International Journal on Semantic Web and Information Systems
Volume 19 • Issue 1

Enforcing Information System Security:
Policies and Procedures for Employee Compliance

Abdullah Almuqrin, King Saud University, Saudi Arabia*
https://orcid.org/0000-0002-6692-9694

Ibrahim Mutambik, King Saud University, Saudi Arabia
https://orcid.org/0000-0001-6819-5244

Abdulaziz Alomran, King Saud University, Saudi Arabia
https://orcid.org/0000-0002-3309-6614

Justin Zuopeng Zhang, University of North Florida, USA
https://orcid.org/0000-0002-4074-9505

ABSTRACT

Every year brings numerous security breaches that lead to highly destructive ransomware attacks, data leaks, and reputational damage to governments, companies, and other organizations around the world. As a result, there is a growing need to ensure that workers comply with critical policies put in place to avoid such incidents. This study investigated how factors from social bond theory and involvement theory affected compliance with information security policies and procedures. All of the factors examined were found to have a significant influence on attitudes about compliance, and attitude had a significant impact on intention to comply. The findings of this study revealed that it is vital to raise employees' awareness about compliance with security policies by improving their information security behavior. Moreover, all the factors were found to have a significant influence on the attitude of employees towards compliance with their organizational information security policies and procedures.

KEYWORDS

Compliance, Employee Attitude, Information Security, Involvement Theory, Policy, Procedure, Social Bond Theory, Structural Equational Modeling

INTRODUCTION

In 2021 alone, there were 5,258 confirmed data breaches in organizations from 88 countries (Verizon, 2021, p. 4). In this context, a *breach* is any "incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party" (p. 4). Data breaches and the financial and reputational losses associated with them have forced organizations to pay more attention to the security

DOI: 10.4018/IJSWIS.331396 *Corresponding Author

of their information systems (Khando et al., 2021). There are many examples of such breaches caused by employees. In January 2021, for instance, a group of lawyers working inside the law firm Elliott Greenleaf stole sensitive files, including client data, for personal gain and to help a competing law firm open a new office. This led to the closure of Elliott Greenleaf's office and severe reputational harm (Ekran System, 2023; Liolis, 2022). In July 2020, phishing attacks by Twitter employees led to the transfer of about $180,000 in Bitcoin to scam accounts. The accounts of millions of followers were hacked, including those of Elon Musk, Apple, Jeff Bezos, and Bill Gates (Ekran System, 2023).

Information system security (ISS) breaches can have technical and nontechnical causes and associated preventive measures (Dong et al., 2021). Technical solutions include authentication and detection, antimalware, antispyware, and firewalls, but these alone are insufficient for ensuring security (Alassaf & Alkhalifah, 2021). Thus, there is a need for nontechnical solutions that take human behavior into account to guarantee information security policy (ISP) compliance (Almomani et al., 2021; Dong et al., 2021). While the terms *cybersecurity* and *information security* (IS) are sometimes used interchangeably, they are distinct concepts. IS is concerned with safeguarding the integrity, confidentiality, and availability of information and managing its loss (Greene et al., 2021). In contrast, cybersecurity involves the security of information, technology, processes, and people (Kovacevic et al., 2020). Therefore, it is important for organizations to create a safe environment in both regards (Antunes et al., 2022).

Hackers jeopardize system security by gaining access to weak points by targeting management and employee behavior (Huang et al., 2021). The human factor and unsafe user behavior, such as sharing passwords and usernames and opening insecure links, are the most common factors contributing to data breaches (Almuqrin et al., 2023; Kovacevic et al., 2020). As a result, employees are the weakest point in the data security of any organization and contribute to a large number of breaches (58%), 33% of which are a consequence of noncompliance with information security policies and procedures (ISPP; Alassaf & Alkhalifah, 2021). Despite this, organizations typically focus more on the technical aspects of IS than employee behavior (Khando et al., 2021).

Any breach can cause major challenges for organizations (Hwang & Um, 2021; Khando et al., 2021). One is that organizations must work vigorously to install high expectations for ISPP compliance. Another challenge is the shortage of skilled workers inside the organization who can conduct security training. Moreover, some board members fail to support spending on improving IS compliance. The inability to find guidelines based on best practices to keep up with IS threats that are continuously changing is a challenge as well. Therefore, it is vital for organizations to raise awareness among employees, improve their IS behavior, and motivate them to comply with ISP (Alassaf & Alkhalifah, 2021; Carmi & Bouhnik, 2020; Chen et al., 2022; Dong et al., 2021; Hina et al., 2019; Huang et al., 2021).

This study proposes a multi-perspective approach to address IS breaches (see Raddatz et al., 2020). Hwang and Um (2021) used social bond theory to investigate its applicability to this area. They postulated that most IS breaches come from organization insiders. The present study investigated to what extent factors from social bond theory empowered employees and improved their attitude toward ISPP compliance. The effect of attitude on the intention to comply with ISPP was also examined.

Two research questions guided the study:

1. What motivates employees to comply with organizational ISPP?
2. How can the factors of social bond theory and involvement theory contribute to IS by empowering employees and facilitating their compliance with organizational ISPP?

THEORETICAL FRAMEWORK AND LITERATURE

This study examined factors responsible for employee policy compliance to reduce the danger of security breaches. The theoretical framework was based on social bond theory, investigating the

impact of commitment, attachment, involvement, and personal belief on employee attitudes toward following ISPP. However, the concept of involvement was used separately under involvement theory, encompassing the factors of IS knowledge sharing, collaboration, intervention, and experience. This framework is illustrated in Figure 1.

Social Bond Theory

Social bond theory was proposed by Hirschi (1969) and later became known as social control theory. It assumes that any act aiming to breach a rule results from weak or fragmented bonds with society. These bonds are the factors (i.e., commitment, attachment, involvement, and personal belief) controlling an individual's behavior when attempting to break the law or engage in an unusual or unaccepted behavior (Hirschi, 1969). This theory focuses on the relationship between individuals and their society and the shared values they acquire from this relationship, shaping their interaction with peers, organizations, and society (Hirschi, 1969). The strength of social values and ties determines how much an individual can deviate from an accepted behavior. As a result, the present study used social bond theory to examine compliance with ISP (see Dong et al., 2021; Hwang & Um, 2021; Ifinedo, 2014, 2018; Safa et al., 2016). Using this theory, Peterson et al. (2016) found that attachment to parents (represented in parental supervision) and commitment (represented in a GPA increase) were the main factors in reducing juvenile delinquency. The factors of attachment, commitment, and personal belief are described in the following sections, while involvement is discussed separately under "Involvement Theory."

