Issues in Information Systems
Volume 26, Issue 3, pp. 183-193, 2025

DOI: https://doi.org/10.48009/3_iis_2025_2025_115

The impact of leadership in cybersecurity risk management on information security policy compliance and perceived information security success: The moderating role of IT complexity

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

Abstract

Recent information security research increasingly highlights the impact of complexity on data breaches. Information Technology (IT) complexity, characterized by overwhelming information, system interdependence, and rapid technological change, can impair decision-making, hinder policy compliance, and diminish overall security outcomes. This paper investigates how cybersecurity leadership promotes policy adherence and supports successful security practices, while also showing that excessive IT complexity can undermine this influence. Data from 135 subjects were collected, and the results indicate that IT complexity moderates the relationship between cybersecurity leadership and information security policy compliance.

Keywords: IT complexity, leadership in cybersecurity risk management, remote collaboration, Information security policy compliance, perceived information security success

Introduction

IT complexity refers to users' perception that technology is time-consuming and cognitively demanding, often due to the volume, diversity, and speed of information (Wood, 1986). When this complexity exceeds users' cognitive capacity, it can impair decision-making, elevate anxiety, and hinder the implementation of management policies—especially in environments overwhelmed by rapid and diverse data streams. As Schneier (2018, p. 197) observes, greater complexity involves more parts, people, and interactions, making effective solutions harder to achieve. Although technology is intended to enhance decision-making and performance, overly complex systems can frustrate users. When employees perceive that technology impedes rather than supports their work, dissatisfaction and distress may follow (Wang et al., 2014). In organizational settings, this complexity can also compromise information security. Recent studies (Liang et al., 2025; Tanriverdi et al., 2025) use large datasets to show that organizational complexity—measured through proxies like mergers or service diversity—can predict data breach risks.

In such environments, effective cybersecurity leadership becomes crucial. Leadership defines strategic direction and promotes employee engagement in policy compliance. Strong leadership in risk management has been shown to increase adherence to information security policies (Posey et al., 2015), particularly when employees recognize elevated threat levels. However, rising IT and organizational complexity may weaken the influence of leadership on compliance. Fragmented oversight, shifting risks, and intricate

regulations can diminish leaders' ability to enforce top-down governance. These challenges require additional support mechanisms.

One aspect of effective cybersecurity leadership is the provision of IT security training. As part of broader leadership efforts to manage cybersecurity risks, such training helps raise employee awareness, improve vulnerability detection, and encourage secure behaviors such as regular updates and strong password practices (Datta & Krancher, 2024). By investing in these educational initiatives, leaders help reduce the perceived burden of compliance and reinforce shared security expectations (Fard Bahreini et al., 2023). Research also shows that employees with strong organizational commitment are more likely to adhere to policies, even when doing so involves personal inconvenience (Hwang & Cha, 2018; Meyer et al., 2004). Ultimately, higher levels of policy compliance contribute to stronger perceptions of information security success. When employees consistently follow security policies, it supports the credibility and overall effectiveness of an organization's security program.

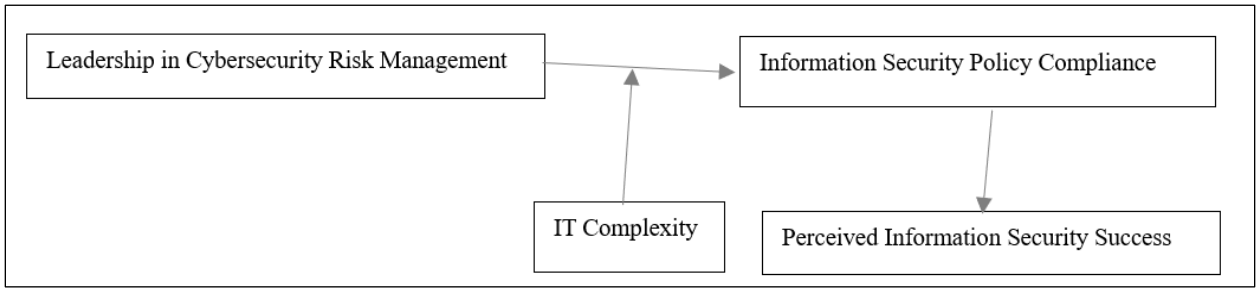

Figure 1. The Impact of Leadership in Cybersecurity Risk Management on Information Security Policy Compliance and Perceived Information Security Success

