Extending the Unified Model of ISP Compliance: The Role of Meso-level Factors

Early stage paper

Dawei Wang
Missouri S&T
dwang@mst.edu

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

Alan Dennis
Indiana University
ardennis@indiana.edu

ABSTRACT

Unified model of information security compliance (UMISPC) integrates various theoretical models explaining employees' intention to comply with information security policies (ISP) (Moody et al. 2018). The UMISPC reduces many similar constructs to 11 micro-level factors. Since the introduction of UMISPC, several studies identified new constructs salient to ISP compliance at the meso- and macro-levels. This study aims to extend the well-established UMISPC by incorporating newly identified meso- and macro-level constructs. In doing so, we propose that a substantial disparity in ISP compliance exists among meso-level predictors. Expected contributions are discussed.

Keywords

UMISPC, Information security policy, non-compliance, compliance, meso, workgroup

INTRODUCTION

IS security research has long drawn upon various theoretical perspectives to explain and predict employees' insecure behaviors in the workplace (Cram et al. 2019; Moody et al. 2018). In some cases, different theoretical models offer similar or identical constructs. To examine the extent to which the competing and complementing theories overlap, Moody and colleagues (2018) reviewed and compiled 11 theories used by prior ISP research to predict ISP compliance.

Moody et al. (2018) integrated and empirically tested a unified model of ISP compliance (UMISPC) by drawing upon these findings. UMISPC is robust and has been replicated using different samples (Masuch et al. 2020; Moody et al. 2018).

UMISPC provides great insights into understanding different-yet-similar theoretical models and streamlines many predictors into fewer and more manageable factors. The UMISPC was developed based primarily on micro-level theoretical models (i.e., ones that focus on individual personality traits, cognitions, attitudes, and beliefs). Since the seminal work of UMISPC, numerous ISP studies have been published that examine meso- or macro-level factors (e.g., Johnston et al. 2019; Sarkar et al. 2020; Wang et al. 2023; Yoo et al. 2020). Meso-level factors (e.g., workgroups, professional groups) are those between the micro (individual) and macro (organizational or industry) levels. Prior research shows that meso-level factors exert a strong influence on a wide array of employee behavior (Bollmann and Krings 2016), including insecure behavior (Wang et al. 2023). A recent meta-analysis by Cram et al. (2019) suggests insufficient meso-level studies to assess the effects of workgroups. As such, we have little understanding of the effects of meso-level factors on information security. Further, since information security is a multi-level phenomenon (Hsu et al. 2015; Tsohou et al. 2015), it is imperative to incorporate newly identified meso- and macro-level factors into UMISPC.

Against this backdrop, we reviewed extant meso-level ISP research and incorporated these constructs into the UMISPC to enrich our understanding of ISP compliance. In doing so, we will also include new outcome constructs non-included in the original UMISPC and examine how the predictors of extended UMISPC affect micro- and meso- ISP compliance, respectively.

We propose that (1) a substantial disparity in ISP compliance can be observed among meso-level factors; (2) meso-level factors have at least equal predictive power as micro-level factors (from UMISPC) in explaining ISP compliance.

This research-in-progress paper offers the following expected contributions. First, the study extends UMISPC by highlighting the essential roles of meso- and macro-level predictors. Second, the study will draw a sample from the United States to increase its comparability to Finish and German samples used by UMISPC (Masuch et al. 2020; Moody et al. 2018).

RELATED RESEARCH AND RESEARCH MODEL

As UMISPC is validated and replicated (Masuch et al. 2020; Moody et al. 2018), we will theorize factors not included in the original model at the meso and macro-level.

Theorizing Meso-level Predictors of ISP Compliance/Non-compliance

Meso-level predictors are those between the micro (e.g., individual personality traits) and macro levels (e.g., organizational security policies and training, industry regulatory restrictions). In ISP literature, meso-level predictors are often considered as either coming from one's professional groups, such as physicians, nurses, and staff (Sarkar et al. 2020), or from one's workgroup(s) within the larger organizational unit (Johnston et al. 2019; Yoo et al. 2020).