Attachment

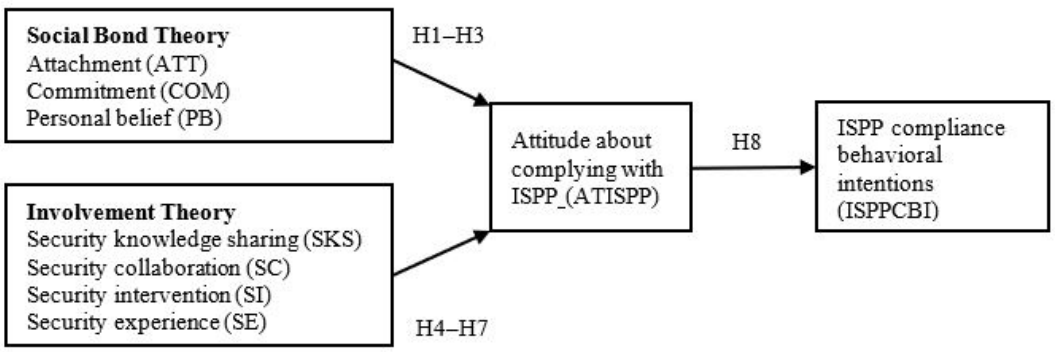
Attachment to others is considered a sign of psychological well-being (Hirschi, 1969). Those who have no attachment to others may lack social restraints, making it more likely they will violate societal norms and act against the expectations of their peers. Likewise, employee attachment to an organization increases their bonds with peers and encourages them to comply with ISP (Dong et al., 2021). Moreover, when employees discuss IS with peers, they become more compliant with associated policies (Alassaf & Alkhalifah, 2021; Antunes et al., 2022; Carmi & Bouhnik, 2020; Dong et al., 2021). Prior work on this factor thus shaped the first hypothesis of the present study:

Hypothesis 1: Employee attachment to an organization has a positive influence on attitudes toward complying with its ISPP.

Commitment

Commitment is a factor that Hirschi (1969) claimed could lead to social conformity. IS can be achieved through individual users' association with a social group or organization, holding them accountable

Figure 1. Theoretical framework



for safeguarding information by their commitment to policies and rules. Strong commitment will encourage positive IS behavior; otherwise, negative security behavior can become predominant (Dong et al., 2021). Thus, it is important to align employee interests with organizational interests (Carmi & Bouhnik, 2020; Khando et al., 2021; Mutambik et al., 2023a). In this regard, committed employees are more likely to invest in career development and promotions, less likely to violate ISPP, and more likely to see compliance as imperative (Hwang & Um, 2021). This was reflected in the second hypothesis:

Hypothesis 2: Employee commitment to an organization has a positive influence on attitudes toward complying with its ISPP.

Personal Belief

Despite well-established value systems, some individuals still violate their norms (Hirschi, 1969). An individual's personal beliefs represent the values shaping their social interactions and relationships with other individuals or entities in their society. Personal belief forms a person's perception of behaviors justified by society (Hwang & Um, 2021). Regarding IS compliance, research supports the influence of positive personal beliefs on attitudes toward organizational norms and policies (Dong et al., 2021; Hwang & Um, 2021). Accordingly, employees are more likely to comply with policies in which they have a strong personal belief (Hwang & Um, 2021). This line of research led to the third hypothesis:

Hypothesis 3: Employees' personal beliefs in an organization's norms have a positive influence on attitudes toward complying with its ISPP.

Involvement Theory

Involvement theory explores the factors influencing the degree of involvement in a certain activity and has been used to investigate various behaviors (Safa et al., 2016). Customer involvement, for example, has been related to the extensiveness of decision-making, the depth of interest in advertising for a product, enjoyment in shopping, use of a product, and commitment to a brand (Mittal & Lee, 1989). The theory has also been used to examine student development and create better learning environments capable of changing student behavior and facilitating development (Astin, 1999).

Hirschi (1969) framed involvement as a means of avoiding noncompliance. Awareness about the significance of IS among employees can determine their level of involvement in related practices (Dada et al., 2021; Tatu et al., 2018; Wu et al., 2022). Attitude can be affected by employee involvement in IS, including IS knowledge sharing, collaboration, intervention, and experience. These factors demonstrate the level of participation, time, and effort an individual devotes to protect and secure information, a major asset for most organizations. In this study, these factors were investigated for their influence on employee compliance with ISPP, as detailed in the following subsections.

Information Security Knowledge Sharing

Knowledge sharing represents a powerful behavior for increasing people's awareness of a problem and helping them find solutions, avoid making the same mistakes again, and comply with best practices (Tatu et al., 2018). All types of knowledge, internal and external, contribute to the invaluable asset of organizational knowledge shared among employees. This knowledge assists in improving decision making, competencies, capabilities, decreasing costs, and alleviating risks (Pham et al., 2021; Safa et al., 2016; Safa & Von Solms, 2016). Knowledge sharing is crucial in maximizing employee awareness and is an important indication of IS involvement. It provides real-time problem-solving and reduces the wasted effort, time, and cost associated with replicating the same solutions for similar problems (Wang, 2022; Żywiołek et al., 2021). However, Pham et al. (2021) found that many participants did not see IS knowledge sharing with peers as necessary. They only shared security problems with

the IT department. Moreover, employees' unwillingness to share knowledge is a huge barrier to IS knowledge sharing (Żywiołek et al., 2021), since sharing knowledge about breaches and threats can increase IS awareness (Tatu et al., 2018). Therefore, it is crucial to encourage employees to share knowledge about these issues (Tatu et al., 2018; Żywiołek et al., 2021) to improve their awareness and attitudes about security-related behavior (Othman et al., 2019; Safa et al., 2016). This issue was reflected in the fourth hypothesis:

Hypothesis 4: Employee IS knowledge sharing has a positive influence on attitudes toward complying with an organization's ISPP.

