Issues in Information Systems
Volume 25, Issue 3, pp. 26-35, 2024

DOI: https://doi.org/10.48009/3_iis_2024_103

The impact of organizational factors on security behavioral intentions

Linwu Gu, *Slippery Rock University, linwu.gu@sru.edu*
Jianfeng Wang, *Kutztown University, jwang@kutztown.edu*

Abstract

Previous studies have explored the implementation of information security technology and its impact on individuals and organizations in reducing security threats. However, few studies have investigated the organizational factors that influence individuals' intentions to use information security technology. This paper reviews previous research on the relationship between perceived security culture, IT use governance, perceived. organizational sanctions, and behavioral intentions. To proceed with this research, we analyzed a survey dataset containing 116 responses to empirically validate our research model. The results support the proposed hypotheses, except for the relationship between organizational sanctions and behavioral intentions, which was not significant. Perceived security culture and perceived IT use governance are found to be influential factors in promoting security behavioral intentions.

Key Words: cybersecurity, IT use governance, security culture, organizational, sanctions, security behavioral intention

Introduction

In recent years, cybersecurity has emerged as a critically important focus within the fields of information technology research and practice, with the average cost of a security incident due to cyber-attacks reaching $8.64 million (Johnson, 2022). However, the existing literature doesn't clearly explain the impacts of organizational culture and IT use governance on the Individual's behavioral intentions to use security technology.

IT use governance provides the structure, processes, and mechanisms for efficient IT decision-making, moderating security risks associated with IT implementation and ensuring effective utilization of IT resources (Lunardi et al., 2014; Weill and Ross, 2004). Additionally, these IT use governance practices have been shown to support behavioral intentions (Bowen et al., 2007).

Alongside IT use governance, information security culture also plays a crucial role in creating an environment that cultivates shared security intentions, beliefs, and practices within an organization (Van Niekerk and Von Solms, 2010). Researchers have found that employees in organizations with a strong information security culture are more likely to exhibit positive intentions toward information security behaviors (Parsons et al., 2015).

Additionally, organizational sanctions, or formal penalties imposed by employers, are effective in deterring individuals from engaging in deviant or undesirable behaviors (Vance et al., 2020). Together, IT use governance, a robust information security culture, and organizational sanctions form a solid framework for enhancing security behaviors and mitigating risks.

We propose a research model (Figure 1) to investigate the organizational factors influencing individual behavioral security intentions. In our methodology, we conducted a comprehensive review of relevant literature, focusing initially on the constructs in our research model. We then introduce our research methodology, present the analysis findings, and discuss the results.

Theoretical Background and Hypothesis Development

Perceived IT Use Governance

IT use governance, defined as the degree of employee involvement in decision-making regarding IT usage management, includes addressing information security issues and concerns (Lin et al., 2022). This approach enables organizations to efficiently manage IT decision-making and mitigate IT risks, supporting the achievement of business objectives (Grace, 2018). Implementation of IT use governance involves a set of practices aimed at managing, controlling, and ensuring the reliability of IT operations (Joshi et al., 2018). It seeks to optimize IT resource utilization and align IT with organizational objectives (Bernroider, 2008). By providing effective tools, IT use governance enhances internal IT efficiency, ensuring that IT plays a pivotal role in supporting organizational objectives (Cenfetelli, 2004).

Research explores the impact of IT use governance on individual practical information security behavior (Kearney & Kruger, 2016). From a governance-knowledge-fit viewpoint, IT use governance emphasizes empowering employees in decision-making related to security issues (Huang et al., 2010). Studies indicate that the extent of IT use governance implementation positively affects individual behavioral intentions (Wu et al., 2015).

