective enforcement of ISP requirements.^{33,34}

Leaders should be able to persuade, inspire, and motivate employees to comply with ISP requirements.³⁵ To effectively lead employees to comply with the information security policy requirements within organizations, leaders should create and guide a strong information security culture to protect resources against security threats.²

Researchers have studied various factors that leaders are responsible for influencing employees' intention to comply with the ISP requirements. For example, organizational culture³⁶, threat perceptions about the severity of breaches and resource availability³⁷, the use of rewards to motivate compliance², regulatory requirements, employee competence, commitment, ethical values, personality, values, attitude and motivation⁵, employees' perceived severity, vulnerability, self-efficacy, normative beliefs and attitude.³⁸

Trust

Trust has been viewed as an imperative element for organizational success.³⁹ There are many activities, traits, and attributes in organizations that are influenced by trust, e.g., inter-organizational cooperation⁴⁰, team performance^{41,42}; reducing costs and improving ability to handle complexity^{43,44}, long-term relationships^{45,46},

effective implementation of strategies⁴⁷, environmental uncertainty, i.e., when a firm faces disruptive changes in technology^{44,48}, sharing of knowledge^{49,50}, knowledge creation⁵¹, and organizational performance.^{52,53}

Researchers have found that individuals' perceptions about the security features of technology lead to their trust in technology.^{20,54} In addition, a higher level of trust in technology is linked to a better quality of security decisions that are made by employees.⁵⁵

While trust in relation to ISP has not been researched widely, there are studies that have linked the existence of trust with ISP awareness, employee participation, and compliance.^{56,57} From an economic point of view, scholars argue that building trust into security systems is a necessity for any organization^{58,59} and that trust-based information security protects organizations from security threats.⁶⁰ Several studies have looked at positive relation between trust and leadership in terms of employee's intention to comply with the ISP requirements.^{21,53,61}

Role value

Role value as a new construct was proposed by Moody, Siponen, & Pahnila.¹³ The authors defined role values as the requirements within the ISP guidelines that are viewed as suitable and acceptable which are associated with the nature of the work individuals perform. The role values are comprised of nine factors from four constructs previously explored in the literature. These constructs are taken from various behavioral theories such as the control balanced theory⁶², the extended parallel processing model⁶³, and the theory of interpersonal behavior.⁶⁴ The four constructs are self-concept⁶⁵, roles⁶⁶, perceived behavioral control²⁰, affect⁶⁷, and moral definitions.⁷

The variables of self-concept construct are 1) one's feeling guilty from not complying, 2) consistency with one's principles to comply, and 3) one's view of accepting to walk away from complying.⁶⁵ The variables of role construct include 1) one's understanding that complying is one's work style and 2) one's zero justification for defying compliance.⁶⁶ The variable from the perceived behavioral control construct includes one's having control over breaking the compliance policy.²⁰ The variables of affect construct are 1) one's understanding of not being smart to violate the organization's ISP and 2) one's understanding of not being pleasing to violate the organization's ISP.⁶⁷ Finally, the moral definitions construct with one variable indicates that it is morally wrong to violate the organization's ISP.⁷ All these variables collectively make up the role values construct. Moody, Siponen, & Pahnila¹³ asserted that role values were the most significant justification for ISP compliance.

Awareness

Scholars agree that information security awareness is a determinant variable of ISP compliance.^{2,10,22,68–70} Information security awareness as “... the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient

levels of information security control.⁷¹ Siponen (see ref. 72, p. 31) defined information security awareness as “... a state where users in an organization are aware of – ideally committed to – their security mission (often expressed as end-user security guidelines).” The ISP awareness is defined as “... an employee’s knowledge and understanding of the requirements prescribed in the organization’s ISP and the aims of those requirements (see ref. 2, p. 532).”

Information security awareness is a vital part of a practical and efficient information security management program.² For example, Lee and Lee⁷³ stated that in organizations, information security awareness programs prevent computer abuse. ISP awareness has been linked to increased positive attitudes among employees.⁷⁴ Box and Pottas⁷⁵ linked the positive influence of awareness to information security behavior. Information security awareness impacts an employee’s attitude to comply with the ISP, directly and indirectly, therefore, safeguarding information security within organizations.²

Methodology

Instrument

The instrument used for the present study consisted of five constructs. They are leadership, trusting beliefs, role values, ISP awareness, and compliance (intention to comply).