Information Security Collaboration

Professional collaboration involves employees working together to perform an activity or achieve a shared goal (Safa et al., 2016; Tatu et al., 2018). It is "a process through which parties who see different aspects of a problem can constructively explore their differences and search for solutions that go beyond their own limited vision of what is possible" (Gray, 1989, p. 58). Collaboration facilitates acquiring, exchanging, and using knowledge, increasing the information disseminated about an issue (Mennens et al., 2018; van Rensburg, 2021). IS collaboration involves gathering, integrating, organizing, and sharing IS knowledge with experts and employees (Tatu et al., 2018). It can facilitate sending, improving, or reviewing knowledge and expand the knowledge communicated between employees and IT security specialists, alerting both to threats and breaches and raising their security awareness. In this way, collaboration helps minimize such incidents, protect against breaches, and draw employee attention to the significance of compliance with ISPP (Safa et al., 2016; Safa et al., 2017; Tatu et al., 2018). These ideas led to the fifth hypothesis:

Hypothesis 5: Employee IS collaboration has a positive influence on attitudes toward complying with an organization's ISPP.

IS Interventions

IS interventions offer a practical approach to changing IS behavior among employees by developing their awareness and translating it into policy implementation (Alshaikh & Adamson, 2021). This awareness should be frequently updated through effective, relative, and consistent programs (Juma'h & Alnsour, 2022; Liu et al., 2020). For Bauer et al. (2017), incorporating interventions such as active participation, feedback, dialogue, and reflection into IS awareness programs resulted in higher awareness and involvement and enhanced employee perceptions of the risks, both individually and organizationally. Such interventions influenced users' neutralization behaviors and improved IS knowledge and responsibility regarding policy compliance. Based on this, the sixth hypothesis was:

Hypothesis 6: IS interventions have a positive influence on employee attitudes toward complying with an organization's ISPP.

Information Security Experience

Experience was defined by Randolph Frederick Pausch as "What you get when you didn't get what you wanted" (Benzel, 2021, p. xiii). Benzel (2021) explained that experience involves learning from one's mistakes, a significant approach to personal development by reflecting on actions and their consequences. Thus, an individual can become more proficient after expending the effort and time to gain experience in a field and more prone to handle problems by looking for effective solutions (Blythe & Coventry, 2018; Liang et al., 2022; Tatu et al., 2018). In IS, experience increases user awareness

of potential threats (Tatu et al., 2018), an important aspect of a secure information environment (Safa et al., 2017). This informed the seventh hypothesis:

Hypothesis 7: Employee IS experience has a positive influence on attitudes toward complying with an organization's ISPP.

Attitude

As "a learned tendency to evaluate things in a certain way," attitude plays a major role in behavior (Cherry, 2018, p. 1). Through attitude, people can assess others, issues, events, and things positively or negatively or be uncertain. Attitudes are based on three components: a cognitive component, the ideas and beliefs about something; an affective component, involving how the person, issue, or event affects emotions and feelings; and a behavioral component, determining how attitude can affect behavior or intention to perform a behavior (Cherry, 2018). Moreover, past and present experience shapes attitudes (Ajzen, 2001; Mutambik et al., 2023b; Safa et al., 2016; Safa et al., 2017). This applies to IS, where a positive attitude toward policy compliance should result in more employee compliance. Therefore, the eighth hypothesis was:

Hypothesis 8: Employee attitudes toward complying with an organization's ISPP have a positive influence on their behavioral intentions to comply with those policies and procedures.

METHODOLOGY

This study investigated employee ISPP compliance and potentially influential factors drawn from social bond theory and involvement theory. Data were collected using an online questionnaire to reach a wide range of the intended population.

Instrument

The questionnaire items were developed from validated scales in the literature and modified to fit the context of the study. The items were tested for suitability, clarity, and readability through a panel of five faculty members specialized and experienced in information management and security. In addition, the items were checked by conducting a pilot study with 18 employees from one of the Saudi organizations participating in the study. Items were designed to investigate how factors drawn from social bond theory and involvement theory might influence employee attitudes and intention to comply with ISPP. Table 1 shows the number of items used per variable and defines each construct. Responses were measured on a five-point Likert scale ranging from *strongly disagree* to *strongly agree*.

Data Collection

Data were collected from employees in different departments in three Saudi companies known for their strict ISPP. An initial version of the questionnaire was piloted to make certain items were easy to understand. Respondents were informed about the study and were asked to answer the questionnaire and report their feedback regarding the readability, wording, and clarity of the items. The pilot study included 18 items, and its results showed that respondents understood the questionnaire and there were no ambiguous items. The original version of the questionnaire contained 42 items and respondents were given access to the questionnaire through Google Forms. The link for completing the questionnaire was made available from June to September 2022.

Table 1. Constructs

Construct	Definition	Items	Item Source
Attachment (ATT)	Respect and affection that an individual has with significant others (co-workers, supervisors, jobs, and organizations can be significant others)	4	Safa et al. (2016, p. 74)
Commitment (COM)	Totality of internalized normative pressures to act in a way that meets organizational interests	4	Wiener (1982, p. 418)
Personal belief (PB)	Feelings of a moral obligation to perform a certain behavior	4	Doran and Larseni (2016, p. 160)
Information security knowledge sharing (SKS)	Collaboration with others by sharing experiences, ideas, and knowledge in order to safeguard information assets in organizations.	5	Safa and Von Solms (2016, p. 442)
Information security collaboration (SC)	Interactive affair with a shared common objective (i.e., increasing IS) sustained by voluntary membership, mutual decision making, acceptance of procedures (i.e., compliance with ISP), and a predefined timeline in order to achieve a certain goal	4	Tatu et al. (2018, p. 3738)
Information security intervention (SI)	Set of tools that deploy insights gained from security incidents, aiming to change employee IS behavior	4	Tatu et al. (2018, p. 3738)
Information security experience (SE)	Lessons one can learn from direct exposure to an IS risk	4	Tatu et al. (2018, p. 3738)
Attitude toward complying with ISPP (ATISPP)	Degree to which compliance behavior is valued	4	Ajzen (1991), Fishbein and Ajzen (1975)
ISPP compliance behavioral intentions (ISPPCBI)	Decision to protect the information and technology resources of the organization from potential security breaches	5	Ajzen (1991), Fishbein and Ajzen (1975)

Population and Sampling

The target population consisted of all employees at three Saudi companies. To obtain a reasonable sample, opportunistic and snowball sampling were utilized. The sample contained 438 individuals who responded to the questionnaire. However, 118 of them did not answer all items and were removed (cf. Hair et al., 2021). The remaining 320 responses were complete, representing 73% of all respondents. Their average age was 31, and their other demographics are presented in Table 2.