The former theorizing approach theorizes meso-level factors by *profession* (Sarkar et al. 2020). A profession is "a vocation or career, especially one that involves prolonged training and a formal qualification" (OxfordEnglishDictionary 2023). A profession is a group of occupations based on the knowledge base and expertise and consists of distinct groups of professionals within an organization. For example, Sarkar et al. (2020) focused on the profession and showed that ISP non-compliance varies widely among professional groups (physicians, nurses, and staff) because of the disparity in power, prestige, and multitasking. This suggests that one's profession should

be considered to mitigate ISP non-compliance.

In the latter theorizing approach, meso-level factors are theorized by *workgroup membership* (Guo et al. 2011; Johnston et al. 2019; Wang et al. 2023; Yazdanmehr and Wang 2021; Yoo et al. 2020). Unlike a professional group, a workgroup may consist of employees from distinct professional groups with a group boundary within a functional unit. One important meso-level factor well studied and rooted in groups is subjective norms (e.g., Guo et al. 2011; Herath and Rao 2009). Subjective norms are what employees think should be done based on their perceptions of what *important others* (e.g., supervisors, top management, security professionals, and coworkers) across the organization think security compliance ought to be. Early ISP research showed that subjective norms affect ISP compliance/non-compliance (e.g., Bulgurcu et al. 2010; Herath and Rao 2009).

While prior ISP studies drawing upon subjective norms offer great insights, they do not specify the boundary of "important others." As such, terms such as "peers," "coworkers," "friends," "executives," and "colleagues" are thus often used interchangeably. Further, an employee may belong to multiple workgroups in the workplace. And "important others" may include friends from other workgroups or institutions, spouses from home, and executives who work in the same organization but rarely being observed. And executives, senior managers, and close coworkers from other units can hold very different beliefs than employees for behaviors that are socially desirable or mandated by organizational policies (Fugas et al. 2011; Westaby and Lowe 2005). Given the confusion and ambiguity of "important others," Guo et al. (2011) defined a workgroup (a functional unit including supervisors and peers) and theorized ISP non-compliance as a group phenomenon. They surveyed 335 office workers about non-malicious security violations. They found that workgroup norms (the expected approval or disapproval of

coworkers) significantly influenced the extent to which participants intended to engage in non-malicious security violations. In line with this theorizing, Yazdanmehr and Wang (2021) hypothesized peer monitoring in groups and demonstrated that monitoring group members can inhibit one's intention to violate ISPs. Finally, Wang et al. (2023) focused on the immediate workgroup, a relatively stable small group of coworkers and the supervisor with whom employees spend much of their time. They found that an employee's immediate workgroup significantly affects security decisions, over and above the micro- and macro-level predictors.

Relatedly, other newly identified meso-level predictors are workgroup collective efficacy and security knowledge coordination (Johnston et al. 2019; Yoo et al. 2020). Collective security efficacy refers to an employee group's collective understanding of its ability to recognize and react to information security incidents that align with information security policies. Using a single-group case study, Johnston et al. (2019) showed that collective security efficacy plays a part in influencing how one recognizes and responds to information security incidents. Similarly, Yoo et al. (2020) focused on workgroups. They found that workgroups facilitate workgroup security effectiveness and that security knowledge coordination is as effective as workgroup collective efficacy in improving workgroup security effectiveness.

In sum, a disparity in ISP compliance/non-compliance has been observed by profession (e.g., Sarkar et al. 2020) and workgroup membership (e.g., Johnston et al. 2019; Wang et al. 2023; Yoo et al. 2020). Together, this line of work suggests that meso-level factors are vital in advancing our understanding of ISP compliance/non-compliance above and beyond the original constructs of UMISPC. Thus, we propose that,

Proposition 1: Ceteris paribus, a substantial disparity in one's ISP compliance/non-compliance can be observed between meso-level factors.

Theoretical Base of Meso-level Predictors of ISP Compliance/Non-compliance

Extant meso-level ISP research draws up a diverse set of theories. Table 1 presents illustrative meso-level ISP studies not included in UMISPC.

