WITHDRAWN: Factors Influencing Employees' Information Security Awareness in the Telework Environment

Jie Zhen
Chongqing Technology and Business University
Kunxiang Dong
dongkx@sdufe.edu.cn

Shandong University of Finance and Economics
Zongxiao Xie
China Financial Certification Authority
Lin Chen
Shandong University of Science and Technology

Research Article

Keywords: Information security awareness, Knowledge inertia, Knowledge-attitude-behavior model, Telework

Posted Date: April 13th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1544020/v1

Additional Declarations: No competing interests reported.

EDITORIAL NOTE:

The full text of this preprint has been withdrawn by the authors while they make corrections to the work. Therefore, the authors do not wish this work to be cited as a reference. Questions should be directed to the corresponding author.

Abstract

This study aims to identify and examine factors influencing employees' information security awareness (ISA) in the telework environment. Specifically, the authors identify and examine the influence factors rooted in the knowledge-attitude-behavior (KAB) model (i.e., knowledge, attitude, and behavior) and knowledge inertia theory (i.e., experience and learning inertia). This research is among pioneering studies that identify and examine the factors influencing employees' ISA in the telework environment. Our study is also one of the first to investigate antecedents to employees' ISA rooted in the KAB model and knowledge inertia theory in a telework environment. Results show that employees' ISA in the telework environment is significantly influenced by their knowledge, behavior toward following security guidelines, and learning inertia, whereas attitude and experience inertia have no significant effect on employees' ISA.

1. Introduction

With the extensive application of online meetings, instant messaging, and document collaboration in organizations, remote work (also known as telework) could become more productive. The number of teleworkers is drastically increasing across various industries (Onken-Menke *et al.*, 2018; Dima *et al.*, 2019), especially during the COVID-19 pandemic. Telework is a work style in which employees remotely undertake their tasks without commuting to their organization's office (Hatashima and Sakamoto, 2017; Ansong and Boateng, 2018; Thulin *et al.*, 2019). Empirical studies on information security have indicated that employees are often the security weakness and flaws of information systems (IS) in organizations (Cram *et al.*, 2017; Li *et al.*, 2019; Paliszkiewicz, 2019; Hwang *et al.*, 2021). Thus, organizations create information security policies (ISPs) to provide employees with guidelines on ensuring information security in their jobs (Zhen *et al.*, 2021). Telework inevitably increases information security risks because of out-of-sight and distributed controls of the organization (Ansong and Boateng, 2018). For example, employees who choose to work from home cannot ensure that the home environment is equipped to adhere to basic security requirements. Furthermore, some organizations do not develop a telework security policy that defines teleworkers' standards, boundaries, and responsibilities to prevent and respond to security incidents. These situations could put organizations at increased risk from network security threats. Therefore, understanding what factors motivate teleworkers to plan their security behaviors deliberately and being aware of the security risks are central to help information security managers solve behavioral issues in information security management.

In the information security literature, prior studies have suggested that organizations capable of effectively improving their employees' information security awareness (ISA) have successfully reduced security risks led by employees' improper behaviors (Chen *et al.*, 2016; Bauer *et al.*, 2017; Ki-Aries and Faily, 2017; Hadlington *et al.*, 2019; Wiley *et al.*, 2020). An increasing number of organizations invest heavily in information security training programs to foster and improve their employees' ISA (Hwang *et al.*, 2021). Compared with office work, ISA plays a more critical role in shaping employees' information security behaviors in a telework environment for three reasons. First, the ISPs of some organizations do not or vaguely describe how to ensure information security in a telework environment, which increases

the possibility of risks caused by teleworkers' improper behaviors. Second, some employees' information security knowledge is relatively deficient, resulting in their lack of ability to identify the security risks associated with telework. Third, home-based telework may bring some unique security risks to the organization. For example, important customer data may be intercepted during transmission between the organization and the teleworker's smart device. However, not much work has been done in exploring the factors facilitating ISA in the telework environment. Therefore, handling telework security risks by improving employees' ISA is a thorny issue for many organizations during the COVID-19 pandemic.

Recent empirical studies have identified and examined some factors that influence employees' ISA in the traditional workplace. For example, individual difference variables, such as age, gender, education, personality, risk-taking propensity, learning style, and habits of Internet usage are associated with employees' ISA (Ogutcu *et al.*, 2016; McCormac *et al.*, 2017; Pattinson *et al.*, 2020; Hwang *et al.*, 2021). Furthermore, organizational variables, such as leadership, organizational trust, organizational culture, management participation, and ISA programs have remarkable effects on employees' ISA (Flores and Ekstedt, 2016; Bauer *et al.*, 2017; Hwang *et al.*, 2021; Koohang *et al.*, 2020). These studies have confirmed that these individual and organizational factors influence employees' ISA in organizational ISP scenarios (i.e., employees undertake their work tasks in an office environment). Past research has explored some individual and organizational factors that influence employees' ISA in the office. However, limited research has examined factors that may affect employees' ISA in a telework environment, a different way of working.