Table 2. Respondent demographics

Variable	Sub-variable	Percentage
Gender	Female	52.8%
	Male	47.2%
Education level	Diploma	9.7%
	Bachelor's degree	55.9%
	Master's degree	32.3%
	PhD	2.1%
Position	Manager	6%
	Vice manager	14%
	Staff	80%

Data Analysis

For the data analysis, a two-level approach was employed based on the recommendations of Anderson and Gerbing (1988). This included analyzing the measurement model and structural relationships between latent constructs. The purpose of this approach was to evaluate the validity and reliability of the measures and review the estimates of the structural model by checking for collinearity and significance of the path coefficients.

The estimates of the structural model were obtained using structural equation modeling (SEM), which involves testing hypothesized relationships between dependent and independent variables (Hair et al., 2006; Hair et al., 2021). This technique also effectively assessed the loadings of the hypothesized items (indicators) on their latent constructs (measurement model; Hair et al., 2006; Hair et al., 2021). To investigate the effect of the constructs of employee commitment, attachment, and personal beliefs as well as IS knowledge sharing, collaboration, intervention, and experience on attitude toward complying with organizational ISPP, both the structural and measurement models were assessed using SEM. In addition, the maximum likelihood was selected for estimated relationships between dependent and independent variables to determine their strength and direction.

Construct Validation

Construct validity was tested using confirmatory factor analysis (CFA), a multivariate procedure, in the AMOS software (Version 26), thus allowing constructs to freely co-vary with each item and work as a reflective indicator of its latent construct. Model estimation was performed using the maximum likelihood approach, taking the item correlation matrix as an input. The CFA results and Cronbach's alphas and composite reliabilities of all constructs are depicted in Table 3. Data gathered from validated measures were employed to examine the linear causal relationships developed in the structural model. The results showed a proper model fit, as depicted in Table 4, and its indices were within the value thresholds for CMIN/DF 2.38 (CMIN = 1478, DF = 454), RMSEA 0.061, CIF 0.948, NNFI 0.959, NFI 0.934, and AGFI 0.859 (Byrne, 2001; Hair et al., 2006; Hayduk, 1987; Hu & Bentler, 1999). In addition, multicollinearity was tested, and variance inflation factor (VIF) values were within an acceptable range (1.35–1.82) for all constructs.

Similarly, by utilizing the three criteria developed by Fornell and Larcker (1981), it was possible to verify the convergent validity for the measurement scales. These criteria require that (a) all indicator loadings should be significant and over the threshold value of 0.7, (b) construct reliabilities should be over 0.8, and (c) the average variance extracted (AVE) by each construct must be significant and more than its variance, i.e., over 0.5 (Fornell & Larcker, 1981). As demonstrated in Table 3, all loadings in the CFA model exceeded the 0.7 threshold. In addition, the composite reliabilities of all constructs were between 0.85 and 0.91, and the AVE values ranged from 0.61 to 1.00. Accordingly, all three of Fornell and Larcker's (1981) criteria for verifying convergent validity were justified.

Furthermore, Fornell and Larcker's (1981) guidelines were used for evaluating discriminant validity. They revealed that the square root of the AVE from a certain construct should be more than the value of the correlation between this construct and the rest of the constructs in the model. Table 5 gives a list of correlations between all constructs and the value of the square root of the AVE, located on the diagonal. All values of AVE on this diagonal exceeded the inter-construct correlations. As a result, discriminant validity was verified for all constructs.

RESULTS

This study examined the effectiveness of the proposed model and the relationships between its constructs. Construct variance was identified through collinearity and path coefficients. To avoid collinearity, VIF values must be less than 5.00, and this study found no collinearity problems since the VIF values were less than 5.00 for all predictors. Furthermore, evaluating the significance and

Table 3. Confirmatory factor analysis

Construct	Items	Mean	Loading	Composite reliability	Cronbach's alpha
Attachment (ATT)	ATT1	4.58	0.746	0.736	0.806
	ATT2	4.69	0.676		
	ATT3	4.58	0.694		
	ATT4	3.93	0.586		
Commitment (COM)	COM1	3.85	0.688	0.813	0.799
	COM2	4.30	0.721		
	COM3	3.86	0.692		
	COM4	4.20	0.722		
Personal belief (PB)	PB1	4.29	0.702	0.847	0.736
	PB2	4.33	0.742		
	PB3	4.65	0.522		
	PB4	3.96	0.789		
Information security knowledge sharing (SKS)	SKS1	4.22	0.765	0.833	0.751
	SKS2	3.98	0.592		
	SKS3	4.32	0.635		
	SKS4	4.20	0.722		
	SKS5	3.78	0.698		
Information security collaboration (SC)	SC1	3.95	0.598	0.765	0.801
	SC2	3.90	0.689		
	SC3	4.45	0.722		
	SC4	4.70	0.734		
Information security intervention (SI)	SI1	3.95	0.628	0.845	0.798
	SI2	4.33	0.586		
	SI3	3.96	0.724		
	SI4	4.10	0.698		
Information security experience (SE)	SE1	4.45	0.762	0.758	0.745
	SE2	4.38	0.746		
	SE3	3.89	0.686		
	SE4	3.75	0.732		
Attitude toward complying with ISPP (ATISPP)	ATISPP1	4.15	0.699	0.735	0.864
	ATISPP2	4.54	0.742		
	ATISPP3	4.65	0.712		
	ATISPP4	4.28	0.564		
ISPP compliance behavioral intentions (ISPPCBI)	ISPPCBI1	4.41	0.706	0.822	0.788
	ISPPCBI2	4.15	0.689		
	ISPPCBI3	3.91	0.521		
	ISPPCBI4	3.85	0.712		
	ISPPCBI5	4.50	0.716		