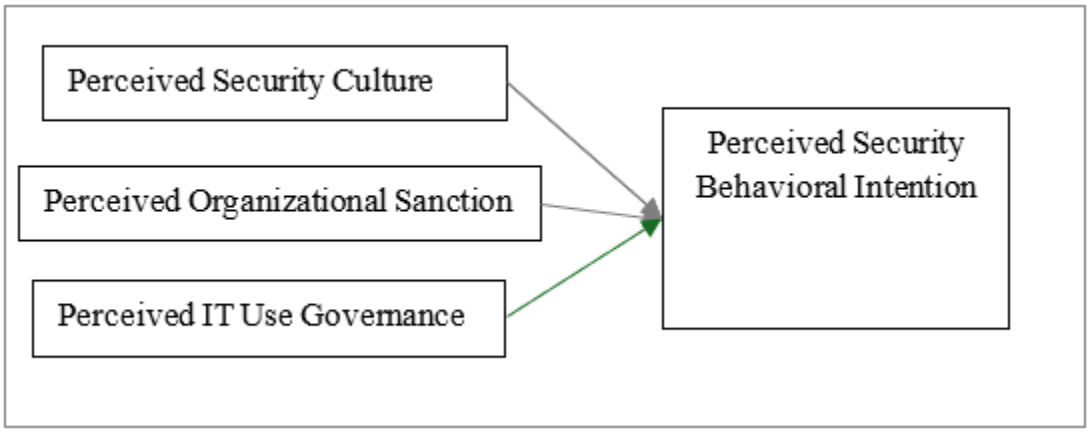

Figure 1: The Impacts of Organizational Factors on Security Behavioral Intentions

A security culture is established within a company by integrating the principles of information security into every employee's job performance (Von Solms and Von Solms, 2000). Previous research has primarily focused on exploring the concept of information security culture and identifying its foundational aspects (AlHogail, 2015). Additionally, some studies have delved into methods for assessing information security culture (Parsons et al., 2015) and analyzing existing security cultures to understand how dominant cultures can positively influence employee intentions (Da Veiga and Martins, 2017; Karjalainen et al., 2020). Connolly et al. (2019) explore the impact of perceived security culture on employees' information security

behaviors, finding that an organization-level security culture significantly shapes employees' security attitudes and behaviors. Promoting a security culture is essential for minimizing security risks within the organizational information security environment. Organizations often emphasize cultivating a security culture to mitigate a broad spectrum of potential InfoSec threats (Chen et al., 2022). When employees are aware of a security culture, they are more likely to promote good security practices within their organizations. Furthermore, an organizational security environment that supports the implementation of security technologies reinforces desired security behaviors (O'Brien et al., 2013).

Perceived Organizational Sanctions

Sanctions are formal policy controls consisting of rules and procedures designed to ensure employees' compliance and deter rule-breaking behavior (D'Arcy, et al. 2009). These sanctions are established through organizational activities implemented by individuals within an organization (Guo and Yuan, 2012). Within an organizational setting, employees interact with other members daily, influencing compliance dynamics. The application of avoidance theory in information security management has led to the examination of organizational sanctions in various studies aimed at preventing user violations of policies (D'Arcy and Herath, 2011). Previous research has emphasized that organizations use personnel sanctions to promote desirable behavior and deter rule-breaking behavior by using organizational sanctions (Tyler and Blader, 2005).

Further studies have investigated the impact of organizational sanctions on employee intentions to comply with security behaviors and attitudes (Jaeger et al., 2021). When employees understand the significance of organizational information security, they are more likely to advocate for necessary security controls (Chen et al., 2018). Implementing technologies to create an integrated platform that fosters InfoSec awareness leads to an organizational environment that encourages a security-conscious mindset (Hassandoust et al., 2022). In their efforts for protecting unclassified information along their supply chain, CIO Office of Department of Defense (2021) published cybersecurity maturity model certification assessment guide, where they refer to PS-8 personnel control as defined by NIST SP 800-53. As NIST defines in SP 800-53, personnel sanction is an organizational level control which employs a formal sanction process for individuals failing to comply with established information security policies and procedures (NIST, 2021). There is actually a discussion about third party personnel sanctions. In ISO/IEC 27001, they list people controls in Table A.1 of the document. In controls for employment terms and conditions, personnel's and the organization's responsibilities are specified. In controls for disciplinary process, it states that "a disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation" (page 20, ISO/IEC 27001:2022(E)). Both NIST SP 800-171 and SP 800-53 and ISO/IEC 27001 highlight the necessity of using such an organizational sanction.