Leadership construct

The leadership construct was originally designed by Hu et al. [2012] and modified by Paliszkiwicz.²¹ This construct defines the role of leadership in 1) articulating a clear vision about the ISP, 2) formulating a clear strategy for achieving effective ISP, and 3) establishing clear goals/objectives for attaining effective ISP to protect the organization’s assets against threats. The items of this construct are as follows.

- Leadership in my organization has articulated a clear vision of the ISP to protect the organization’s assets against threats.
- Leadership in my organization has formulated a clear strategy for achieving effective ISP to protect the organization’s assets against threats.
- Leadership in my organization has established clear goals and objectives for attaining effective ISP to protect the organization’s assets against threats.

Trusting beliefs construct

The trusting beliefs construct was modified from a study conducted by Paliszkiwicz.²¹ This construct is about employee’s trusting beliefs (i.e., competence, benevolence, and integrity) related to all aspects of the ISP requirements. The items of this construct are as follows.

- My organization has the skills and knowledge to effectively implement ISP requirements.
- My organization’s ISP requirements are meant for the best interest of the organization and employees.
- My organization fulfills its promises and commitments related to all aspects of the ISP requirements.

Role values construct

The role values construct was proposed by Moody, Siponen, & Pahlila.¹³ The role values construct is the requirements within the ISP guidelines that are viewed as justified and appropriate which are associated with the nature of the work individuals perform. This construct includes nine items.

- I would feel guilty if I don’t comply with ISP (i.e., sharing my password with a coworker, etc.)
- It is consistent with my principles to comply with my organization’s ISP.
- It is never acceptable to me to walk away from complying with my organization’s ISP.
- Complying with my organization’s ISP is my work style.
- I cannot justify defying compliance with my organization’s ISP.
- I feel that I am in control of either accepting or breaking the information security compliance policy in my organization.
- It is not smart to violate my organization’s ISP (i.e., sharing my password with a coworker, etc.)
- I don’t find it pleasing to violate my organization’s ISP.
- I think it is morally wrong to violate my organization’s ISP.

ISP awareness construct

The information security awareness construct was developed by Bulgurcu et al.² This construct is about employees’ awareness about rules and regulations of the ISP requirements. It also includes employees’ understanding of their responsibilities regarding the ISP requirements. The items of this construct are as follows.

- I know the rules and regulations prescribed by the ISP of my organization.
- I understand the rules and regulations prescribed by the ISP of my organization.
- I know my responsibilities as prescribed in the ISP to enhance the security of my organization.

Intention to comply – ISP compliance construct

Intention to comply – ISP compliance construct was originally designed by Ajzen¹⁶ and modified by Bulgurcu et al.² This construct is about employees’ intention to comply with the requirements of the ISP. The items of this construct are as follows.

- I intend to comply with the requirements of the ISP of my organization.
- I intend to protect information and technology resources according to the requirements of the ISP of my organization.
- I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology.

The Likert-type instrument contained the following scoring strategy: 7 = completely agree, 6 = mostly agree, 5 = somewhat

agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, 1 = completely disagree.

Subjects and procedure

We electronically administered the survey instrument to 1472 employees of a university in the USA (758 faculty members and 714 staff members) after receiving approval from the university's institutional research board (IRB). On the consent form, we explained the purpose of the survey instrument and emphasized that completing it would be voluntary. The subjects were guaranteed confidentiality in regard to the findings of the study. After two weeks, we received 257 responses. Next, we examined the completeness of the responses. As a result, we eliminated 20 incomplete surveys. This yielded 237 completed surveys resulting in a response rate of 16%.