Table 4. Measurement model fit indices

Fit index	Results	Recommended criteria	Source
CMIN/DF (χ2/DF)	1478/454 = 2.38	≤ 5	Hair et al. (2006)
RMSEA	0.061	≤ 0.08	Byrne (2001)
CIF	0.948	≥ 0.90	Hu and Bentler (1999)
NNFI	0.959	≥ 0.90	Hayduk (1987)
NFI	0.934	> 0.90	Hair et al. (2006)
AGFI	0.859	≥ 0.80	Hayduk (1987)

Table 5. Inter-item correlations

	AVE	ATT	COM	PB	SKS	SC	SI	SE	ATISPP	ISPPCBI
ATT	0.62	**0.79**								
COM	0.67	0.35	**0.82**							
PB	0.72	0.26	0.34	**0.85**						
SKS	0.65	0.16	0.35	0.48	**0.81**					
SC	0.67	0.34	0.44	0.29	0.48	**0.82**				
SI	0.61	0.32	0.34	0.24	0.42	0.44	**0.78**			
SE	0.70	0.45	0.23	0.31	0.55	0.32	0.44	**0.84**		
ATISPP	0.69	0.23	0.42	0.47	0.49	0.43	0.29	0.45	**0.83**	
ISPPCBI	0.63	0.31	0.55	0.36	0.43	0.56	0.43	0.35	0.25	**0.79**

relevance of the path coefficients and their weights makes it easy to explain the significance of the effect of one variable on another and its relative statistical importance. According to Hair et al. (2021), when using a two-tailed *t*-test, the significance level of path coefficients should be 5% and their values should be between -1 and +1. Furthermore, strong negative relationships are when path coefficients are closer to-1, and strong positive relationships are when they are closer to +1. Table 6 presents the path coefficients and *t*-values of all hypothesized relationships between variables.

Table 6. Path coefficients

Hypothesis	Estimate (β)	*t*	Supported
H_1: ATT → ATISPP	0.478	4.10	Yes
H_2: COM → ATISPP	0.298	4.85	Yes
H_3: PB → ATISPP	0.249	5.45	Yes
H_4: KS → ATISPP	0.302	3.45	Yes
H_5: SC → ATISPP	0.236	4.45	Yes
H_6: SI → ATISPP	0.141	3.20	Yes
H_7: SE → ATISPP	0.274	3.95	Yes
H_8: ATISPP → ISPPCBI	0.363	3.35	Yes

The outcomes revealed a positive impact from employee attachment ($\beta = 0.478$, $t = 4.10$), commitment to their organization ($\beta = 0.298$, $t = 4.85$), personal belief ($\beta = 0.249$, $t = 5.45$), IS knowledge sharing ($\beta = 0.302$, $t = 3.45$), IS collaboration ($\beta = 0.236$, $t = 4.45$), IS interventions ($\beta = 0.141$, $t = 3.20$), and IS experience ($\beta = 0.274$, $t = 3.95$) on their attitude toward complying with ISPP. Moreover, this attitude positively affected employee intention to comply with those policies and procedures. Therefore, all proposed hypotheses were supported and all relationships between constructs in this structural model were statistically significant.

Discussion

This study examined factors that might motivate employees to comply with organizational policies and procedures related to IS and how these factors could protect information by empowering employees and facilitating their compliance. The study used factors from social bond theory (attachment, commitment, and personal belief) and involvement theory (IS knowledge sharing, collaboration, experience, and intervention) to investigate their effect on employee IS awareness and compliance. Evidence suggests that most IS breaches come from inside the organization (Hwang & Um, 2021), and raising employee IS awareness is a significant part of reducing breaches (Dada et al., 2021; Tatu et al., 2018). This study is one of the few to use the factors of social bond theory and involvement theory together to understand employee intentions to comply with their organization's ISPP. Table 7 illustrates some of the studies that were conducted between 2017 and 2023 on employee compliance with ISPP and the results of these studies.

Table 7. Factors influencing security compliance used by some studies

Study	Factors Influencing Security Compliance	Results
Bauer et al. (2017)	Implementation of IS awareness (ISA) programs that include perception of risks, responsibilities, importance, and knowledge.	ISA program designs and factors influenced users' ISP compliance.
Amankwa et al. (2018)	Supportive organizational culture, end-user involvement, and compliance leadership.	Supportive organizational culture and end-user involvement significantly influenced employee attitude toward ISP compliance, while leadership showed a weak influence.
Hina et al. (2019)	Attitude, subjective norms, self-efficacy, response efficacy, perceived severity, perceived vulnerability, provision of policies, SETA (security education, training, and awareness) program, and negative experience.	Negative experience had no direct effect on perceived severity and vulnerability. Response efficacy and subjective norms had no effect on ISP compliance. Subjective norms were highly influential when goal-oriented cultural values were stronger.
Carmi and Bouhnik (2020)	Attitude, normative beliefs, personal capabilities, evaluation of the benefits of compliance, costs of compliance, costs of noncompliance, general awareness, and ISP awareness.	All factors had a positive effect on and were important for employee ISP compliance.
Dong et al. (2021)	Top management beliefs about IS security issues, organization's control of IS security issues, attachment, commitment, involvement, and personal norms.	ISP compliance was enhanced through top management beliefs and the organization's control of IS. The influence of these factors was more significant when exposed to the mediating effect of the factors of social bond theory.
Karlsson et al. (2022)	Some types of organizational culture, including clan culture, adhocracy, bureaucratic culture, and market culture.	Focusing organizational culture on people in the organization was positively related to employee ISP compliance. With respect to control and flexibility, differences in organizational culture had less effect on compliance. A bureaucratic culture fostered compliance.
Zhu et al. (2023)	The three dimensions of paternalistic leadership—authoritarian leadership (AL), benevolent leadership (BL), and moral leadership (ML), sanctions, and IS climate.	The influence of AL was partially mediated by employee perceptions of sanctions, the influence of BL was partially mediated by employee perceptions of IS climate, and the influence of ML was partially mediated by employee perceptions of both sanctions and IS climate.