Theory Foundation and Literature Review

High information security policy compliance contributes to positive perceptions of information security success when organizations actively promote adherence to security controls, emphasize data protection, recognize the value of their security programs, trust their effectiveness in safeguarding critical assets, and maintain a proper risk-control balance. Cybersecurity leadership plays a pivotal role in shaping these perceptions by clearly communicating policy objectives, modeling ethical behavior, and fostering a culture of trust that encourages voluntary compliance. In contrast, weak leadership often relies on punitive enforcement, leading to unsustainable compliance. Effective leadership can transform reluctant compliers into willing participants, thereby strengthening overall security posture. This relationship is further moderated by IT complexity, which affects how leadership influences policy compliance (Cram et al., 2019; Willison et al., 2018; Liu et al., 2020).

Information Security Policy Compliance

Information security policy compliance refers to employees' adherence to security policies, often shaped by education, training, and awareness programs that help establish policy-related norms (Hu et al., 2012). These policies require employees to internalize security practices based on either moral obligations or role responsibilities (Siponen, 2000). Employees with positive attitudes associate compliance with internal norms, while others rely more on external motivators such as penalties (Yazdanmehr & Wang, 2016). Pogarsky (2002) distinguishes between inclined compliers, who follow policies due to internal convictions, and disinclined compliers, who do so only under external pressure. While inclined compliers adhere without

the need for deterrence, disinclined compliers rely on enforcement mechanisms—highlighting the role of management in shaping compliance behavior.
Although effective risk management has been shown to support compliance, there is ongoing debate over whether training alone is sufficient to sustain user compliance. This indicates a need for motivational strategies that complement training (Jaeger et al., 2021).

Leadership in Cybersecurity Risk Management
Leadership plays a central role in shaping the attitudinal foundation of information security policy compliance (Lanz, 2017). By promoting shared values, communicating policy importance, and building trust, cybersecurity leaders can help employees move from surface-level compliance to meaningful commitment (Anderson et al., 2024). Strong leadership increases the number of inclined compliers and reduces reliance on constant monitoring or punishment systems. Conversely, weak or authoritarian leadership tends to promote compliance based on fear, which is less stable and harder to sustain (Chen et al., 2014; Matteson, 2017). Effective cybersecurity leadership involves governance, strategic alignment, and the creation of sound security policies. It also encompasses training and awareness, asset prioritization, risk assessment, physical and regulatory compliance, monitoring controls, and adapting to emerging threats (Sveen et al., 2022). Leaders must understand technical systems, security frameworks, and threats in order to oversee security initiatives and support policy adherence effectively (Choi, 2015; Loonam et al., 2022; Vedadi et al., 2024).

IT Complexity
IT complexity has been identified as a key challenge to effective cybersecurity. It creates unpredictable risks and complicates risk management (Dekker et al., 2013). Defined by factors such as system interdependencies and technical integration, IT complexity can hinder organizational performance and reduce the effectiveness of security initiatives (Ghasemaghaei, 2020; Aboagye-Darko et al., 2024). From a complex theory perspective, increased task and system complexity impairs users' ability to filter and prioritize information, leading to decision-making fatigue, confusion, and frustration (Reychav & Wu, 2016, Yener et al., 2021). Complex systems also reduce employees' ability to follow rules efficiently, resulting in lower productivity and dissatisfaction—often due to the cognitive dissonance experienced when using complicated technologies (Phillips-Wren & Adya, 2020; Ansari et al., 2024). As a result, IT complexity may weaken security policy compliance and disrupt overall security effectiveness.

Perceived Information Security Success
While technical and risk-management outcomes have long been used to evaluate information security success, recent studies highlight the importance of user-centered measures, including system usability, employee compliance, and user perceptions. Beyond reducing breaches, perceived security success incorporates subjective elements such as trust and ease of use (Dunkerley, 2011; Parsons et al., 2015). Studies have found that security initiatives are more successful when aligned with organizational values and supported by strong leadership (Anderson et al., 2024). Awareness and compliance efforts contribute significantly to perceived success. For instance, Dunkerley and Tejay (2010) emphasize the influence of organizational culture on policy violations, while Chen et al. (2022) show how user perceptions shape behavior in response to threats.

Focusing on cybersecurity risk management helps users recognize the consequences of noncompliance and reinforces practices such as proper password usage and regular system updates. Datta and Krancher (2024) further highlight how individual perceptions of risk shape compliance or deviance. Ultimately, user perceptions—shaped by leadership, compliance behavior, and IT environment—play a critical role in determining the success of an organization's security program (Tejay & Mohammed, 2023).