Data analysis

Using SPSS™ version 25, we chose multiple regression analysis, the *Enter* method to analyze the data. The *Enter* method enters all independent variables in the model one by one regardless of their significant contribution. The analysis shows which of the independent variables can best predict the dependent variable. According to Stevens⁷⁶, multiple regression analysis encompasses a few procedures. First, the data is analyzed to see if multicollinearity among the independent variables exists. The presence of multicollinearity among independent variables limits the size of R, it undermines individual effects caused by overlapping information, and it tends to raise the variances of the regression coefficients resulting in unreliable prediction equation.⁷⁶ The tolerance level and the variance inflation factor (VIF) determine the existence or nonexistence of multicollinearity among the independent variables in the model. The nonexistence of multicollinearity is determined when the tolerance level values for all independent variables are above .1 and the VIF values for all independent variables are below 10.

Second, the model fit is determined by the values of the correlation coefficient (multiple R), the coefficient of

determination (R^2), and the adjusted coefficient of determination (R^2_{adj}). These values determine how well the independent variables predict the dependent variable. Furthermore, the linear relationship between the dependent variable and the independent variables must exist. This can be determined by the ANOVA test which should yield a significant p -value.

Upon establishing the nonexistence of multicollinearity and the model fit, the coefficients table is generated to show the beta weights, t values and p values for the independent variables showing the independent variables that are most influential in predicting the dependent variable.

Results

Through SPSS, we first used *Mahalanobis Distance* analysis to identify and eliminate outlier cases from our sample of 237 completed surveys. This resulted in the elimination of four cases which yielded a final total subject of 233 to be used for regression analysis. Table 1 shows the demographics of the subjects.

Second, the analysis of the multicollinearity test among independent variables suggested the nonexistence of multicollinearity. The tolerance level values for all independent variables were above .1 and the VIF values for all independent variables were below 10 (See Table 2).

Second, the model fit was determined by the values of the correlation coefficient (multiple R), the coefficient of determination (R^2), and the adjusted coefficient of determination (R^2_{adj}). Specifically, the model accounted for 67% of the variance for ISP compliance. These values are shown in Table 3. As can be seen, these values showed that the independent variables effectively predicted the dependent variable. The existence of a linear relationship between the dependent variable and the independent variables was determined by the ANOVA test which yielded a significant p -value (See Table 4).

Upon successful establishment of the nonexistence of multicollinearity and the model fit, the coefficients table (See Table 5) was generated to show the beta weights, t values and p values for the independent variables showing all independent variables (leadership, trusting beliefs, role values, and ISP awareness) were significantly influential in predicting the dependent variable (ISP compliance). In addition, bivariate

Table 1. Demographics.

Awareness of University's ISP			Age		
	Freq.	%		Freq.	%
Completely Aware	33	14.2	20–30	16	6.9
Mostly Aware	80	34.3	31–40	49	21
Somewhat Aware	101	43.3	41–50	77	33
Completely Unaware	19	8.2	51–60	62	26.6
Total	233	100	Above 60	29	12.4
			Total	233	100
			Position at the University		
Gender			Faculty	121	51.9
Male	120	51.5	Staff	112	48.1
Female	113	48.5	Total	233	100
Total	233	100			
			Knowledge of Information Technology		
Years of Experience in Current Position			Excellent	51	21.9
1 – 3 years	11	4.7	Good	114	48.9
4 – 6 years	78	33.5	Average	68	29.2
7 – 9 years	46	19.7	Total	233	100
10 – 12 years	38	16.3			
13 – 15 years	26	11.2			
Over 15 years	34	14.6			
Total	233	100			

Table 2. Multicollinearity test.

	Tolerance	VIF
Leadership	.516	1.939
Trusting Beliefs	.451	2.220
Role Values	.668	1.498
Awareness	.780	1.282

Table 3. Model summary.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.670	.449	.440	.50357

Predictors: (Constant), Leadership, Trusting Beliefs, Role Values, Awareness

Table 4. ANOVA test.

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	47.146	4	11.786	46.480	.000
Residual	57.816	228	.254		
Total	104.961	232			

Dependent Variable: ISP Compliance | Predictors: (Constant), Leadership, Trusting Beliefs, Role Values, Awareness

Table 5. Coefficients.