Regarding social bond theory, attachment was one of the main factors affecting employee attitudes toward policy compliance. This result was in line with Dong et al. (2021), which found that employee attachment to an organization strengthened bonds among peers and encouraged them to comply with ISPP. Employee commitment also significantly positively affected attitude toward compliance in the present study. Similarly, Hwang and Um (2021) found that committed employees were more devoted to their roles, more likely to invest in career development and promotions, and less likely to violate ISP (Hwang & Um, 2021). Personal belief likewise had a significant positive impact, in line with Dong et al. (2021) and Hwang and Um (2021). Personal belief reflects the values shaping social interactions and relationships with others, and a strong personal belief in organizational norms can encourage compliance with ISPP (Almuqrin et al., 2022; Hwang & Um, 2021). Organizations can foster attachment, commitment, and personal belief to enhance compliance with security policies by sharing values and goals with employees, providing a positive work environment, supporting their professional growth, encouraging team bonding, respecting their needs, and appreciating their progress.

Regarding involvement theory, IS knowledge sharing was a powerful factor in increasing employee awareness regarding breaches, highlighting the importance of complying with ISPP, in line with prior studies (e.g., Pham et al., 2021; Safa et al., 2016). In accordance with this finding, Pham et al. (2021) showed that knowledge sharing resulted in more effective IS practices. Furthermore, IS collaboration among employees positively influenced their attitude toward complying with ISPP. This conformed to Tatu et al. (2018), in which employee collaboration effectively minimized breaches and drew attention to the significance of compliance with ISPP (Mennens et al., 2018; Shih et al., 2021). IS intervention had a positive influence on employee attitudes as well. Bauer et al. (2017) similarly concluded that IS intervention influenced users' neutralization behaviors and improved IS knowledge and responsibilities. Finally, experience effectively increased awareness of potential IS threats and positively influenced attitudes about policy compliance, in line with other studies (e.g., Safa et al., 2017; Tatu et al., 2018).

Thus, all proposed hypotheses were supported with statistically significant results, indicating that all proposed constructs effectively changed attitudes toward compliance with ISPP. The results of this study and previous research have shown a consensus that many factors influence levels of employee compliance with organizational ISPP. These factors include sufficient knowledge of ISPP, their attitude toward complying with ISPP, their belief that noncompliance can lead to punishment and that compliance can lead to recognition and rewards, offering training and education programs on ISPP, commitment of leadership to IS, and having an organizational culture that fosters ISPP compliance.

Leadership plays a key role in fostering a culture of security compliance. Leaders need to serve as good role models and show employees that their security behavior protects the organization. In this capacity, leaders should continuously communicate ISPP and take these policies and procedures seriously. Leaders should also provide periodic training programs for employees to ensure they receive up-to-date knowledge about security risks and the importance of following ISPP (Kilgore, 2021).

Implications and Future Research

The findings of this study offer important implications for IS. The impact of factors from social bond theory and involvement theory on employee attitudes shows their importance in driving ISPP compliance. These findings could be expanded in future research to include different countries, and differences in ISPP compliance between employees of different organizations could be detected based on gender, age, job responsibilities, and level of education. Programs for enhancing IS compliance could be created based on the importance of each construct discussed in this study. The constructs and other perspectives could also be analyzed in future research to extend the possibility of optimizing employee compliance and reducing the risk of IS breaches. Moreover, future research should explore other factors from different theories that could motivate employees and influence their attitudes regarding ISPP. While employee involvement with organizations, interactions with others, and available knowledge make a difference in compliance, other factors, such as rewards and

other forms of compensation, could also promote policy respect and compliance. In addition, the relationship between different personalities and levels of compliance could be analyzed. Researchers should explore the influence of training and education on employee awareness of and compliance with these policies. Designing an effective training program could include the following:

- Increasing the determination of employees to acquire more knowledge on security and compliance.
- Presenting existing knowledge and the gaps that cause security threats and hinder compliance.
- Introducing weak points and necessary skills.
- Constructing and delivering instructions based on motivating employees and enabling the cognitive processing of information.
- Assessing the program's success by verifying to what degree employee compliance has been achieved (Puhakainen & Siponen, 2010).

Researchers could analyze specific organizations or industries and develop new methods to promote IS compliance. One area that should be researched more thoroughly is organizational culture. Organizations can shape employee attitudes toward ISPP through a sound organizational culture based on mutual values and discussed factors influencing overcoming IS threats and complying with ISPP (Karlsson et al., 2022). Some of the strategies that should be adopted by organizations to ensure this compliance are:

- Security should be incorporated into an organization's vision and mission statements.
- Organizations should provide security awareness programs, find creative and fun ways to present them and make them effective enough to increase the ability of each employee to assess threats.
- After receiving training on security, employees should be held accountable for their decisions.
- It is important to recognize and reward employees who have completed security programs (Romeo, n.d.).

CONCLUSION

Because of the increasingly critical role IS plays in a growing number of fields, organizations often provide training or instructions in this regard, but employees might not comply for various reasons. It is, therefore, important for organizations to encourage a culture that values security policy. This study investigated factors taken from social bond theory and involvement theory to understand their impact on employee ISPP compliance. These factors included attachment, commitment, personal belief, IS knowledge sharing, collaboration, intervention, and experience. All factors were found to motivate employees, positively influence their attitude, raise their awareness, and help them comply with an organization's policies. Taking these factors into consideration could thus help organizations mitigate IS threats in the future.