Perceived Security Behavioral Intention

The Theory of Planned Behavior (TPB) (Ajzen, 1991) predicts an individual's intention to engage in a behavior. According to TPB, intention is recognized as a good predictor of actual behavior, driving a person to behave in a certain way. Behavioral intention is predicted by attitude, subjective norms, and perceived behavioral control, which serve as antecedents influencing behavior. Previous studies indicate a link between security intentions and the TPB factors (Vedadi et al., 2021). Similarly, the Protection Motivation Theory (Rogers 1975), suggests that higher levels of perceived responses are associated with a positive inclination to protect against security threats by adopting recommended security technologies (Johnston & Warkentin, 2010).

Organizational IT use governance can foster a favorable perception of these recommended responses. Additionally, it can be argued that lowering security risk policies is influenced by individuals' personal intentions when making decisions about security technology adoption (Djajadikerta et al., 2015). Prior research has also shown that security culture significantly influences the adoption and implementation of information technology (Palanisamy, 2007). In the research field of behavioral information security, some studies have demonstrated that formal sanctions have a greater deterrent effect on individuals who have a negative attitude toward security policy compliance (Jaeger et al., 2021).

In summary, extending from previous research, we propose the following hypotheses:

H_1: *Perceived security culture positively influences security behavioral intention.*

H_2: *Perceived Organizational sanctions positively influence security behavioral intention.*

H_3: *Perceived IT use governance positively influences security behavioral intention.*

Data Collection and Analysis

To evaluate the research model presented in Figure 1, we used a questionnaire survey method. All items were derived from previous literature and measured using a seven-point Likert scale ranging from "strongly disagree" to "strongly agree." The measurement items of the model are shown in Appendix A. We posted the online survey on our social media accounts through out accounts at wechat and facebook.com. We also post survey links through our learning management system, D2L. We obtained 116 valid responses out of 352 samples. Information on respondents' organization size, industry field, and positions was collected, but we did not record their genders or ages. The sample characteristics are listed in Table 1.

Table 1: Sample Characteristics

	Percentage (n=116)
Industry	
Technology	48 (41.4%)
College	40 (34.5%)
Bank & Financials	10 (8.6%)
Health Care	5 (4.3%)
Others	13 (11.2%)
Size- class of the organization	
Micro(1 - 9 employees)	3 (2.6%)
Small (10- 49 employees)	18(15.5%)
Medium(50-249 employees)	25(30.2%)
Large (230+ employees)	60(51.7%)
Respondent Positions	
Student/Faculty	35 (30.2%)
Software engineer/ IT professionals/	52(44.8%)
Business analyst/Consultant	21(18.1%)
Others	8 (6.9%)

We analyzed the data using partial least squares (PLS). The measurement scales, including the factor loadings, Cronbach's alphas for each construct, and the constructs' average variance extracted (AVE), are also provided in Appendix A. All Cronbach's alphas are above the 0.7 criterion, indicating high reliability. To ensure validity, we assessed both the convergent and discriminant validity of the study constructs. Discriminant validity is confirmed when the construct's AVE has a square root above 0.50 (see Table 2) and is much higher than any correlation among pairs of constructs (Gefen & Straub, 2005).

Results

We examined the relationships of the constructs (PSC- Perceived security culture, POS- Perceived organizational sanction, ITUG – IT Use governance, SBI- Security Behavioral Intention) in the model as shown in Table 3. The data indicates that the results support H1 ($\beta = 0.391$, $T = 2.012$, $p \leq 0.01$) and H3 ($\beta = 0.178$, $T = 3.367$, $p \leq 0.05$). This means that a better organizational security culture and effective IT use governance are associated with a higher and positive behavioral intention to use security technology. However, the result does not support H2 ($\beta = -0.265$, $t = 2.401$, $p = 0.1$), suggesting that perceived organizational sanctions do not significantly affect individual perceived behavioral intentions.