Following the analysis above, this study aims to extend the knowledge about employees' ISA by identifying and examining influence factors rooted in the knowledge-attitude-behavior (KAB) model and knowledge inertia theory in the telework environment. This line of enquiry fills critical gaps in the literature. First, the KAB model is usually used to explore whether these three factors are related to individuals' information security beliefs in recent years (McCormac *et al.*, 2017). The KAB model factors are directly related to what employees think, know, or do about information security issues (Parsons *et al.*, 2014; Ahlan *et al.*, 2015). However, whether these factors influence employees' ISA in the telework environment remains under-researched. Thus, verification of the KAB model as applied in this way is still necessary. Second, models that consider individual inertia factors to understand better employees' ISA in a paradigm swing must be developed and tested from the normal way of working to telework. The reason is that the traditional way of work to teleworking influences employees' technical and social knowledge (Taskin and Bridoux, 2010). Therefore, drawing on the KAB model and knowledge inertia theory, this study postulates that an employee's ISA is influenced by knowledge, attitude, behavior, experience, and learning inertia. The influence factor "behavior" in the current study refers to the expected employees' behaviors described in the telework security guidelines by the organization.

The structure of this paper is as follows. The next section reviews the relevant literature and theoretical background. Section 3 presents the research model and hypotheses. Section 4 introduces the methodology. Section 5 presents the findings. Section 6 demonstrates the critical discussion and conclusions for the implications, limitations, and future research directions.

2. Theoretical Background

This study aims to synthesize a theoretical model that incorporates factors rooted in the KAB model and knowledge inertia to understand their impact on employees' ISA in the telework environment. The logic for our theoretical model is influenced by the paradigm swing from the usual way of work to telework. The overall rationale for the model is that the improvement of ISA needs the support of employees' perceptions from the aspects of knowledge, attitude, and behaviors. When facing information security issues, employees generally resort to prior knowledge and experience for solutions. Thus, our study aims to extend the knowledge about employees' ISA by identifying perception-based factors rooted in the KAB model and knowledge inertia theory. A lack of a clear conceptual definition can harm constructs' original meanings and increase the risk of different interpretations (Rivard, 2014). Thus, we describe the elements of our theoretical model in the following section.

2.1 Information security awareness (ISA)

Information security researchers have defined ISA from different perspectives. For example, ISA can be defined as the extent to which employees understand the significance of their organizations' information security policies, rules, and guidelines, and the extent to which they behave following these policies, rules, and guidelines (Bulgurcu *et al.*, 2010; Wiley *et al.*, 2020). In addition, ISA refers to the focus of employees' intention on security to recognize security concerns and respond appropriately (Hwang *et al.*, 2021).

Our interest lies in examining employees' ISA in a telework environment. Considering that many organizations' ISPs do not thoroughly describe telework requirements at this stage, this study combines these two definitions and defines ISA as employees' attention on security, seeking to understand the importance of information security to recognize security concerns and respond appropriately in the telework environment.

2.2 KAB model

The KAB model includes three basic components, i.e., knowledge, attitude, and behavior. It has been widely applied to studies on information security to explain employees' ISA change (Kruger and Kearney, 2006; Kaur and Mustafa, 2013; Parsons *et al.*, 2014; Wiley *et al.*, 2020). In the KAB model, knowledge focuses on what an employee knows, attitude focuses on what an employee thinks, and behavior is about what an employee does (Kaur and Mustafa, 2013; Parsons *et al.*, 2014, 2017). Prior empirical studies have indicated that the KAB model helps predict employees' perceptions of information security.

In the context of information security management, knowledge reflects employees' cognition of information security, attitude reflects how employees view information security, and behavior reflects the actions employees should take when facing information security risks. Considering that many employees have not experimented with teleworking before, taking into account the instructions concerning the potential information security challenges of teleworking is necessary. Based on this description, we argue that attitude, knowledge, and behavior influence employees' ISA in the telework environment.

2.3 Knowledge inertia

The term inertia comes from physics, which means objects continue in a state of reset or uniform motion unless interrupted by outside forces (Liao *et al.*, 2008). In recent years, inertia is often used to describe individuals on how to tackle their work tasks or issues in a hyperdynamic environment (Sillic, 2019; Tsai *et al.*, 2020). The phenomenon of inertia in individual cognition, namely, knowledge inertia, refers to the systematic problem-solving strategy using past knowledge and experience until the situation is no longer feasible (Liao *et al.*, 2008). Furthermore, employees must actively acquire new knowledge and methods to solve their work problems, breaking the inertia (Xie *et al.*, 2016).

Although previous studies have distinguished different forms of inertia within the knowledge inertia (Xie *et al.*, 2016; Sillic, 2019), our analysis of knowledge inertia focuses on the working environment change from workplace to telework. We thus divide knowledge inertia into experience and learning inertia, according to Xie *et al*. (2016), given the dynamic environment. Specifically, experience inertia refers to resorting to prior experience and knowledge when facing situations in telework. In contrast, learning inertia refers to acquiring new knowledge and methods to solve telework problems and thus breaking the inertia of thinking in terms of working in the office.