ACKNOWLEDGMENT

This research was funded by Researchers Supporting Project RSP2023R453 at King Saud University, Riyadh, Saudi Arabia.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, *52*(1), 27–58. doi:10.1146/annurev.psych.52.1.27 PMID:11148298

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 162687–162705. doi:10.1109/ACCESS.2021.3132574

Almomani, A., Al-Nawasrah, A., Alomoush, W., Al-Abweh, M., Alrosan, A., & Gupta, B. B. (2021). Information management and IoT technology for safety and security of smart home and farm systems. *Journal of Global Information Management*, *29*(6), 1–23. doi:10.4018/JGIM.20211101.oa21

Almuqrin, A., Mutambik, I., Alomran, A., Gauthier, J., & Abusharhah, M. (2022). Factors influencing public trust in open government data. *Sustainability (Basel)*, *14*(15), 1–13. doi:10.3390/su14159765

Almuqrin, A., Mutambik, I., Alomran, A., & Zhang, J. Z. (2023). Information system success for organizational sustainability: Exploring the public institutions in Saudi Arabia. *Sustainability (Basel)*, *15*(12), 1–27. doi:10.3390/su15129233

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829–841. doi:10.1007/s00779-021-01551-2

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security*, *26*(4), 420–436. doi:10.1108/ICS-09-2017-0063

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. doi:10.1037/0033-2909.103.3.411

Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences (Basel, Switzerland)*, *12*(9), 4102. doi:10.3390/app12094102

Astin, A. W. (1999). Student involvement: A developmental theory for higher education. *Journal of College Student Development*, *40*(5), 518–529.

Bauer, S., Bernrolder, E., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. doi:10.1016/j.cose.2017.04.009

Benzel, E. (2021). Experience. *World Neurosurgery*, *156*, xiii. doi:10.1016/j.wneu.2021.09.096 PMID:34802682

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviors. *Computers in Human Behavior*, *87*, 87–97. doi:10.1016/j.chb.2018.05.023

Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing, 1*(1), 55–86.10.1207/S15327574IJT0101_4

Carmi, G., & Bouhnik, D. (2020). The effect of rational based beliefs and awareness on employee compliance with information security procedures: A case study of a financial corporation in Israel. *Interdisciplinary Journal of Information, Knowledge, and Management*, *15*, 109–125. doi:10.28945/4596

Chen, C., Cai, Z., & Wen, D.-W. (2022). Designing and evaluating an automatic forensic model for fast response of cross-border e-commerce security incidents. *Journal of Global Information Management*, *30*(2), 1–19. doi:10.4018/JGIM.20220301.oa5

Cherry, K. (2018). Attitudes and behavior in psychology. *Very Well Mind*, 1–4. https://www.academia.edu/download/58765604/attitudes-how-they-form-change-shape-behavior-279589720190401-68603-x2xhp3.pdf

Dada, O. S., Irunokhai, E. A., Shawulu, C. J., Nuhu, A. M., & Daniel, E. E. (2021). Information security awareness, a tool to mitigate information security risk: A literature review. *Innovative Journal of Science, 3*(3), 29–54. https://journals.rasetass.org/index.php/ijs/article/view/106

Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability (Basel)*, *13*(5), 2800. doi:10.3390/su13052800

Doran, R., & Larseni, S. (2016). The relative importance of social and personal norms in explaining intentions to choose eco-friendly travel options. *International Journal of Tourism Research*, *18*(2), 159–166. doi:10.1002/jtr.2042

Ekran System. (2023, March 22). *7 examples of real-life data breaches caused by insider threats*. Ekran System. https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable and measurement error. *JMR, Journal of Marketing Research*, *18*(1), 39–50. doi:10.1177/002224378101800104

Gray, B. (1989). *Collaborating: Finding common ground for multiparty problems*. Jossey-Bass., doi:10.5465/amr.1990.4309133

Greene, L., Hur, I., Levy, Y., Wang, L., & Kang, K. (2021). Assessing effects of media affordances and information security awareness on knowledge sharing in global software development. *Journal of Information Systems*, *36*(1), 111–132. doi:10.2308/ISYS-2020-072

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (6th ed.). Springer.

Hair, J. F., Hult, G. T., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R*. Springer. doi:10.1007/978-3-030-80519-7

Hayduk, L. A. (1987). *Structural equation modeling with LISREL: Essentials and advances*. Johns Hopkins University Press. doi:10.2307/3341309

Hina, S., Dominic, D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594. doi:10.1016/j.cose.2019.101594

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55.10.1080/10705519909540118

Huang, C., Guo, Y., Guo, W., & Li, Y. (2021). HackerRank: Identifying key hackers in underground forums. *International Journal of Distributed Sensor Networks*, *17*(5), 155014772110151. doi:10.1177/15501477211015145

Hwang, K., & Um, H. (2021). Social controls and bonds of public information consumer on sustainable utilization and provision for computing. *Sustainability (Basel)*, *13*(9), 5263. doi:10.3390/su13095263

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence and cognition. *Information & Management*, *51*(1), 69–79. doi:10.1016/j.im.2013.10.001

Ifinedo, P. (2018). Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal*, *31*(1), 53–82. doi:10.4018/IRMJ.2018010103

Juma'h, A. H., & Alnsour, Y. (2021). How do investors perceive the materiality of data security incidents. *Journal of Global Information Management*, *29*(6), 1–32. doi:10.4018/JGIM.20211101.oa4

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, *30*(3), 382–401. doi:10.1108/ICS-06-2021-0073

Khando, K., Gao, S., Islam, S., & Salam, A. (2021). Enhancing employees' information security awareness in private and public organizations: A systematic literature review. *Computers & Security*, *106*, 102267. doi:10.1016/j.cose.2021.102267

Kilgore, M. (2021). *8 ways to get employees to follow IT security policies*. Global Knowledge. https://www.globalknowledge.com/ca-en/resources/resource-library/articles/8-ways-to-get-employees-to-follow-it-security-policies/

Kovacevic, A., Putniki, N., & Toskovic, O. (2020). Factors related to cyber security behavior. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 125140–125148. doi:10.1109/ACCESS.2020.3007867

Liang, X., Ruan, W., Xu, Z., & Liu, J. (2022). Analysis of safe storage of network information data and financial risks under blockchain combined with edge computing. *Journal of Global Information Management*, *30*(11), 1–20. doi:10.4018/JGIM.312580

Liolis, S. (2022, May 9). Chasing invisible adversaries. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/05/09/chasing-invisible-adversaries