Model	UC		SC		Correlations		
	B	Std. Error	Beta	t	Sig.	Bivariate <i>r</i>	Partial <i>r</i>
(Constant)	3.168	.261		12.126	.000		
Leadership	-.068	.027	-.170	-2.489	.014	.260	-.163
Trusting Beliefs	.171	.044	.286	3.902	.000	.463	.250
Role Values	.409	.050	.493	8.190	.000	.626	.477
Awareness	.065	.028	.131	2.357	.019	.402	.154

Dependent Variable: ISP Compliance | UC = Unstandardized Coefficients, SC = Standardized Coefficients

and partial correlation coefficients are presented in Table 5. The descriptive statistics and correlations are presented in Tables 6 and 7.

Discussion

We built a prediction model and choose four variables as the predictor variables, i.e., leadership, trusting beliefs, role values, and ISP awareness. We then sought to find out which four predictor variables are influential in predicting employees' ISP compliance. The findings indicated that all four predictor

Table 6. Descriptive statistics.

	Mean	Std. Deviation	N
ISP Compliance	6.6795	.67262	233
Leadership	4.8369	1.68584	233
Trusting Beliefs	5.7067	1.12500	233
Role Values	6.1102	.80930	233
Awareness	5.6037	1.35960	233

Table 7. Correlations.

	ISP Compliance	Role Values	Leadership	Trusting Beliefs	Awareness
ISP Compliance	1.000	.626**	.260**	.463**	.402**
Role Values	.626**	1.000	.396**	.503**	.439**
Leadership	.260**	.396**	1.000	.693**	.285**
Trusting Beliefs	.463**	.503**	.693**	1.000	.360**
Awareness	.402**	.439**	.285**	.360**	1.000

**Correlation is significant at the 0.01 level

variables were influential in predicting employees' ISP compliance. In this section, we discuss these findings and their implications for practice and future research focusing on ISP compliance training programs.

In regard to leadership, the findings indicated that leadership is a predictor of employees' ISP compliance. Scholars agree that information security should be treated as a top strategic priority. The commitment from leadership supports the effective enforcement of ISP compliance within organizations.^{33,34} As a predictor of employees' ISP compliance, leadership should articulate a clear vision for the ISP within organizations, formulate a clear strategy for achieving effective ISP, and establish clear goals and objectives for attaining effective ISP that embark upon the ISP compliance requirements to protect the organization's assets against security threats. ISP compliance must be built into the organizational culture by leaders. They should promote organizational culture through influencing, empowering, motivating, and effective communication. Moreover, we assert that achieving ISP compliance requirements, ISP compliance training must be adopted and promoted by leaders. The ISP compliance training should be a required part of organizations activities.

In regard to trusting beliefs, the findings revealed this variable as a predictor of employees' ISP compliance. Mayer et al.⁷⁷ asserted that trust is the propensity to have the intention to depend on others and the propensity influences the amount of trust one has in a trustee. Zucker⁷⁸ referred to trust as a *set of shared social expectations* within an environment. In this environment, trust creates various expectations that are shared and followed by everyone involved. Once trust is built, it strengthens relationships.⁷⁹ Weitzl⁸⁰ stated that trust influences people's intentions and behaviors. In the context of ISP compliance, employees' trusting beliefs (competence, benevolence, and integrity) toward organizations' ISP become vital as it is directly associated with leadership and leadership positively impacts employees' trust to effectively perform requirements of the ISP within organizations.^{53,61} In advancing the ISP compliance training programs, the following questions merit attention for future research. How can ISP compliance training programs demonstrate competence (information security skills and knowledge), benevolence (have the best interest of the organization and employees in mind), and integrity (fulfilling promises and commitments related to all aspects of the ISP requirement) to effectively implement the ISP requirements that will safeguard organizations resources against security threats, breaches, and risks? How can leaders promote and sustain trust as a set of shared social expectations?

As regards role values, the findings implied the role values as a predictor of employees' ISP compliance. As stated by Moody, Siponen, & Pahlila¹³, role values are the beliefs/principles/standards associated with the nature of the work individuals perform. They are deemed appropriate and justified by individuals. Role values should be the focus of future research and the following questions should be answered. How can leadership influence individuals' role values to comply with ISP? Would training and education influence individuals' role values – their beliefs/principles/standards associated with the nature of the work individuals perform? Should the design of ISP compliance training programs pay attention to role values?