Hypotheses

Based on the literature review, the following hypotheses are proposed:

H_1: *Leadership in cybersecurity risk management positively affects information security policy compliance.*

H_2: *Information security policy compliance positively affects perceived information security success.*

H_3: *Information security policy compliance mediates the relationship between leadership in cybersecurity risk management and perceived information security success.*

H_4: *IT complexity moderates the relationship between leadership in cybersecurity risk management and information security policy compliance*.

Research Methodology and Data Collection

This study employed a survey method to test the proposed research model, using a structured questionnaire. The survey included items related to leadership in cybersecurity risk Management, IT Complexity, Information security policy compliance, and perceived information security success. Of the 152 questionnaires distributed, 135 were returned with valid responses, yielding an effective response rate of 88.9%.

Among the respondents, 56.3% were male and 43.7% were female. On average, participants reported 3.8 years of cybersecurity-related education, experience, or training. Most respondents demonstrated a moderate to high level of information security knowledge, based on self-assessment. Additionally, 85% indicated a clear understanding of their organization's information security policies. Approximately 37.6% reported having personally experienced or responded to cybersecurity incidents or attacks using their personal computers. The four constructs were measured using 7-point Likert scales, incorporating established items or those adapted from prior studies, as detailed in Appendix A.

Results

We used partial least squares (PLS) to test our hypotheses. PLS, a component-based approach, is less restrictive regarding model identification and indicator distribution compared to covariance-based methods. Since PLS prioritizes predictive accuracy, it is well-suited for exploratory research like ours, which examines relationships involving leadership in cybersecurity management, information security policy compliance, and perceived information security success (Gefen et al., 2011).

Measurement validity and reliability were assessed using standard criteria. All constructs in Appendix A achieved average variance extracted (AVE) values above 0.50 (Table 1). Item loadings exceeded 0.70 (Table 2), supporting convergent validity. Discriminant validity was confirmed, as each construct's square root of AVE exceeded its inter-construct correlations, all of which were below 0.90. Table 2 further supported discriminant validity by showing that each item's loading on its corresponding construct was higher than its loadings on other constructs.

Table 1. Correlation, AVEs and Reliabilities of Constructs

Constructs	CR	AVE	1	2	3	4
Leadership in Cybersecurity Risak Management	0.8071	0.7342	***0.857***			
Information Security Policy Compliance	0.765	0.8621	0.467	***0.928***		
IT Complicity	0.8113	0.7526	0.356	0.262	***0.868***	
Perceived Information Security Success	0.7832	0.7278	0.364	0.257	0.221	***0.853***

Note: CR= composite reliability, diagonal elements represent square roots of AVEs

Table 2. Cross loadings

	Mean	SD	LCRM	LSPC	ITC	PISS
LCRM1	5.4186	1.202	**0.867**			
LCRM2	5.2527	1.235	**0.852**			
LCRM3	5.0513	1.056	**0.903**			
LCRM4	4.9784	1.278	**0.886**			
LCRM5	5.3671	1.349	**0.832**			
LSPC1	6.2568	1.635	0.429	**0.819**		
LSPC2	6.0363	1.595	0.412	**0.853**		
LSPC3	6.4375	1.554	0.351	**0.874**		
LSPC4	6.3048	1.527	0.267	**0.826**		
ITC1	4.0744	1.364	2.243	0.431	**0.773**	
ITC2	4.5223	1.376	0.365	0.363	**0.792**	
ITC3	4.7382	1.308	0.218	0.228	**0.765**	
PISS1	5.1206	1.532	0.165	0.165	0.474	**0857**
PISS2	5.8769	1.467	0.325	0.103	0.328	**0.825**
PISS3	5.6752	1.513	0.170	0.226	0.126	**0.808**
PISS4	5.0163	1.508	0.185	0.148	0.119	**0.812**
PISS5	5.1968	1.491	0.139	0.127	0.102	**0.834**

Note: LCRM(Leadership in Cybersecurity Risak Management); ISPC (Information Security Policy Compliance); ITC (IT Complicity); PISS (Perceive Information Security Success)

Figure 2 presents the PLS test results. The research model accounts for 37.9% of the variance in perceived information security success, confirming positive relationships between leadership in cybersecurity risk management and information security policy compliance ($\beta = 0.225$, $p < 0.01$), and between information security policy compliance and perceived information security success ($\beta = 0.427$, $p < 0.001$), thus supporting H1 and H2.