Liu, C., Huang, P., & Lucas, H. C. Jr. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, *37*(3), 758–787. doi:10.1080/07421222.2020.1790190

Mennens, K., van Gils, A., Odekerken-Schröder, G., & Letterie, W. (2018). Exploring antecedents of service innovation performance in manufacturing SMEs. *International Small Business Journal*, *36*(5), 500–520. doi:10.1177/0266242617749687

Mittal, B., & Lee, M. (1989). Acausal model of consumer involvement. *Journal of Economic Psychology*, *10*(3), 363–389. doi:10.1016/0167-4870(89)90030-5

Mutambik, I., Lee, J., Almuqrin, A., & Zhang, J. Z. (2023a). Transitioning to smart cities in Gulf Cooperation Council countries: The role of leadership and organisational culture. *Sustainability (Basel)*, *15*(13), 1–22. doi:10.3390/su151310490

Mutambik, I., Lee, J., Almuqrin, A., Zhang, J. Z., Baihan, M., & Alkhanifer, A. (2023b). Privacy concerns in social commerce: The impact of gender. *Sustainability (Basel)*, *15*(17), 1–22. doi:10.3390/su151712771

Othman, M., Alqahtani, F., Bari, M. A., Pee, A., Rahim, Y., & Sulaiman, H. (2019). The level of information security awareness among academic staff in IHL. *Journal of Telecommunication, Electronic and Computer Engineering*, *10*(2–5), 65–68. https://jtec.utem.edu.my/jtec/article/view/4353

Peterson, B. E., Lee, D., Henninger, A. M., & Cubellis, M. A. (2016). Social bonds, juvenile delinquency, and Korean adolescents: Intra- and inter-individual implications of Hirschi's social bonds theory using panel data. *Crime and Delinquency*, *62*(10), 1337–1363. doi:10.1177/0011128714542505

Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. *AJIS. Australasian Journal of Information Systems*, *25*. doi:10.3127/ajis.v25i0.2177

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *Management Information Systems Quarterly*, *34*(4), 757–778. doi:10.2307/25750704

Raddatz, N. I., Coyne, J. G., & Trinkle, B. S. (2020). Internal motivators for the protection of organizational data. *Journal of Information Systems*, *34*(3), 199–211. doi:10.2308/isys-18-067

Romeo, C. (n.d.). *6 ways to develop a security culture from top to bottom*. TechBeacon. https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

Safa, N. S., Maple, C., Watson, T., & Furnell, S. (2017). Information security collaboration formation in organizations. *IET Information Security*, *12*(3), 238–245. doi:10.1049/iet-ifs.2017.0257

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. doi:10.1016/j.chb.2015.12.037

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. doi:10.1016/j.cose.2015.10.006

Shih, H., Lai, K., Guo, X., Guo, X., & Cheng, T. C. (2021). Believe it or not: Employees intend to comply with information security policy because of the desire for trade-offs. *Journal of Global Information Management*, *29*(6), 1–20. doi:10.4018/JGIM.294329

Tatu, T., Ament, C., & Jaeger, L. (2018). Lessons learned from an information security incident: A practical recommendation to involve employees in information security. *Proceedings of the 51st Hawaii International Conference on System Sciences*, (pp. 3736–3745). IEEE Computer Society. doi:10.24251/HICSS.2018.471

van Rensburg, S. K. J. (2021). End-user perceptions on information security: Pragmatic lessons on social engineering attacks in the workplace in Gauteng, South Africa. *Journal of Global Information Management*, *29*(6), 1–16. doi:10.4018/JGIM.293290

Verizon. (2021). *Data breach investigations report*. Verizon. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Wang, H. (2022). Big data security management countermeasures in the prevention and control of computer network crime. *Journal of Global Information Management*, *30*(7), 1–16. doi:10.4018/JGIM.295450

Wiener, Y. (1982). Commitment in organizations: A normative view. *Academy of Management Review*, *7*(3), 418–428. doi:10.2307/257334

Wu, W., Shi, K., Wu, C., & Liu, J. (2022). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. *Journal of Global Information Management*, *30*(3), 1–16. doi:10.4018/JGIM.313188

Zhu, J., Feng, G., Liang, H., & Tsui, K. (2023). How do paternalistic leaders motivate employees' information security compliance? Building a climate and applying sanctions. *Journal of the Association for Information Systems*, *24*(3), 782–817. doi:10.17705/1jais.00794

Żywiołek, J., Rosak-Szyrocka, J., & Jereb, B. (2021). Barriers to knowledge sharing in the field of information security. *Management Systems in Production Engineering*, *29*(2), 114–119. doi:10.2478/mspe-2021-0015

Abdullah Almuqrin is an associate professor in the King Saud University Information Science Department in Saudi Arabia. He completed a master's degree in information systems at Lawrence Technological University (USA) and a PhD in information assurance at Eastern Michigan University (USA). His research interests include information systems and security, knowledge management, knowledge sharing, innovation technologies, social media (networks), privacy, and information security.

Ibrahim Mutambik is an associate professor in the Department of Information Science at King Saud University, Saudi Arabia. He received his PhD from the Informatics School at The University of Edinburgh, UK. He also received a master's degree from the Department of Computer Science of Heriot-Watt University, UK. He also received his bachelor's degree in computer from Jazan University. His current research interests focus on open data, smart cities, data management knowledge management, knowledge sharing, privacy, and security.

Abdulaziz Alomran is an assistant professor of information science at the King Saud University, Riyadh, Saudi Arabia. He is focusing on user services and user studies of information-providing agencies. His teaching interests include information services, user studies, and information resources. He holds a PhD in Library and Information Science from the School of Information Science at the University of Pittsburgh.

Justin Zhang is a faculty member in the Department of Management at Coggin College of Business at the University of North Florida. He received his PhD in business administration with a concentration in management science and information systems from Pennsylvania State University, University Park (USA). His research interests include the economics of information systems, knowledge management, electronic business, business process management, information security, and social networking. He has published research articles in various scholarly journals, books, and conference proceedings. He is the editor-in-chief of the Journal of Global Information Management. He also serves as an associate editor and an editorial board member for several other journals.