Table 1. Theoretical Perspectives of Meso-level ISP Research	
Illustrative Study	**Theory Base**
(Guo et al. 2011)	Composite behavior model
(Yoo et al. 2020)	Social cognitive theory
(Johnston et al. 2019)	Social disorganization theory
(Yazdanmehr and Wang 2021)	Agency theory
(Wang et al. 2023)	Social structure and social learning

Note: we left out theoretical bases if they are used only for moderating constructs.

Composite behavior model

Developed by Eagly and Chaiken (1993), the composite behavior model (CBM) focuses on attitude-behavior relation and illustrates mechanisms by which attitudinal predictors lead to behavioral outcomes. Adapting CMB to ISP context, Guo et al. (2011) showed that workgroup norms, adapted from the construct of normative outcome expectation in CBM, was a significant meso-level predictor of non-malicious security violations.

Social cognitive theory

Social cognitive theory (SCT) is a theory of social learning. It posits that learning occurs in one's social context and explains how one's goal-directed behavior is regulated and maintained via social interaction with others (Bandura 1997).

Applying SDT to group-level (Tasa et al. 2007) and the ISP context, Yoo et al. (2020) argued that collective efficacy can regulate the collective actions of a workgroup so that the employees and managers of a workgroup can achieve security goals as a whole. They showed that workgroup collective efficacy and security knowledge coordination, meso-level constructs, were significant predictors of workgroup-level security performance.

Social disorganization theory

Social disorganization theory (SDT) is a theory of crime and deviance. Social disorganization refers to "the inability of a community to realize the common values of its members and maintain effective social controls" (Kubrin and Wo 2015, p. 122). It posits that the ecological and social properties of one's community can lead to social disorganization, thereby resulting in crime and deviance.

Drawing upon SDT, Johnston et al. (2019) adapted the construct of collective efficacy to ISP context and showed that collective security efficacy was an important meso-level predictor of security incidents.

Agency theory

Agency theory (AT) is a theory of governance and control. Agency theory suggests that peer monitoring, an informal organizational control, can help mitigate agency problems (e.g., moral hazard and opportunistic behavior) (Arnott and Stiglitz 1991) because peer monitoring helps align the behavior of agents (employees) with the interests of principals (organizations). Yazdanmehr and Wang (2021) adapted peer monitoring to the ISP context and found that peer monitoring was a significant meso-level predictor of ISP non-compliance.

Social structure and social learning

Social structure and social learning (SSSL) is a theory of deviance that focuses on one's intermediate social context (Akers 2017). SSSL highlights the role of interaction in one's social context and proposes that individual deviant behaviors are a function of social environments and immediate situations conducive to deviance. Meanwhile, SSSL explains why the workgroup effects become stronger or weaker.

Applying SSSL to ISP context, Wang et al. (2023) showed one's immediate workgroup, consisting of one's supervisor and coworkers, was a significant meso-level predictor of security decisions.

Synthesizing Meso-level Theoretical Bases

While the theoretical bases described above have unique premises and characteristics, they share a commonality –social influence and social context. For example, CBM highlights the salience of one's social context – the beliefs of coworkers and a supervisor. SCT emphasizes social reinforcement via social interaction with others. AT suggests that peer monitoring, one's social context, can be an informal organizational control. SDT foregrounds the ecological and social properties of one's community. SSSL highlights social environments and immediate situation as key inputs to deviant behavior. These meso-level ISP studies point to social influence processes and reveal the role of an employee's immediate social context in ISP compliance/non-compliance, regardless of whether the constructs are belief- or observation-based. Given the salience of the social context, we propose that,

Proposition 2: *Ceteris paribus, meso-level factors have at least equal predictive power as micro-level factors (constructs from UMISPC) in explaining ISP compliance/non-compliance.*