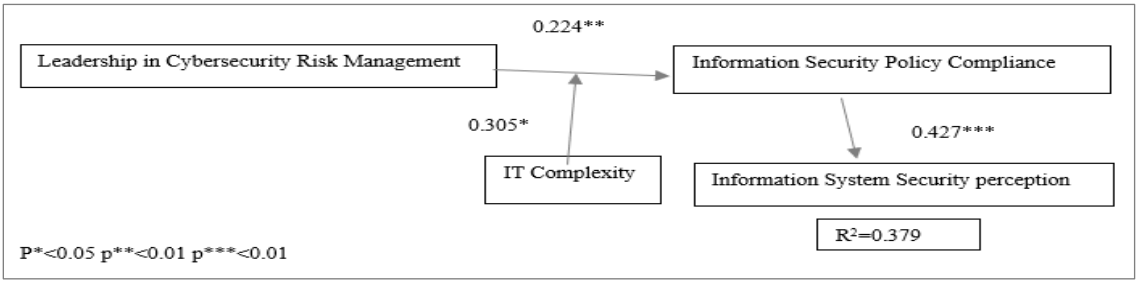

Figure 2. PLS Test Results

The mediating effect of information security policy compliance was tested using bootstrapping (Hayes, 2009). Results indicate that leadership in cybersecurity risk management does not significantly influence perceived information security success through information security policy compliance, with an indirect effect of $a \times b = 0.093$, 95% CI [–0.005, 0.141], $p > 0.05$. Since the confidence interval includes zero, the mediation effect is not significant (Preacher & Hayes, 2004). Thus, H3 is not supported.

A simple slope analysis (Cohen et al., 2003) illustrates the moderating role of IT complexity. leadership in cybersecurity risk management positively affects information security policy compliance when IT complexity is low ($\beta = 0.305$, $p < 0.05$), but not when it is high ($\beta = –0.014$, $p > 0.05$).

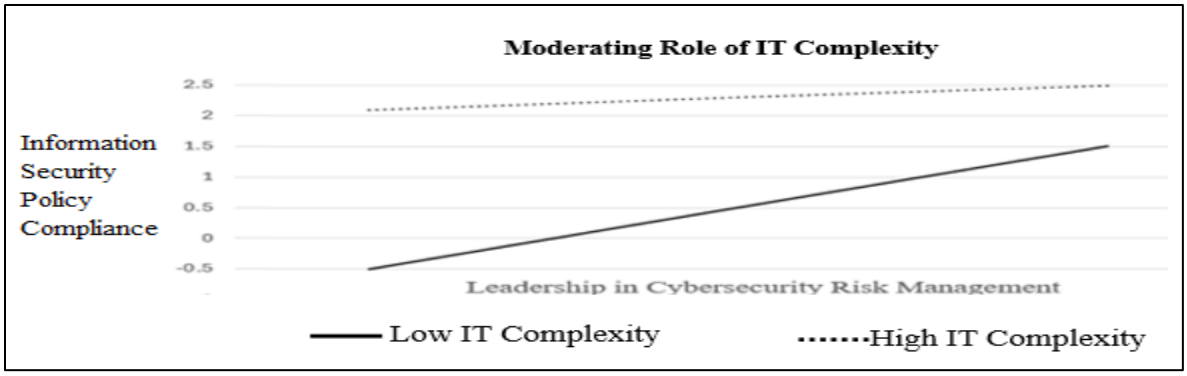

Figure 3. The Moderation Effects of IT Complexity

In summary, the PLS results support all hypotheses except H3 (Table 3).

Table 3 - Hypotheses Testing

Hypotheses	β	T- value	P-value	Hypothesis
H_1: Leadership in Cybersecurity Risk Management -> Information Security Policy Compliance	0.224	1.783	P<0.01	Supported
H_2: Information Security Policy Compliance ->Perceived Information Security Sucess	0.427	2.675	P<0.001	Supported
H_3: Leadership in Cybersecurity Risk Management -> Information Security Policy Compliance->Perceived Information Security Sucess	0.093	1.835	P>0.05	Not Supported
H_4: IT Complexty * Leadership in Cybersecurity Risk Management -> Information Security Policy Compliance	0.305	1.942	P<0.05	Supported

Discussion

This study examined the relationships among leadership in cybersecurity risk management, information security policy compliance, and perceived information security success. It also investigated the mediating role of information security policy compliance and the moderating effect of IT complexity. The findings support three of the four hypotheses. First, leadership in cybersecurity risk management significantly enhances information security policy compliance (H1), underscoring the critical role of leadership in promoting secure behaviors and fostering policy adherence. This supports prior research emphasizing leadership as a cornerstone of successful information security initiatives.