3. Research Model And Hypothesis Development

Building on the theoretical background literature discussed above, we propose our research model and hypotheses, as shown in Fig.1 The research model illustrates the relationship between knowledge, attitude, behavior, experience inertia, learning inertia, and employees' ISA. Furthermore, this model presents gender, age, and education as control variables. In the following sections, we detail the relationships among different factors and ISA.

3.1 KAB model and ISA

As mentioned above, knowledge reflects an employee's cognition toward information security. It interacts with the organization's systems and conducts relevant procedures and daily work tasks (Wiley *et al.*, 2020). Prior studies have shown that information security knowledge profoundly impacts employees' behavioral intentions and decisions, which are very important for reducing information security risks (Hu *et al.*, 2012; Sommestad *et al.*, 2019; Zwilling *et al.*, 2020). Facing employees performing their tasks outside of the workplace unexpectedly, many organizations feel overwhelmed at telework security. In such a case, an overlooked training or education program about information security may lead to a lack of knowledge among employees (Pattinson *et al.*, 2020; Hewitt and White, 2020), resulting in their poor judgment and handling risks associated with telework. Organizations could establish formal and informal communication channels to provide support to improve employees' knowledge of telework security. Once employees have information security knowledge, they will be equipped with ISA and thus meet the security needs for work and can identify the potential risks on the device they use to telework. Thus, we hypothesize the following hypothesis:

H1. Knowledge is positively associated with employees' ISA.

Within the information security field, attitude reflects what an employee thinks about the organization's information security management (Kaur and Mustafa, 2013; Shropshire *et al.*, 2015). Employees' wrong attitude toward information security leads to their incorrect perception of information security risks (Posey *et al.*, 2014). Conversely, once employees understand the consequences of information security risks, their attitude toward information security changes (Taneja *et al.*, 2014). In such a situation, employees promote a security-conscious attitude and remain alert when faced with information security risks. This feature has been demonstrated by scholars' analysis of users' Internet-of-things usage behaviors and security awareness (Park *et al.*, 2019). In the context of this study, employees who hold a positive attitude toward telework security are likely to embody a high level of ISA. Thus, the following hypothesis is proposed:

H2. Attitude is positively associated with employees' ISA.

In this study, behavior refers to what an employee should do according to the organization's information security guidelines concerning telework. Prior studies on IS have indicated that rules and guidelines for the appropriate use of information security resources within the organization are crucial in cultivating employees' ISA (Pham, 2019; Hwang *et al.*, 2021). Several organizations developed comprehensive training workshops to arm their employees with the skills and tips during telework, including information security precautions. Many employees have been trained on handling information risks, thereby raising their awareness of the consequences of their inappropriate actions. For example, employees informed to perform a particular secure practice (e.g., password protection) may become aware of their security role in protecting the organization's other information resources (Kajzer *et al.*, 2014; Ogutcu *et al.*, 2016; Hong and Furnell, 2019). Similarly, improving employees' ISA by clearly informing employees of the secure usage behavior of devices and systems is beneficial in the telework scenario. Thus, the following hypothesis is proposed:

H3. Behavior toward following guidelines is positively associated with employees' ISA.

3.2 Knowledge inertia and ISA

Knowledge inertia includes experience and learning inertia (Xie *et al.*, 2016). On the one hand, employees' experience inertia relies on their existing knowledge structure, experience, and sources, which help them identify and handle telework security risks. For example, the organization has rules or policies concerning personal smart devices for work in the office space. These rules or guidelines are applicable in the use of employees' own devices to work remotely. Therefore, employees with strong experience inertia refrain from breaking any rules and think twice before committing any unauthorized work behaviors in a telework environment. On the other hand, employees' learning inertia depends on exploring and acquiring new ideas, knowledge, and methods to solve problems they meet in a telework setting. Thus, employees with strong learning inertia tend to seek new knowledge and methods to improve their telework skills and capability. Overall, employees with considerable experience and learning inertia can seek sources of

knowledge and attempt to seek ways of maintaining their telework security. Hence, the study presents the following hypotheses:

H4. Experience inertia is positively associated with employees' ISA.

H5. Learning inertia is positively associated with employees' ISA.

4. Research Methodology

4.1 Sample and data collection

Data used to test the research model were collected through an online survey method. Given our focus on the impact of factors on employees' ISA in a telework environment, ensuring that these participants have experience working remotely is important. Therefore, this study's survey was conducted with support from a certification authority offering IT-related services in Beijing, China. We distributed online questionnaires to employees who worked from home during the COVID-19 pandemic. The participants are full-time employees from various organizations in China. Temporary workers and retirees are not considered in the sample by setting a filter question to ensure that selected respondents had sufficient experience in telework. Participation in the survey was voluntary and anonymous, and no bonus incentive was provided for participants.