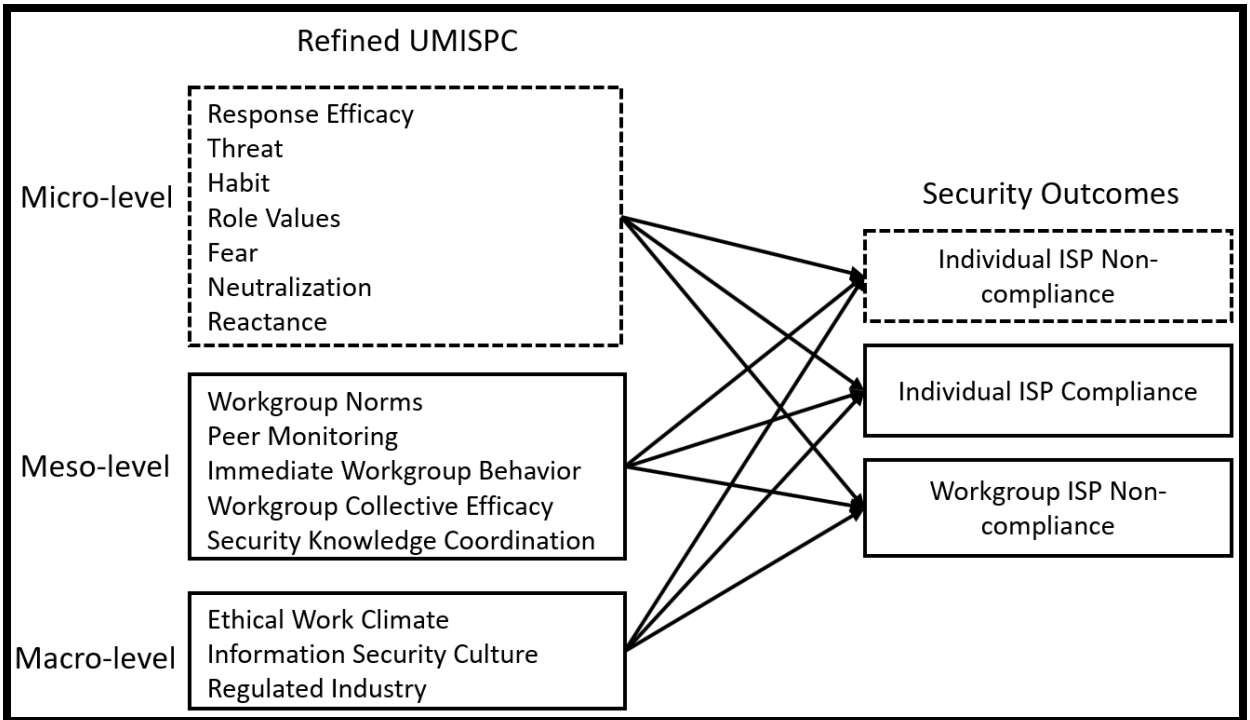

Figure 1. Research Model – Extended UMISPC

Note: boxes with dotted line indicate constructs from refined UMISPC

METHODS

Data Collection

We will employ Prolific for data collection. Original and repliaction UMISPC research collected survey responses from Finland (Moody et al. 2018) and Germany (Masuch et al. 2020). To ensure the external validity of the extended UMISPC, we will recruit respondents from the United States. In particular, qualified respondents will be working employees who 1) regularly work with a computer, 2) have a formal organizational ISP in the workplace, and 3) work in a workgroup most of the time. Once the initial screening is complete, the qualified respondents will face screening questions such as being aware of the ISPs (e.g., Johnston et al. 2016), when they last read the ISPs, and to what extent they understand the ISPs (Cram and D'Arcy 2023). Last, to further ensure the response quality, we will employ a few attention check questions throughout the survey (Abbey and Meloy 2017). Respondents who fail the attention check

questions will be disqualified. As one may belong to multiple workgroups or professions, we will ask the respondents to focus on their main workgroup from the beginning of the survey.

We will rely on procedural and statistical remedies to address common method bias. For procedure remedy, our data collection will use a temporal separation (two weeks) between our independent and dependent variables (e.g., Feng et al. 2019; Wang et al. 2023; Yazdanmehr and Wang 2021). Specifically, we plan to send out 1,500 survey invitations to respondents and try to obtain at least 800 observations from wave-2 survey responses (Soper 2023). We will use Harman's one-factor test and marker variable technique for statistical remedy.

Last, due to the sensitivity of the survey topic (ISP non-compliance), respondents may not be willing to reveal their actual intentions. As such, we will first assure respondents of the anonymity of the survey. Second, our survey will include a social desirability question (Krumpal 2013; Reynolds 1982).