Regarding IS awareness, the findings implied that IS awareness is a predictor of employees' ISP compliance. D'Arcy et al.¹⁰ stated that security education training awareness programs significantly impact employees' information security awareness. These programs are built to boost employees' knowledge and awareness of security threats and risks. They also educate employees with ISP and how to comply with the organizations' ISP.^{10,73} Haeussinger & Kranz⁸¹ stated that security policies and employees' knowledge are the most influential antecedents of information security awareness.

Future research should focus on innovative design of ISP compliance training programs. In designing these programs, the following questions merit attention. Are there specific ISP compliance training programs that are associated with employees' intention to comply with ISP? Are necessary knowledge and skills incorporated into ISP compliance training programs to ensure that employees know and understand IS breaches, threats, and risks? Should ISP compliance training programs be tailored for different audiences? Should learning theories be incorporated in the design of the ISP compliance training programs? How often these programs should be offered to the employees? How long should ISP compliance training programs last in a given time?

Conclusion

This study showed that leadership, trusting beliefs, role values, and ISP awareness are influential in predicting the success of employees' intention to comply with the ISP requirements. We conclude that these predictor variables are essential to the success of employees' IS compliance. We also posit that leadership can play a vital role in employees' trusting belief (the competence, benevolence, and integrity related to all aspects of the ISP requirements that are exhibited and supported by leaders), the role values (values associated with the nature of the work individuals perform that leaders can influence), and IS awareness (built as a part of the organizational culture) to promote employees IS compliance which can result in protecting the organization's resources against security threats. This study has limitations that may impact the generalizability of the results. The self-reported data may be a limitation. While we included a consistent wording for the items of each construct to improve the validity of the self-reported data. However, self-reported data can have possible sources of bias that may impact the generalizability of the results. Future studies may consider collecting data through methods other than self-reported data. The sample included faculty and staff from one university in the USA. Future studies should focus on a sample from various higher education institutions in the USA and around the globe. Furthermore, this study should also be carried out in other types of organizations, i.e., public, not for profit, business, and government.

ORCID

Jeretta Horn Nord  <http://orcid.org/0000-0001-7590-9022>

References

- Nieles M, Dempsey K, Pillitteri V. An introduction to information security. *NIST Special Publication 800-12 Revision*; 2017 [accessed 2019 Aug 12]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>.
- Bulgurcu B, Cavusoglu H, Benbasat I. ISP compliance: an empirical study of rationality-based beliefs and information security awareness. *Mis Q.* 2010;34(3):523–48. doi:10.2307/25750690.
- Lowry PB, Moody GD. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Inf Syst J.* 2015;25(5):433–63. doi:10.1111/isj.12043.
- Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Inf Manage.* 2014;51(1):69–79. doi:10.1016/j.im.2013.10.001.
- Padayachee K. Taxonomy of compliant information security behavior. *Comput Secur.* 2012;31(5):673–80. doi:10.1016/j.cose.2012.04.004.
- Vance A, Siponen M, Pahnla S. Motivating IS security compliance: insights from habit and protection motivation theory. *Inf Manage.* 2012;49(3):190–98. doi:10.1016/j.im.2012.04.002.
- Vance T, Siponen M. IS security policy violations: a rational choice perspective. *J Organ End User Comput.* 2012;24(1):21–41. doi:10.4018/joeuc.2012010102.
- Kim SS, Yong JK. The effect of compliance knowledge and compliance support systems on information security compliance behavior. *J Knowl Manage.* 2017;21(4):986–1010. doi:10.1108/JKM-08-2016-0353.
- Cram WA, D'Arcy J, Proudfoot JG. Seeing the forest and the trees: a metaanalysis of the antecedents to ISP compliance. *Mis Q.* 2019;43(2). doi:10.25300/MISQ/2019/15117.
- D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf Syst Res.* 2009;20(1):79–98. doi:10.1287/isre.1070.0160.
- D'Arcy J, Lowry PB. Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study. *Inf Syst J.* 2019;29(1):43–69. doi:10.1111/isj.12173.
- Alotaibi MJ, Furnell S, Clarke N. A framework for reporting and dealing with end-user security policy compliance. *Inf Comput Secur.* 2019;27(1):2–25. doi:10.1108/ICS-12-2017-0097.
- Moody GD, Siponen M, Pahnla S. Toward a unified model of ISP compliance. *Mis Q.* 2018;42:1. doi:10.25300/MISQ/2018/13853.
- Chen X, Chen L, Wu D. Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective. *J Comp Inf Syst.* 2018;58(4):312–24. doi:10.1080/08874417.2016.1258679.
- Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput Secur.* 2012;31(1):83–95. doi:10.1016/j.cose.2011.10.007.
- Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Process.* 1991;50(2):179–211. doi:10.1016/0749-5978(91)90020-T.
- Woon IMY, Tan G-W, Low R. A protection motivation theory approach to home wireless security. In: Avison D, Galletta D, DeGross JI, editors. *Proceedings of the 26th international conference on information systems*; 2005 Dec 11–14; Las Vegas (NV), pp. 367–80.
- Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. *Mis Q.* 2010;34(3):487–502. doi:10.2307/25750688.
- Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *J Assoc Inf Syst.* 2010;11(7):394–413. doi:10.17705/1jais.
- Ajzen I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *J Appl Soc Psychol.* 2002;32:665–83. doi:10.1111/jasp.2002.32.issue-4.
- Paliszkievicz J. ISP compliance: leadership and trust. *J Comp Inf Syst.* 2019;59(3):211–17. doi:10.1080/08874417.2019.1571459.
- Putri F, Hovav A. Employees' compliance with BYOD security policy: insights from reactance, organizational justice, and protection motivation theory. *Proceedings of the European conference on information systems*; 2014 June 9–11; Tel Aviv.