The respondents filled out the questionnaire based on their home-based telework experience. From an initial sampling of 420 employees, 373 responses were received. We excluded 68 responses due to missing values. Finally, 305 valid responses were collected with a reasonable response rate of 72.6%. A possible nonresponse bias was needed to be addressed. We compared the first 25% and the last 25% of respondents' data using a chi-squared test of the critical measurement items. No significant differences were found between the two groups. Thus, we concluded that nonresponse bias was not an issue in this study.

Table 1 presents the demographic characteristics.

Table 1 Demographic characteristics

Category	Number (N = 305)	Percentage
Gender		
Male	192	62.9%
Female	113	37.1%
Age		
18–30	196	64.3%
31–40	77	25.2%
>40	32	10.5%
Education		
Polytechnic and below	67	21.9%
Bachelor	149	48.9%
Master and PhD	89	29.2%

4.2 Measurement items

The measurement items for the variables were adapted from prior studies, and some terms were fine-tuned to suit the research context of telework. We increased content validity and assessed the clarity of the questions by verifying the measurement items using a two-step procedure. First, we invited four academic domain experts in information security management to assess the content validity of the items. After refining the items according to their suggestions, we distributed the questionnaire to three managers familiar with information security to further validate the items. All measures used a five-point Likert-type scale (1= strongly disagree, 3 = neutral, and 5 = strongly agree).

Knowledge was measured using the three-item scale adapted from Kaur and Mustafa (2006). Attitude was measured using the three-item scale adapted from Kaur and Mustafa (2006) and Ahlan *et al*. (2015). A three-item scale for behavior was adapted from Kaur and Mustafa (2006) and Ahlan *et al*. (2015). Knowledge inertia was divided into two dimensions, namely, experience and learning inertia. Experience and learning inertia were measured using three indicators drawing on the findings of Xie *et al*. (2016). Employees' ISA was measured using the four-item scale adapted from Bulgurcu *et al*. (2010) and Sillic (2019). Finally, gender, age, and education were identified as control variables. Appendix A provides the measurement items for each construct.

5. Data Analysis And Results

In this study, we analyzed the research model and tested the hypotheses by using the partial least squares (PLS) technique for three reasons. First, the PLS method can specify and test path models with latent constructs (Gefen *et al*., 2000). Second, the PLS method can be used to address a small sample

size (Gefen *et al.*, 2000); this study has (N = 373). Finally, this study employed the PLS method because it is suitable for predictive applications and theory building (Shao *et al.*, 2017; Zhen *et al.*, 2021). In particular, we used SmartPLS version 2.0 for model validation and analyses.

5.1 Measurement model

We tested the quality of the measurement model for reliability, convergent validity, and discriminant validity (Guan and Hsu, 2020). Table 2 shows that Cronbach's alpha values for all constructs were higher than the general criteria of 0.7, indicating that the items are reliable measures for their perspective constructs. That is, the instruments have good internal consistency reliability. All factor loadings are above 0.8, suggesting positive individual item reliability. These values indicated positive reliability for all constructs.

Furthermore, confirmatory factor analysis was used to evaluate convergent and discriminant validity. Table 2 shows that the composite reliability (CR) for all constructs exceeded 0.8, which was more than the recommended score of 0.7. The average variance extracted (AVE) for all constructs are above 0.5, indicating high reliability and adequate convergent validity. As shown in Table 3, the correlation between the construct and other constructs is lower than the square root of AVE for each construct, suggesting good discriminant validity of the measurement model. Based on these results, our measurement model has sound reliability and validity.

Table 2 Construct reliability and validity

Constructs	Items	Factor loadings	AVE	CR	Cronbach's alpha
Knowledge	K1	0.885	0.836	0.938	0.902
	K2	0.929			
	K3	0.825			
Attitude	A1	0.894	0.856	0.947	0.915
	A2	0.945			
	A3	0.935			
Behavior	B1	0.903	0.789	0.918	0.866
	B2	0.861			
	B3	0.901			
Experience inertia	EI1	0.958	0.892	0.961	0.939
	EI2	0.934			
	EI3	0.942			
Learning inertia	LI1	0.921	0.884	0.958	0.934
	LI2	0.954			
	LI3	0.946			
Information security awareness	ISA1	0.941	0.863	0.962	0.947
	ISA2	0.938			
	ISA3	0.911			
	ISA4	0.925			

Table 3 Correlation analysis of latent variables

	Mean	Std.	K	A	B	EI	LI	ISA
K	3.551	0.771	**0.914**					
A	3.691	0.809	0.711	**0.925**				
B	3.568	0.750	0.752	0.806	**0.888**			
EI	3.584	0.782	0.773	0.749	0.815	**0.944**		
LI	3.607	0.757	0.723	0.690	0.802	0.828	**0.940**	
ISA	3.597	0.772	0.764	0.721	0.828	0.819	0.845	**0.929**
Note: Values in the diagonal area and bold figures pertain to the square root of the AVE								

5.2 Common method variance (CMV)

This study used a single questionnaire survey to collect data for all latent constructs at one point in time, which may lead to CMV. This study took two steps to detect the CMV problem. First, we used Harman's one-factor test to conduct an exploratory factor analysis. The results indicated that the first factor only accounted for 45.036% of the total variance. Second, following Podsakoff *et al*. (2003) and Liang *et al.* (2007), we assessed CMV in PLS. Table 4 shows the result, which indicates that the proportion of variance in each observed indicator explained by its focal construct exceeded the variance explained by the method factor. Furthermore, the average substantively explained variance of the indicators was 51.2% versus 2.4% for the method constructs, suggesting that CMV was not a major concern in this study.