Second, information security policy compliance significantly contributes to perceived information security success (H2), indicating that compliance efforts directly impact organizational security outcomes, such as breach reduction and user confidence. However, the mediating effect of information security policy compliance between leadership and perceived success was not significant (H3). This suggests that while leadership influences compliance and compliance influence perceived success, the indirect pathway does not fully explain the relationship.

Third, IT complexity moderates the relationship between the leadership in cybersecurity risk management and security policy compliance (H4). Leadership has a stronger influence on compliance in low-complexity IT environments, but this influence diminishes under high complexity. This highlights how intricate systems can dilute leadership effectiveness—potentially due to challenges in communication, training, or policy enforcement.

These results in our study contribute to the literature on cybersecurity governance by integrating leadership theory with compliance and perceived success outcomes. The study supports the behavioral compliance model and suggests that leadership alone may be insufficient in complex IT environments, where other organizational dynamics come into play.

Limitations and Future Research

Several limitations should be acknowledged in this study. First, because the data were collected using a cross-sectional design, it is difficult to draw causal conclusions. A longitudinal approach in future studies would be more suitable for capturing how leadership, compliance, and perceived information security success changes over time. Second, this study relied on self-reported measures for compliance and security success. While these measures provide insight into participants' perceptions, they may introduce bias and might not fully reflect objective performance or actual security outcomes. Finally, although IT complexity was examined as a moderating factor, other potentially relevant variables—such as employee cybersecurity awareness, regulatory pressure, or organizational support—were not explored and could be considered in future work.

Future studies may consider integrating objective performance indicators, such as audit reports, incident rates, or system monitoring logs, to validate the self-reported responses and reduce potential bias. It would also be useful to investigate additional moderating variables, such as organizational structure, sector characteristics, or compliance culture, to better understand under what conditions leadership is effective. Addressing these aspects may offer a more comprehensive understanding of how leadership supports compliance and contributes to security success in evolving technological environments.

Practical Implications

This study highlights important implications for practice. Our findings suggest that strong, engaged leadership plays a critical role in promoting compliance with information security policies. Organizations should invest in leadership development programs that emphasize cybersecurity risk management, effective communication, and support for compliance initiatives. In highly complex IT environments, leadership alone may not be sufficient to ensure consistent compliance. Therefore, organizations should consider implementing complementary strategies such as targeted employee training, simplified and accessible policy designs, or automated controls to support secure behavior. Additionally, treating compliance not just as a procedural requirement but as a strategic element can contribute to a stronger overall cybersecurity posture.

References

Aboagye-Darko, D., Attuquayefio, S. N. B., Ankomah, N., Okronipa, A. Q., & Nyame, J. Y. (2024). Information systems research on mergers and acquisitions: A systematic literature review. *Kybernetes, 53*(12), 5560– 5581.

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management, 61*(7), 104015.

Ansari, K., Ghasemaghaei, M., & Turel, O. (2024). Cutting corners as a coping strategy in information technology use: Unraveling the mind's dilemma. *Information & Management, 61*, 104057. https://doi.org/10.1016/j.im.2024.104057

Chen, Y., Luo, X., & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & Management, 59*(2), 103575.

Chen, Y., Ramamurthy, K., & Wen, K-W. (2014). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157–188.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. Sustainability, 8(7), 638 https://doi.org/10.3390/su8070638

Cohen, J., Cohen, P., & Stephen, G. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences*. Lawrence Erlbaum Associates.

Cram, W., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525–554.

Datta, P. M., & Krancher, O. (2024). Cybersecurity end-user compliance: Password management versus update compliance. *Information & Management, 61*(1), 104060

Dekker, S., Bergström, J., Amer-Wåhlin, I., & Cilliers, P. (2013). Complicated, complex, and complaint: best practice in obstetrics. *Cognition, Technology & Work, 15*(2), 189–195.

Dunkerley, K., & Tejay, G. (2010). Theorizing information security success: Towards secure E-government *International Journal of Electronic Government Research, 6*(3), 31–41.