Table 2- Inter-Construct Correlation

	PSC	POS	ITUG	SBI
PSC	***0.796***			
POS	*0.703*	***0.853***		
ITUG	*0.612*	*0.532*	***0.743***	
SBI	*0.605*	*0.627*	*0.578*	***0.807***

Table 3 –Test Results of The Full Dataset (n= 116)

Hypotheses	β	t	
H_1: Perceived security culture -> security behavioral intention.	0.391	2.012**	supported
H_2: Perceived organizational sanctions -> security behavioral intention.	-0.265	2.401	Not supported
H_3: Perceived IT use governance -> security behavioral intention.	0.178	3.367*	supported

p* <=0.05, p** <=0.01

We also assessed the overall explanatory power of the model by examining R^2. As Figure 2 indicates, the model explains 50.7% of the variation in security behavioral intention, demonstrating the high explanatory power of the factors of the behavioral intention to use security technology. Additionally, the model accounts for 51.2% and 46.8% of the variances in perceived security culture and perceived IT use governance, indicating an acceptable level of explanatory power.

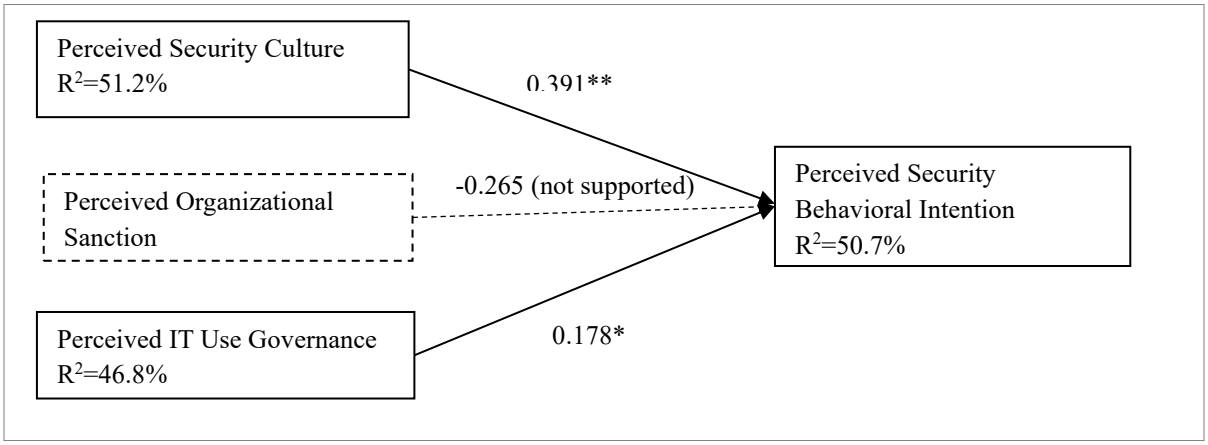

Figure -2: Estimation Results

Discussion and Conclusion

This study holds both theoretical and practical significance. It investigates organizational factors that affect the intention to use information security technology. Observing all the antecedents that were analyzed in this study, both perceived security culture and perceived IT use governance positively influence the behavioral intentions. The results of this study contribute to the organizational factors of users' behavioral intentions to use and manage security technology and provide recommendations for the organizations to further cybersecurity investment and manage their cybersecurity technologies.

However, the generalizability of our findings could be constrained by the limitations of sample size, and complexity of information security culture in different industries; therefore, it may induce much uncertainty for non-technical users in small size of organizations where cybersecurity is often managed in very different ways than medium or large-sized organizations. Future studies should analyze organizational characteristics with more different industry types on users' intentions to employ security technologies and include interactions between these variables. Nord et al. (2022) find that age and gender could be significant factors affect policy compliance. Future research may include user age and gender as variables. But policy compliance is a more dynamic and complex process and target. Not only behavioral, managerial and social factors but also regulatory requirements and technological complexity may affect policy and regulatory compliance. That's why in this research, we use security behavioral intention as the dependent variable.

In both NIST and ISO/IEC documents, organizational sanctions (NIST SP 800-53) and people controls (ISO/IEC 27001) are necessary requirements for security compliance. It is quite counterintuitive that the hypothesis on organizational sanction is not supported by the data. Future research should collect more data with a much large sample size. On the other hand, organizational sanctions are personnel sanctions or disciplinary processes. Security culture, organizational sanctions, and IT use governance can affect each other. Future research can try to include such interactions in a model. In an organization with good security culture and IT-usage management, personnel sanctions may not be used for a while. That is, employees mostly try to abide by IT usage rules and policies. Avoidance of policy or rule violation is part of the security culture in a well managed organization.