Scenarios

Scenario selection. Given the abundant types of workplace insecure behaviors (e.g., ISP non-compliance), we will apply three criteria for scenario selection. First, following Yoo et al. (2020), we will draw upon a diverse set of scenarios ranging from physical security, password security, remote access, and collaborative activities. This would ensure our various scenarios sufficiently cover workgroup-level insecure behaviors. Second, the selected scenarios must be readily observable and are the most frequently occurring insecure behaviors in the workplace (Cram and D'Arcy 2023), with variation in insecurity visibility and technical challenge. Third, a panel of domain experts (e.g., CISOs and cybersecurity faculty members) will examine the selected scenarios regarding scenario relevance and readability. Less relevant scenarios will be removed, and less readable scenarios will be reworded.

To see if there is a consistent pattern across scenarios in ISP research, we follow prior scenario-based studies to ask respondents to read and respond to *all* scenarios (D'Arcy et al. 2009; Moody et al. 2018).

Measures

Dependent variables

Table 2 presents the key outcome variables we will use for the study. Following Yoo et al. (2020), we will employ a referent-shift design to capture meso-level phenomena (e.g., workgroup information security effectiveness). Chen et al. (2021) noted that the assumption of "non-compliance is merely the opposite of compliance" is problematic because "reasons for non-compliance might be different from those for compliance" (p. 1044). As such, we include both ISP compliance/non-compliance in the extended UMISPC as outcomes.

Table 2. Key Micro- and Meso-Level Outcomes in ISP Literature

Construct	Definition	Source
ISP compliance intentions	Employees' intentions to NOT follow what the character described in the scenario.	(Chen et al. 2021)
ISP non-compliance intentions	Intentions of employees to follow what the character did described in the scenario.	(Chen et al. 2021; D'Arcy et al. 2009; Siponen and Vance 2010)
Workgroup information security effectiveness	The extent to which a workgroup effectively accomplishes its information security goals	(Yoo et al. 2020)

Note: as the link between an micro-/meso-level ISP predictors and macro-level outcomes (e.g., organizational data breaches) is weak (Cram and D'Arcy 2023), we do not include macro-level outcome constructs.

Independent variables

We will use all the pre-validated constructs in refined UMISPC (see boxes with dotted line in Figure 1. Table 3 describes the final constructs and their definitions.

Table 3. Micro-level UMISPC Predictors from Moody et al. (2018) and Masuch et al. (2020)

Construct	Definition	Source
Response Efficacy	"The perceived effectiveness of the behavior in mitigating or avoiding the perceived threat"	(Moody et al. 2018)

Threat	"Perceived severity and susceptibility to a perceived potential harm"	(Moody et al. 2018)
Habit	"A regular tendency that does not require conscious thought to be compliant with the ISP"	(Moody et al. 2018)
Punishments	"Negative reinforcement that is perceived to be imposed if found to be noncompliant with the ISP"	(Moody et al. 2018)
Fear	"Negative emotional response to stimuli"	(Moody et al. 2018)
Neutralization	"Rationalized thinking that allows one to justify departure from compliance intentions"	(Moody et al. 2018)

Table 4 summarizes meso-level predictors of ISP compliance/non-compliance since the publication of Moody et al. (2018).

Table 4. Meso-level Predictors of ISP Compliance/Non-compliance

Construct	Definition	Source
Peer monitoring	Degree to which peers notice, report, and/or correct one's ISP-related wrongdoings	(Yazdanmehr and Wang 2021)
Immediate workgroup coworker insecure behavior	Observed coworkers' insecure behaviors in one's immediate workgroup	(Wang et al. 2023)
Immediate workgroup supervisor insecure behavior	Observed supervisor's insecure behaviors in one's immediate workgroup	(Wang et al. 2023)
Team member exchange (TMX)	Perceived quality of social exchange with coworkers	(Seers 1989; Seers et al. 2001)
Leader member exchange (LMX)	Perceived quality of social exchange with supervisor of one's immediate workgroup	(Graen and Uhl-Bien 1995; Huang et al. 2017)
Workgroup collective efficacy (WCE)	A workgroup's collective sense of being able to organize and conduct a series of actions required to attain the workgroup's security goals	(Yoo et al. 2020)
Security knowledge coordination (SKC)	"The process of linked security knowledge and interrelated actions to realize a collective security performance"	(Yoo et al. 2020)
Empowering security leadership (ESL)	A leadership style by which power is shared with workgroup members and that raise their level of intrinsic motivation in the workgroup	(Xue et al. 2011; Yoo et al. 2020)