1. Nieves M, Dempsey K, Pillitteri V. An introduction to information security. *NIST Special Publication 800-12 Revision*; 2017 [accessed

23. Silva A. What is leadership? *J Bus Stud Q.* 2016;8(1):1–5.
24. Northouse PG. *Leadership: theory and practice.* 5th ed. Thousand Oaks (CA): Sage; 2010.
25. Yukl GA. *Leadership in Organizations.* New Jersey, USA: Prentice-Hall; 1989.
26. Ezingear J, Bowen-Schrire M. Triggers of change in information security management practices. *J Gen Manage.* 2007;32(4):53–72. doi:10.1177/030630700703200404.
27. Young RF, Windsor J. Empirical evaluation of information security planning and integration. *Commun Assoc Inf Syst.* 2010;26(1): article 13. doi:10.17705/1CAIS.
28. Whitman ME, Mattord HJ. Information security governance for the on-security business executive. *J Executive Educ.* 2012;11:97–111.
29. Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management & organizational culture. *Decis Sci.* 2012;43(4):615–60. doi:10.1111/dec.2012.43.issue-4.
30. Kayworth T, Whitten D. Effective information security requires a balance of social and technology factors. *MIS Q Executive.* 2010;9:2012–52.
31. Siponen MT, Oinas-Kukkonen H. A review of information security issues and respective research contributions. *ACM SIGMIS Database: DATABASE Adv Inf Syst.* 2007;38(1):60–80. doi:10.1145/1216218.
32. Yildirim EY, Akalp G, Aytac S, Bayram N. Factors influencing information security management in small and medium-sized enterprises: a case study from Turkey. *Int J Inf Manage.* 2011;31(4):360–65. doi:10.1016/j.ijinfomgt.2010.10.006.
33. Dutta A, McCrohan K. Management's role in information security in a cyber economy. *Calif Manage Rev.* 2002;45(1):67–87. doi:10.2307/41166154.
34. Safa NS, Von Solms R, Furnell S. ISP compliance model in organizations. *Comput Secur.* 2016;56:70–82. doi:10.1016/j.cose.2015.10.006.
35. Choi M. Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability.* 2016;8(7):638. doi:10.3390/su8070638.
36. Knapp KJ, Morris RF, Marshall TE, Byrd TA. ISP: an organizational-level process model. *Comput Secur.* 2009;28:493–508. doi:10.1016/j.cose.2009.07.001.
37. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur J Inf Syst.* 2009;18:106–25. doi:10.1057/ejis.2009.6.
38. Siponen M, Mahmood A, Pahlila S. Employees' adherence to information security policies: an exploratory field study. *Inf Manage.* 2014;51(201):217–24. doi:10.1016/j.im.2013.08.006.
39. Noufou O, Ouakouak ML. Impacts of personal trust, communication, and affective commitment on change success. *J Organ Change Manage.* 2018;31(3):676–96. doi:10.1108/JOCM-09-2016-0175.
40. Bond-Barnard T, Fletcher L, Steyn H. Linking trust and collaboration in project teams to project management success. *Int J Managing Projects Bus.* 2018;11(2):432–57. doi:10.1108/IJMPB-06-2017-0068.
41. Costa AC. Work team trust and effectiveness. *Personnel Rev.* 2003;32:605–22. doi:10.1108/00483480310488360.
42. Costa AC, Roe RA, Taillieu T. Trust within teams, the relation with performance effectiveness. *Eur J Work Organ Psychol.* 2001;10:225–44. doi:10.1080/13594320143000654.
43. Luhman N. *Trust and power.* New York, NY: John Wiley; 1979.
44. Dodgson M. Learning, trust, and technological collaboration. *Hum Relat.* 1993;46(1):77–95. doi:10.1177/001872679304600106.
45. Ganesan S. Determinants of long-term orientation in buyer–seller relationships. *J Mark.* 1994;58(2):1–19. doi:10.1177/00224299405800201.
46. Morgan RM, Hunt SD. The commitment trust theory of relationship marketing. *J Mark.* 1994;58(3):20–38. doi:10.1177/00224299405800302.