Dunkerley, K. (2011). Developing an information systems security success model for organizational context (Doctoral dissertation). ProQuest Dissertations Publishing. (UMI No. 3456547)

Fard Bahreini, A., Cavusoglu, H., & Cenfetelli, R. T. (2023). How "What you think you know about cybersecurity" can help users make more secure decisions. *Information & Management, 60*(7), 103860.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii–xiv.

Ghasemaghaei, M. (2020). The role of positive and negative valence factors on the impact of bigness of data on big data analytics usage. *International Journal of Information Management, 50*, 395–404.

Hayes, A. F. (2009). Beyond Baron and Kenny: Statistical mediation analysis in the new millennium. *Communication Monographs, 76*(4), 408–420.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81*, 282–293.

Jaeger, L., Eckhardt, A., & 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), 103318

Lanz, J. (2017). The chief information security officer: The new CFO of information security. *CPA Journal, 87*(6), 52–57

Liang, H., Srinivas, S., & Xue, Y. (2025). How mergers and acquisitions increase data breaches: A complexity perspective. *MIS Quarterly*. Advance online publication.

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management, 54*, 102152.

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2022). Cyber-resiliency for digital enterprises: A strategic leadership perspective. *IEEE Transactions on Engineering Management, 69*(6), 3757–3770.

Matteson, S. (2017). Why your company needs clear security policies: A cautionary tale. *TechRepublic.*

Meyer, J. P., Becker, T. E., & Vandenberghe, C. (2004). Employee commitment and motivation: A conceptual analysis and integrative model. *Journal of Applied Psychology, 89*(6), 991–1007.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & 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.

Phillips-Wren, G., & Adya, M. (2020). Decision making under stress: The role of information overload, time pressure, complexity, and uncertainty. *Journal of Decision Systems, 29*(Suppl. 1), 213–225.

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, & Computers, 36*(4), 717–731.

Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly*, 19(3), 431–452.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214.

Reychav, I., & Wu, D. (2016). The interplay between cognitive task complexity and user interaction in mobile collaborative training. *Computers in Human Behavior, 62*, 333–345.

Schneier, B., & Vance, A. (2025). "Complexity is the worst enemy of security": Studying cybersecurity through the lens of organizational complexity. *MIS Quarterly, 49*(1), 205–210.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.

Tanriverdi, H., Kwon, J., & Im, G. (2025). Taming complexity in the cybersecurity of multihospital systems: The role of enterprise-wide data analytics platforms. *MIS Quarterly, 49*(1), 243–274

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management, 60*(3), 103751

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management, 61*(5), 103968

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36–46.

Yener, S., Arslan, A., & Kilinç, S. (2021). The moderating roles of technological self-efficacy and time management in the technostress and employee performance relationship through burnout. *Information Technology & People, 34*(7), 1890–1919.

Wood, R. E. (1986). Task complexity: Definition of the construct. *Organizational Behavior and Human Decision Processes, 37*(1), 60–82.

Wang, Q., Yang, S., Liu, M., Cao, Z., & Ma, Q. (2014). An eye-tracking study of website complexity from a cognitive load perspective. *Decision Support Systems, 62*, 1–10.

Willison, R., Warkentin, M., & Johnston, A. C. (2016). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 27*(4), 347–371.

Appendix A

Scale	Items	Sources
Leadership in Cybersecurity Risk Management (LCRM)	1. Is there leadership in understanding technological controls? 2. Is there leadership in understanding risk holistically? 3. Is there leadership in understanding cybersecurity standards and frameworks? 4. Is there leadership in managing compliance with legislation, regulations, and standards? 5. Is there leadership in adapting to changing circumstances?	Adapted from Anderson et al. (2024)
IT Complexity	There was too much security information to process at once. 1. It was difficult to identify relevant information due to excessive content. 2. The level of detail exceeded what was necessary for the security task. 3. I felt mentally overloaded by the amount of security information.	Adapted from Ansari & Turel (2024)
Information Security policy compliance (ISPC)	1. Exercises discretion when discussing sensitive information. 2. Secures passwords and other access information 3. Conserves and protects organizational data 4. Adheres to informal rules devised to maintain information security	Adapted from Vedadi, et al. (2024)
Perceived Information Security Success (PISS)	1. Our organization promotes the importance of observing security controls of information systems. 2. Our organization communicates the importance of keeping data secure. 3. The information security program is valuable to the organization. *4.* The information security program should be effective at protecting critical information assets *5.* The information security program should assure that risks and information security controls are in balance. *6.*	Tejay & Mohammed (2023)