Our results show the importance of security culture and IT use governance. The cultivation of security culture and user involvement in IT use governance require the support of top management. An organization should do their due diligence to plan and implement their programs of security awareness education and training, which is essential for security culture and user involvement.

The study has several implications for future research. First, we encourage scholars to explore other organizational factors, such as organizational ethical climate, user age, gender, and organizational IT capabilities, and how they may influence information security investment decision-making differently. Second, more research and theory are needed to better understand various organizational factors affecting security management. For example, future studies could develop a more sophisticated research design for measuring cybersecurity capability maturity and additional organizational information security measures. This approach could further examine whether these new measures would better induce information security behavioral change.

References

AlHogail, A. (2015). Design and validation of information security culture framework, *Computers in Human Behavor*, 49, 567–575.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50* (2), 179-211.

Bernroider, E. W. N. (2008). IT governance for enterprise resource planning supported by the DeLone–McLean model of information systems success, *Information & Management*, 45(5), 257-269,

Bowen, P. L., Cheung, M.-YD.., and Rohde, F.H. (2007). Enhancing IT governance practices: a model and case study of an organization's efforts. *International Journal of Accounting Information Systems*, 8 (3), 191–221.

Cenfetelli, R.T. (2004). Inhibitors and enablers as dual factor concepts in technology usage, *Journal of the Association for Information Systems*, 5(11), 16.

Chen, X., Wu, D., Chen, L., and Teng, J. K.L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables, *Information & Management*, 55(8), 1049-1060,

Chen, Y., Li, Z., Fan, Y., Wang, H., and Deng, H. (2015). Progress and prospects of climate change impacts on hydrology in the arid region of northwest China, *Environmental Research*, 139, 11-19.

Chen, Y., Ramamurthy, K., and Wen, W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems,* 55(3),11–19.

Chen, Y., Luo, X., and Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence, *Information & Management*, 59 (2)

Cheng, X., Huang, X., Yang, B. and Xiao,Y. (2023). Unveiling the paradox of technostress: Impacts of technology-driven stressors on the elderly's avoidance behaviors, *Information & Management*, 60 (8).

CIO Office, Department of Defense, CMMC Self-Assessment Guide. (2021). Retrieved on 07/02/2024 from https://dodcio.defense.gov/CMMC/Documentation/

Connolly, L. Y., Lang, M., and Wall, D.S. (2019). Information security behavior: a cross-cultural comparison of Irish and US employees. *Information System Management*, 36 (4), 306–322.

Da Veiga, A. and Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures, *Computer Security*, 70, 72–94.

D'Arcy, J. and Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings, *European Journal of Information Systems*, 20, 643–658

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, *Information Systems Research* (20), 79–98.

Djajadikerta, H.G, Roni, S.M., and Trireksani, T. (2015). Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research, *Information & Management,* 52(8), 1012-1024.

Gefen, D. & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: tutorial and annotated example, *Communications of the Association for Information Systems* 16, 91–109.

Grace, R.C. (2018). Preference, resistance to change, and the cumulative decision model, *Journal of the Experimental Analysis of Behavior,* 109(1), 33–47.

Guo, K. H. and Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model, *Information & Management, 49* (6), 320-326.

Tejay, G.P.S. and Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective, *Information & Management*, 60(3)

Hassandoust, F., Subasinghage, M., Johnston, A.C . (2022) A neo-institutional perspective on the establishment of information security knowledge sharing practices, *Information & Management*, 59(1).

Huang, R. Zmud, R.W., and Price, R.L. (2010). Influencing the effectiveness of IT government practices through steering committees and communication policies, *European Journal of Information Systems,* 19 (3), 288–302.

ISO/IEC 27001:2022(E) (2002), ISO

Jaeger, L., Eckhardt, A., and Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis, *Information & Management*, 58(3)

Johnston, A.C.& Warkentin M. (2010). Fear appeals and information security behaviors: An empirical study, *MIS Q*uarterly, 34 (3) 549–566.