Table 4 CMV detection

Construct	Indicator	Substantive factor loading (R_1)	R_1^2	Method factor loading (R_2)	R_2^2
Knowledge	K1	0.732**	0.536	0.261*	0.068
	K2	0.508**	0.258	0.106	0.011
	K3	0.643**	0.413	0.139	0.019
Attitude	A1	0.773**	0.598	0.268*	0.072
	A2	0.631**	0.398	0.093	0.008
	A3	0.512**	0.262	0.126	0.016
Behavior	B1	0.819**	0.671	0.225*	0.051
	B2	0.754**	0.569	0.229*	0.052
	B3	0.676**	0.457	0.156	0.024
Experience Inertia	EI1	0.867**	0.752	0.028	0.000
	EI2	0.827**	0.684	0.145	0.021
	EI3	0.653**	0.426	0.126	0.016
Learning inertia	LI1	0.635**	0.403	0.161	0.026
	LI2	0.696**	0.484	0.059	0.003
	LI3	0.589**	0.347	0.097	0.009
Information security awareness	ISA1	0.876**	0.767	0.104	0.011
	ISA2	0.741**	0.549	0.100	0.010
	ISA3	0.825**	0.681	0.155	0.024
	ISA4	0.687**	0.472	0.138	0.019
Average		0.708	0.512	0.143	0.024
Note: $^{**}p < 0.01$; $^{*}p < 0.05$					

5.3 Correlations and multicollinearity

Table 2 indicates that the correlation values of the five inner constructs are above 0.6. Thus, we needed to compute the variance inflation factor (VIF) to eliminate any potential threat of multicollinearity. The results revealed that the highest VIF score was 4.57 (see Table 5), below 5.0 (House and Raja, 2019). Therefore, multicollinearity was not a major concern in this study.

Table 5 Results of collinearity assessment

Variables	Knowledge	Attitude	Behavior	Experience inertia	Learning inertia
VIF	2.86	3.03	4.57	4.30	3.61

5.4 Hypothesis testing

After confirming that all the measurement items have positive reliability, convergent validity, and discriminant validity, we tested the hypotheses in the research model using structural equation modeling with SmartPLS version 2.0. The results indicated that the model could explain 79.6% of the variance of employees' ISA. Table 6 summarizes the results of the hypothesis tests.

Table 6 Summary of hypotheses and results

Hypothesis	Relations	Predicted sign	Supported?
H1	Knowledge → ISA	+	Yes
H2	Attitude → ISA	+	No
H3	Behavior → ISA	+	Yes
H4	Experience inertia → ISA	+	No
H5	Learning inertia → ISA	+	Yes

The results indicated the following findings. Knowledge was positively related to ISA, thus supporting H1 ($\beta = 0.184$, $p < 0.01$). Attitude has no significant effect on employees' ISA, thus rejecting H2 ($\beta = 0.038$, $p > 0.05$). Behavior was positively related to ISA, thus supporting H3 ($\beta = 0.264$, $p < 0.05$).

The results also indicated that experience inertia has no significant effect on employees' ISA, rejecting H4 ($\beta = 0.070$, $p > 0.05$), and that learning inertia was positively related to employees' ISA, supporting H5 ($\beta = 0.416$, $p < 0.001$).

Three control variables exist in the research model: gender, age, and education. Considering that the number of control variables exceeded one, we conducted three tests following Liang *et al*. (2007). Specifically, each test only involved one control variable as an independent variable. When three control variables were included in the research model for testing, the results showed that the coefficients of the three control variables were insignificant (t values were 0.461, 0.996, and 1.235). Therefore, three control variables had no statistically significant effect on employees' ISA.

6. Discussion And Implications

Drawing on factors from the KAB model and knowledge inertia theory, this study investigates the impact of knowledge, attitude, behavior, experience inertia, and learning inertia on employees' ISA in the telework environment. We tested the research model with the data of 305 full-time teleworkers from various organizations in China. The key findings of this study are threefold. First, knowledge, behavior, and

learning inertia positively influence employees' ISA in the telework environment. Second, attitude and experience inertia has no significant impact on employees' ISA in the telework environment. Third, learning inertia plays the most crucial role in motivating employees' ISA in the telework environment. These findings offer insight into the factors facilitating employees' ISA in the telework environment. They also answer the call of Tsohou *et al.* (2015), Ogutcu *et al.* (2016), and Van de Schyff and Flowerday (2021) to apply various theories and constructs in the IS research to explore factors influencing employees' ISA in different contexts.