47. Doney PM, Cannon JP, Mullen MR. Understanding the influence of national culture on the development of trust. *Acad Manage Rev.* 1998;23(3):601–20. doi:10.5465/amr.1998.926629.
48. Sako M. Supplier relationships and innovation. In: Dodgson M, Rothwell R, editors. *The handbook of industrial innovation.* Cheltenham, UK: Edward Elgar Publishing; 1994. p. 268–242.
49. Bao G, Xu B, Zhang Z. Employees' trust and their knowledge sharing and integration: the mediating roles of organizational identification and organization-based self-esteem. *Knowl Manage Res Pract.* 2016;14(3):362–75. doi:10.1057/kmrp.2015.1.
50. Ansari AH, Malik S. Ability-based emotional intelligence and knowledge sharing: the moderating role of trust in co-workers very informal newsletter on library automation. *VINE. J Inf Knowl Manage Syst.* 2017;47(2):211–27. doi:10.1108/VJKMS-09-2016-0050.
51. Wang L, Zhang M, Li X. Trust and knowledge creation: the moderating effects of legal inadequacy. *Ind Manage Data Syst.* 2017;117(10):2194–209. doi:10.1108/IMDS-11-2016-0482.
52. Paliszkievicz J, Gołuchowski J, Koohang A. Leadership. Trust and knowledge management in relations to organizational performance: developing and instrument. *Online J Appl KnowlManage.* 2015;3:19–35.
53. Koohang A, Paliszkievicz J, Goluchowski J. The impact of leadership on trust, knowledge management, and organizational performance: a research model. *Ind Manage Data Syst.* 2017;117(3):521–37. doi:10.1108/IMDS-02-2016-0072.
54. Taherdoost H, Sahibuddin S, Namayandeh M, Jalaliyoon N. Propose an educational plan for computer ethics and information security. *Procedia – Social Behav Sci.* 2011;28:815–19. doi:10.1016/j.sbspro.2011.11.149.
55. Kirschenbaum A, Mariani M, Van Gulijk C, Lubasz S, Rapoport C, Andriessen H. Airport security: an ethnographic study. *J Air Transp Manage.* 2012;18:68–73. doi:10.1016/j.jairtraman.2011.10.002.
56. Kirlappos I, Sasse MA. What usable security really means: trusting and engaging users. In: Tryfonas T, Askoxylakis I, editors. *Human aspects of information security, privacy, and trust.* Bristol (UK): Springer; 2014. p. 69–78.
57. Tyler TR. Trust within organizations. *Personnel Rev.* 2003;32(5):556–68. doi:10.1108/00483480310488333.
58. Sasse A, Ashenden D, Lawrence D, Coles-Kemp L, Fléchais I, Kearney P. *Human factors working group white paper: human vulnerabilities in security systems knowledge transfer networks.* London: University College London; 2007.
59. Keval HU, Sasse MA. Not the usual suspects: a study of factors reducing the effectiveness of CCTV. *Secur J.* 2010;23(2):134–54. doi:10.1057/palgrave.sj.8350092.
60. Hardin R. *Trust and trustworthiness.* New York, NY: Russell Sage Foundation; 2002.
61. Le PB, Lei H. The mediating role of trust in stimulating the relationship between transformational leadership and knowledge sharing processes. *J Knowl Manage.* 2018;22(3):521–37. doi:10.1108/JKM-10-2016-0463.
62. Tittle CR. *Control balance: toward a general theory of deviance.* Boulder (CO): Westview Press; 1995.
63. Witte K. Putting the fear back into fear appeals: the extended parallel process model. *Commun Monogr.* 1992;59(4):329–49. doi:10.1080/03637759209376276.
64. Triandis HC. *Interpersonal behavior.* Monterey (CA): Brooks/Cole; 1977.
65. Gagnon M-P, Godin G, Gane C, Fortin J-P, Lamothe L, Reinharz D, Cloutier A. An adaptation of the theory of interpersonal behavior to the study of telemedicine adoption by physicians. *Int J Med Inform.* 2003;71:103–15.
66. Bamberg S, Schmidt P. Incentives, morality, or habit? Predicting students' car use for university routes with the models of Ajzen, Schwartz, and Triandis. *Environ Behav.* 2003;35(2):264–85. doi:10.1177/0013916502250134.