Note: Number of recent workgroups will be included in the survey as a meso-level control variable

Table 5 summarizes macro-level predictors not included in UMISPC by Moody et al. (2018) and Masuch et al. (2020).

Table 5. Macro-level Predictors of Compliance/Non-compliance		
Construct	**Definition**	**Source**
Ethical work climate	"Prevailing perception of typical organizational policies, practices, and procedures that have ethical content"	(Gwebu et al. 2020; Victor and Cullen 1988)
Information security culture	"The attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e., incidents) evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time."	(Da Veiga et al. 2020; Da Veiga and Eloff 2010) and (Wiley et al. 2020)
Information security climate	Perception of one's organizational state in terms of information security as evidenced through dealings with internal and external stakeholders	(Chan et al. 2005)
Regulated industry	Industries with more regulatory restrictions	(Al-Ubaydli and McLaughlin 2017; McLaughlin and Sherouse 2019)

DISCUSSION AND EXPECTED CONTRIBUTIONS

The study aims to extend the well-established unified ISP compliance (UMISPC) model by incorporating newly identified meso- and macro-level constructs. We highlight the role of meso-level factors in understanding ISP compliance/non-compliance. With multiple competing and complementing theoretical perspectives, the extended model will provide a more complete picture of employees' insecure behavior in the workplace.

REFERENCES

Abbey, J. D., and Meloy, M. G. (2017). Attention by Design: Using Attention Checks to Detect Inattentive Respondents and Improve Data Quality. *Journal of Operations Management*, 53, 63-70.

Akers, R. L. 2017. *Social Learning and Social Structure: A General Theory of Crime and Deviance*, (1st ed.). New York, NY: Routledge.

Al-Ubaydli, O., and McLaughlin, P. A. (2017). Regdata: A Numerical Database on Industry-Specific Regulations for All United States Industries and Federal Regulations, 1997–2012. *Regulation & Governance*, 11(1), 109-123.

Arnott, R., and Stiglitz, J. E. (1991). Moral Hazard and Nonmarket Institutions: Dysfunctional Crowding out of Peer Monitoring? *The American Economic Review*, 81(1), 179-190.

Bandura, A. 1997. *Self-Efficacy: The Exercise of Control*. W.H. Freeman and Company.

Bollmann, G., and Krings, F. (2016). Workgroup Climates and Employees' Counterproductive Work Behaviours: A Social-Cognitive Perspective. *Journal of Management Studies*, 53(2), 184-209.

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.

Chan, M., Woon, I., and Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 1(3), 18-41.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X. R., Moody, G. D., and Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies through the Lens of the Extended Parallel Process Model. *Information Systems Research*, 32(3), 1043-1065. doi.org/10.1287/isre.2021.1014

Cram, W. A., and D'Arcy, J. 2023. "Barking up the Wrong Tree? Reconsidering Policy Compliance as a Dependent Variable within Behavioral Cybersecurity Research," *Proceedings of the 56th Hawaii International Conference on System Sciences*, Hawaii.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 43(2), 525-554.

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(1), 79-98.

Da Veiga, A., Astakhova, L. V., Botha, A., and Herselman, M. (2020). Defining Organisational Information Security Culture—Perspectives from Academia and Industry. *Computers & Security*, 92, 101713.

Da Veiga, A., and Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, 29(2), 196-207.

Eagly, A. H., and Chaiken, S. 1993. *The Psychology of Attitudes*. Fort Worth, TX: Harcourt Brace Jovanovich.

Feng, G., Zhu, J., Wang, N., and Liang, H. (2019). How Paternalistic Leadership Influences It Security Policy Compliance: The Mediating Role of the Social Bond. *Journal of the Association for Information Systems*, 20(11), 2.