6.1 Theoretical implications

Our study makes important contributions to the emerging body of knowledge about information security's behavioral and organizational issues, including employees' ISA, the KAB model, and knowledge inertia. First, the extant literature has investigated factors rooted in individual differences and organizational management to explain employees' ISA in the usual way of work. To the best of our knowledge, the present study is one of the first to examine factors that influence employees' ISA in a telework environment. The results offer a theoretical explanation and empirical support for the positive impact of knowledge, behavior, and knowledge inertia on employees' ISA in the telework environment. Our results provide an opportunity for information security studies to develop information security training for other flexible ways of work, such as telework.

Second, although the KAB model has been extensively applied in prior information security literature, the role of knowledge in prompting employees' ISA has been neglected. Ahlan *et al.* (2015) provided some preliminary empirical evidence that knowledge can significantly prompt ISA. However, few studies have explored whether knowledge influences employees' ISA in a telework environment. The nature of some occupations makes performing away from the standard worksite possible. Thus, exploring the impact of knowledge on employees' ISA in the telework environment is necessary. In this study, the empirical results reveal the positive relationship between knowledge and ISA in the telework environment. This finding confirms the vital role of knowledge in improving employees' ISA in a telework environment, which extends the application of the KAB model to a telework environment.

Third, our study contributes to the knowledge inertia literature. Today's hyper-competitive environment drives employees to pursue constant training on new IT knowledge, such as cloud computing and big data. However, few studies have explored individual learning inertia in information security literature (Sillic, 2019). By applying the knowledge inertia framework of Xie *et al.* (2016), we proved that learning inertia is positively associated with employees' ISA. This finding highlights the critical role of learning inertia in shaping employees' awareness and behaviors, extending the IS literature from knowledge inertia. Thus, lengthening organizational learning literature by establishing connections between employees' ISA with learning factors from knowledge inertia theory is possible.

6.2 Practical implications

This study also has some significant practical implications for organizations to handle telework security risks. Our study shows that knowledge is an important antecedent to employee's ISA. Organizations may need to establish formal and informal communication channels for teleworkers to help them increase knowledge on information security or answer their questions during their telework. For example, suppose employees see unusual activity on the device they use in teleworking. They will know how to handle this problem and report the latter to the security operations center. Furthermore, organizations that were previously familiar with teleworking and organizations that have not experimented with teleworking before need to update existing policies with practical and actionable recommendations.

Our study also confirms the positive role of behavior toward following the organization's telework security guidelines in improving employees' ISA. For organizations with high demand for information security, employees' required information security behaviors in different positions should be described thoroughly in telework. Furthermore, organizations must emphasize the importance of complying with rules or policies regarding telework. For example, employees should be informed how to access and secure important customer data using their own devices. Therefore, we suggest that organizations design appropriate security education, training, and awareness (SETA) programs to improve employees' ISA in the telework environment.

An interesting finding of this study is that learning inertia is positively associated with ISA, whereas experience inertia has no significant effect on ISA. This finding implies that employees' previous experience on information security inside the office space does not work in a telework environment. To enhance the impact of learning inertia, organizations may need to help their employees acquire new knowledge, methods, and skills around handling telework security risks. Furthermore, organizations must encourage employees to establish a dynamic learning mechanism to expand their knowledge sources and scope relevant to telework. Therefore, we believe that information security managers need to reassess old working habits and learn new skills to manage the situation better and prevent information security threats in the telework environment.

6.3 Limitations and future research directions

Similar to most other empirical studies, this study suffers from a few limitations that offer opportunities for future research. First is the narrow set of constructs used to explain employees' ISA. Our adherence to the KAB model and knowledge inertia theory as the theoretical lens restricted the choice of constructs. Many other predictors exist as opportunities for future research with various theoretical perspectives. For example, whether positive or negative emotions employees experience in telework influence their ISA. Therefore, future studies can address this limitation using various theories. Second, the sample population for our data originated from various organizations in China. Thus, a cross-culture study could be conducted to investigate the research model further. For example, employees from a culture that emphasizes individualism may opt to place personal interests first, whereas the opposite is true for employees with a collectivist mindset (Zhen *et al.*, 2020). Therefore, future studies can address this limitation by collecting data from different cultural backgrounds. Third, the control variables in this study

(i.e., gender, age, and education) are crucial and may interact with other factors to influence employees' ISA in the telework environment. Future research could study the control variables in-depth such as the industry type of the sample, which may provide further implications.

7. Conclusions

How to effectively improve employees' ISA has received increasing attention from academics and practitioners in recent years. This study extends our understanding of employees' ISA in the telework environment. On the basis of the KAB model and knowledge inertia theory, we developed and empirically tested a theoretical model that linked knowledge, attitude, behavior, experience inertia, learning inertia, and ISA. Using the PLS method with data collected from 305 employees from various organizations in China, knowledge and behavior were found to be positively associated with ISA, whereas attitude has no significant effect on ISA in the telework environment. Furthermore, learning inertia is positively associated with ISA, whereas experience inertia has no considerable impact on ISA in the telework environment. These findings add cumulative knowledge to the research in the field of individuals' ISA and telework security. They also provide organizations with practical implications for improving information security management by implementing information security awareness programs for their teleworkers.