67. Limayem M, Hirt SG. Force of habit and information systems usage: theory and initial validation. *J Assoc Inf Syst.* 2003;4(1):65–97. doi:10.17705/1jais.
68. Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Q.* 2010;34(3):613–43. doi:10.2307/25750694.
69. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. *Mis Q.* 2010;34(4):757–78. doi:10.2307/25750704.
70. Karjalainen M, Siponen M. Toward a new meta-theory for designing information systems (is) security training approaches. *J Assoc Inf Syst.* 2011;12(8):1343–48. doi:10.17705/1jais.00274.
71. Shaw RS, Chen CC, Harris AL, Huang HJ. The impact of information richness on information security awareness training effectiveness. *Comput Educ.* 2009;52(1):92–100. doi:10.1016/j.compedu.2008.06.011.
72. Siponen M. A conceptual foundation for organizational information security awareness. *Inf Manage Comp Secur.* 2000;8(1):31–41. doi:10.1108/09685220010371394.
73. Lee J, Lee Y. A holistic model of computer abuse within organizations. *Inf Manage Comp Secur.* 2002;10(2/3):57–63. doi:10.1108/09685220210424104.
74. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Comput Secur.* 2014;42:165–76. doi:10.1016/j.cose.2013.12.003.
75. Box D, Pottas D. Improving information security behaviour in the healthcare context. *Procedia Technol.* 2013;9:1093–103. doi:10.1016/j.protcy.2013.12.122.
76. Stevens J. *Applied multivariate statistics for the social sciences.* 4th ed. Hillsdale (NJ): Lawrence Erlbaum Associates; 2001.
77. Mayer RC, Davis JH, Schoorman FD. An integrative model of organizational trust. *Acad Manage Rev.* 1995;20(3):709–34. doi:10.5465/amr.1995.9508080335.
78. Zucker LG. Production of trust: institutional sources of economic structure, 1840–1920. In: Cummings LL, Staw B, editors. *Research in organizational behavior.* Vol. 8. Greenwich, CT: JAI Press; 1986. p. 53–111.
79. Denize S, Young L. Concerning trust and information. *Ind Marketing Manage.* 2007;36(7):843–1018. doi:10.1016/j.indmarman.2007.06.004.
80. Weitzl W. *Measuring electronic word-of-mouth effectiveness.* Berlin, Germany: Springer Gabler; 2017.
81. Haeussinger F, Kranz J. Information security awareness: its antecedents and mediating effects on security compliant behavior. *Proceedings of Thirty-Fourth International Conference on Information Systems, Milan;* 2013.