Johnson, J. (2022). Average Organizational Cost to a Business in the United States. *Statista*

Joshi, A., Bollen,L., Hassink, H., De Haes, S., and Grembergen,W.V. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, 55(3) 368-380

Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. (2020). Universal and culture- dependent employee compliance of information systems security procedures. *Journal Global Information Technology Management*, 23(1), 5–24.

Kearney, W. D. and Kruger, H.A. (2016). Can perceptual differences account for enigmatic information security behavior in an organization? Computer Security, 61, 46–58.

Lin, C., Wittmer, J. L. S., and. Luo, X.R. (2022) Cultivating proactive information security behavior and individual creativity: the role of human relations culture and IT use governance. *Information & Management*, 59, 1–13.

Lunardi, G.L., Becker, J. L., Maçada, A. C. G., and Dolci, P.C. (2014) The impact of adopting IT governance on financial performance: an empirical analysis among Brazilian firms, *International Journal of Accounting Information System*, 15 (1), 66–81.

NIST, SP 800-53. (2021). https://csrc.nist.gov/pubs/sp/800/53/r4/upd3/final, retrieved 07/1/2024

Nord, J. N., Sargent, C. S., Koohang, A. & Marotta, A. (2022). Predictors of success in information security policy compliance. *Journal of Computer Information Systems*, 62(4), 863-873.

O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., & Ma, A. (2013). Information security culture: literature review. Melbourne, The University of Melbourne.

Parsons, K., Young, E. (2015). Butavicius, M., McCormac, A., Pattinson, M., and Jerram, C. (2015). The influence of organizational information security culture on cybersecurity decision making, *Journal of Cognitive Engineering and Decision Making* 9 (2), 117–129.

Palanisamy, R. (2007). "Organizational Culture and Knowledge Management in ERP Implementation: An Empirical Study," *Journal of Computer Information Systems*, 48(2), 100-120.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change". *Journal of Psychology*. 91 (1): 93–114.

Tyler, T.R. and Blader, S.L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal 48*, 1143–1158.

Van Niekerk, J.F. and Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security* 29(4), 476-486.

Vance, A. Siponen, M.T. and Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures, *Information & Management*, 57 (4)

Vedadi, A., Warkentin, M., and Dennis, A. (2021). Herd behavior in information security decision-making. *Information & Management*, 58(8).

Von Solms, R., and Von Solms, B. (2000). From policies to culture. *Computers & Security*, 23(4) 275-279.

Wu, S.P.-J., Straub, D. W., and Liang, T.-P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: insights from a matched survey of business and IT managers, *MIS Quarterly* 39 (2),497–518.

Appendix A

Scale	Item	Sources	Factor Loading	AVE
Perceived Security Culture *Cronbach's Alpha=0.832*	1. Employees in my organization value the importance of security of information and computer systems 2. In my organization, a culture exists that promotes good security and privacy practices. 3. Security has traditionally been considered an important organizational value. 4. Practicing good security of information and computer systems is the accepted way of doing business in my organization. 5. The overall environment in my organization fosters security-minded thinking in all our actions. 6. Information and systems security is a key norm shared by all organizational members/ employees.	*Chen et al. 2015*	0.903 0.876 0.890 0.862 0.885 0.874	0.634
Perceived IT Use Governance *Cronbach's Alpha=0.829*	1. IT use management decisions in my organization is typically made by IT department at the corporate level. 2. Decision making regarding IT us management activities is well performed in our organization. 3. IT use management activities re satisfactorily addressed by decision makers in our organization.	*Lin, et al. 2022*	0.832 0.824 0.811	0.727
Perceived Organizational Sanctions *Cronbach's Alpha=0.817*	1. The likelihood my organization would punish me for engaging in the action is (very low . . . very high). 2. I will be reprimanded eventually if my organization is aware of my action. 3. If the management decides to punish me, the punishment would be (not severe at all . . . very severe	*D'Arcy, et al. 2009*	0.775 0.708 0.742	0.552
Perceived Security Behavioral intention *Cronbach's Alpha=0.806*	1. I plan to use security technology for logging onto websites and apps. 2. I intend to use security technology in the future. 3. I plan to use security technology soon. 4. I predict I will use security technology soon. 5. I expect to adopt security technology soon.	*Vedadi, et al. 2021*	0.812 0.807 0.815 0.826 0.830	0.651