Statements And Declarations

Notes

Telework via a virtual private network or self-built application servers is beyond the scope of this study.

Disclosure statement

Authors declare no conflict of interest.

Acknowledgements

We would like to express our gratitude to the various stakeholders who gave us their time and sincere responses. This research was supported by some funds.

Funding This research was supported by National Natural Science Foundation of China (72102025), National Social Science Fund of China (21CGL017), Natural Science Foundation of Chongqing of China (cstc2020jcyjmsxmX0820), Natural Science Foundation of Shandong Province of China (ZR2020MG024).

Competing Interests The authors declare that they have no conflict of interest.

References

1. Ahlan, A. R., Lubis, M. and Lubis, A. R. (2015) Information security awareness at the knowledge-based institution: its antecedents and measures. Procedia Computer Science 72: 361–373.
2. Ansong, E. and Boateng, R. (2018) Organizational adoption of telecommuting: evidence from a developing country. Electronic Journal of Information Systems in Developing Countries 84(1): 1–15.
3. Bauer, S., Bernroider, E. W. N. and 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.
4. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3): 523–548.
5. Chen, X., Chen, L. and Wu, D. (2016) Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. Journal of Computer Information Systems 58(4): 1–13.
6. Cram, W. A., Proudfoot, J. G. and D'Arcy, J. (2017) Organizational information security policies: a review and research framework. European Journal of Information Systems 26(6): 605–641.
7. Dima, A., Tuclea, C., Vranceanu, D. and Tigu, G. (2019) Sustainable social and individual implications of telework: a new insight into the Romanian labor market. Sustainability 11(13): 1–12.
8. Flores, W. R. and Ekstedt, M. (2016) Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security 59(4): 26–44.
9. Gefen, D., Straub, D., and Boudreau, M. (2000) Structural equation modelling and regression: Guidelines for research practice. Communications of the Association for Information Systems 4 (7): 1–78.
10. Guan, B. and Hsu, C. (2020) The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. Internet Research 30(5): 1383–1405.
11. Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I. and Jones, K. (2019) Exploring the role of work identity and work locus of control in information security awareness. Computers & Security 81(2): 41–48.
12. Hatashima, T. and Sakamoto, Y. (2017) Study on effect of company rules and regulations in telework involving personal devices. Electronics. Information and Communication Engineers 100(10): 2458–2461.
13. Hewitt, B. and White, G. L. (2020) Cyber optimistic bias and exposure affect security incidents on hone computer. Journal of Computer Information Systems, available at: https://doi.org/10.1080/08874417.2019.1697860.
14. Hong, Y. and Furnell, S. (2019) Motivating information security policy compliance: insights from perceived organizational formalization. Journal of Computer Information Systems, available at: https://doi.org/10.1080/08874417.2019.1683781.

15. House, D. and Raja, M. K. (2020) Phishing: message appraisal and the exploration of fear and self-confidence. Behaviour & Information Technology 39(11): 1204–1224.
16. Hu, Q., Dinev, T., Paul, H. and Cooke, D. (2012) Managing employee compliance with information security policies: the critical role of top management and organization culture. Decision Science 43(4): 615–660.
17. Hwang, I., Wakefield, R., Kim, S. and Kim, T. (2021) Security awareness: The first step in information security compliance behavior. Journal of Computer Information Systems 61(4): 345–356.
18. Kajzer, M., D'Arcy, J., Crowell, C. C., Striegel, A. and Bruggen, D. V. (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security 43(4): 64–76.
19. Kaur, J. and Mustafa, N. (2013) Examining the effects of knowledge, attitude and behaviour on information security awareness: a case on SME. Research and Innovation in Information Systems, IEEE Xplore, pp. 286–290.
20. Ki-Aries, D. and Faily, S. (2017) Persona-centered information security awareness. Computers & Security 70(7): 663–674.
21. Koohang, A., Anderson, J., Nord, J. H. and Paliszkiewicz, J. (2020) Building an awareness-centered information security policy compliance model. Industrial Management & Data systems 120(1): 231–247.
22. Kruger, H. and Kearney, W. (2006) A prototype for assessing information security awareness. Computers & Security 25(4): 289–296.
23. Li, Y., Zhang, N. and Siponen, M. (2019) Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. Behaviour & Information Technology 38(5): 435–453.
24. Liang, H., Saraf, N., Hu, Q. and Xue, Y. (2007) Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS Quarterly 31(1): 59–87.
25. Liao, S., Fei, W. and Liu, C. (2008) Relationships between knowledge inertia, organizational learning and organization innovation. Technovation 28(4): 183–195.
26. McCormac, A., Zwaans, T., Parsons, K. and Calic, D. (2017) Butavicius M, Pattinson M. Individual differences and information security awareness. Computers in Human Behavior 69(4): 151–156.
27. Ogutcu, G., Testik, O. M. and Chouseinoglou, O. (2016) Analysis of personal information security behavior and awareness. Computers & Security 56(1): 83–93.
28. Onken-Menke, G., Nuesch, S. and Kroll, C. (2018) Are you attracted? do you remain? meta-analytic evidence on flexible work practice. Business Research 11(2): 239–277.
29. Paliszkiewicz, J. (2019) Information security policy compliance: leadership and trust. Journal of Computer Information Systems 59(3): 211–217.
30. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers &

Security 42(3): 165–176.

31. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security 66(3): 40–51.
32. Park, M., Oh, H. and Lee, K. (2019) Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors 19(9): 1–24.
33. Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsona, K., Calic, D. and McMormac, A. (2020) Matching training to individual learning styles improves information security awareness. Information & Computer Security 28(1): 1–14.
34. Pham, H. C. (2019) Information security burnout: identification of sources and mitigating factors from security demands and resources. Journal of Information Security and Applications 46(3): 96–107.
35. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 88 (5): 879–903.
36. Posey, C., Roberts, T. L., Lowry, P. B. and Hightower, R. T. (2014) Bridge the divide: a qualitative comparison security thought patterns between information security professionals and ordinary organizational insiders. Information & Management 51(5): 551–567.
37. Rivard, S. (2014) Editor's comments: The ions of theory construction. MIS Quarterly 38(2): iii-xiv.
38. Shao, Z., Feng, Y., and Hu, Q. (2016) Effectiveness of top management support in enterprise systems success: A contingency perspective of fit between leadership style and system life-cycle. European Journal of Information Systems 25(2): 131–153.
39. Shropshire, J., Warkentin, M. and Sharma, S. (2015) Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Computers & Security 49(2): 177–191.
40. Sillic, M. (2019) Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the shadow IT context. Computers & Security 80(1): 108–119.
41. Sommestad, T., Karlzen, H. and Hallberg, J. (2019) The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems 59(4): 344–353.
42. Taneja, A., Vitrano, J. and Gengo, N. J. (2014) Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: an empirical investigation. Computers in Human Behavior 38 (9): 159–173.
43. Taskin, L., and Bridoux, F. (2010) Telework: A challenge to knowledge transfer in organizations. The International Journal of Human Resource Management 21(13): 2503–2520.
44. Thulin, E., Vilhelmson, B. and Johansson, M. (2019) New telework, time pressure, and time use control in everyday life. Sustainability 11(11): 1–17.
45. Tsai, S., Wu, W., Ma, S., Wu, C. and Zhou, B. (2020) Benchmarking, knowledge inertia, and knowledge performance in different network structures. Enterprise Information Systems 14(5): 641–660.

46. Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2015) Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems 24(1): 38–58.
47. Van der Schyff, K., and Flowerday, S. (2021) Mediating effects of information security awareness. Computers & Security 106:102313.
48. Wiley, A., McCormac, A. and Calic, D. (2020) More than the individual: Examining the relationship between culture and information security awareness. Computers & Security 88: 1–8.
49. Xie, X., Fang, L., Zeng, S. and Huo, J. (2016) How does knowledge inertia affect firms product innovation?. Journal of Business Research 69(5): 1615–1620.
50. Zhen, J., Xie, Z., Dong, K. and Chen, L. (2021) Impact of negative emotions on violations of information security policy and possible mitigations. Behaviour & Information Technology, DOI: 10.1080/0144929X.2021.1921029.
51. Zhen, J., Xie, Z., and Dong, K. (2021) Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity. International Journal of Accounting Information Systems, 40: 100501.
52. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. and Basim, H. N. (2020) Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, available at: https://doi.org/10.1080/08874417.2019.1650676.

Figures

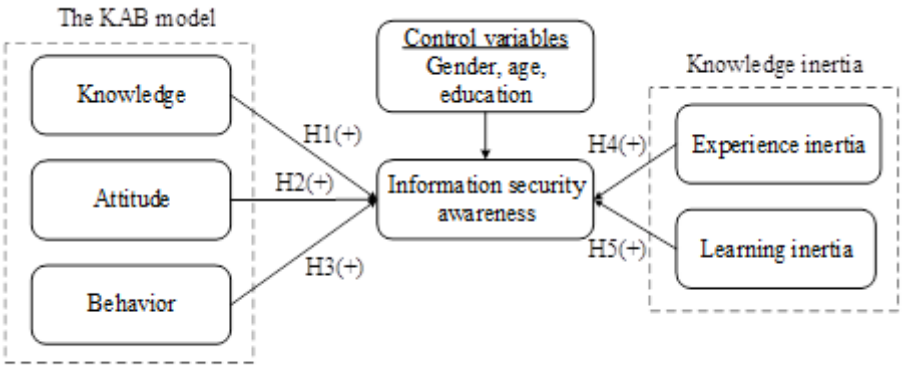

Figure 1

Research model

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Appendix.docx