Fugas, C. S., Meliá, J. L., and Silva, S. A. (2011). The "Is" and the "Ought": How Do Perceived Social Norms Influence Safety Behaviors at Work? *Journal of Occupational Health Psychology*, 16(1), 67-79.

Graen, G. B., and Uhl-Bien, M. (1995). Relationship-Based Approach to Leadership: Development of Leader-Member Exchange (Lmx) Theory of Leadership over 25 Years: Applying a Multi-Level Multi-Domain Perspective. *The Leadership Quarterly*, 6(2), 219-247.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28(2), 203-236.

Gwebu, K. L., Wang, J., and Hu, M. Y. (2020). Information Security Policy Noncompliance: An Integrative Social Influence Model. *Information Systems Journal*, 30(2), 220-269.

Herath, T., and Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18(2), 106-125.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research*, 26(2), 282-300.

Huang, G. H., Wellman, N., Ashford, S. J., Lee, C., and Wang, L. (2017). Deviance and Exit: The Organizational Costs of Job Insecurity and Moral Disengagement. *Journal of Applied Psychology*, 102(1), 26-42.

Johnston, A., Di Gangi, P., Howard, J., and Worrell, J. L. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems*, 20(3), 3.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. (2016). Dispositional and Situational Factors: Influences on Information Security Policy Violations. *European Journal of Information Systems*, 25(3).

Krumpal, I. (2013). Determinants of Social Desirability Bias in Sensitive Surveys: A Literature Review. *Quality & Quantity*, 47(4), 2025-2047.

Kubrin, C. E., and Wo, J. C. 2015. "Social Disorganization Theory's Greatest Challenge: Linking Structural Characteristics to Crime in Socially Disorganized Communities," in *The Handbook of Criminological Theory,* A.R. Piquero (ed.). pp. 121-136.

Masuch, K., Hengstler, S., Trang, S., and Brendel, A. B. (2020). Replication Research of Moody, Siponen, and Pahnila's Unified Model of Information Security Policy Compliance. *AIS Transactions on Replication Research*, 6(1), 13. doi.org/10.17705/1atrr.00056

McLaughlin, P. A., and Sherouse, O. (2019). Regdata 2.2: A Panel Dataset on Us Federal Regulations. *Public Choice*, 180, 43-55.

Moody, G. D., Siponen, M., and Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 42(1), 285-311.

OxfordEnglishDictionary. (2023). "Profession, N.".

Reynolds, W. M. (1982). Development of Reliable and Valid Short Forms of the Marlowe-Crowne Social Desirability Scale. *Journal of Clinical Psychology*, 38(1), 119-125.

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., and Wu, D. T. (2020). The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context. *Information Systems Research*, 31(4), 1240-1259.

Seers, A. (1989). Team-Member Exchange Quality: A New Construct for Role-Making Research. *Organizational Behavior and Human Decision Processes*, 43(1), 118-135.

Seers, A., Ford, L. R., Wilkerson, J. M., and Moormann, T. E. 2001. "The Generation of Influence: Effects of Leader–Member Exchange and Team–Member Exchange," *Southern Management Association*, pp. 340-344.

Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487.

Soper, D. S. 2023. " A-Priori Sample Size Calculator for Structural Equation Models [Software].", from https://www.danielsoper.com/statcalc

Tasa, K., Taggar, S., and Seijts, G. H. (2007). The Development of Collective Efficacy in Teams: A Multilevel and Longitudinal Perspective. *Journal of Aapplied Psychology*, 92(1), 17-27. doi.org/10.1037/0021-9010.92.1.17

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.

Victor, B., and Cullen, J. B. (1988). The Organizational Bases of Ethical Work Climates. *Administrative Science Quarterly*, 33(1), 101-125. doi.org/10.2307/2392857

Wang, D., Durcikova, A., and Dennis, A. R. (2023). Security Is Local: The Influence of Immediate Workgroup on Information Security. *Journal of the Association for Information Systems*. doi.org/10.17705/1jais.00812

Westaby, J. D., and Lowe, J. K. (2005). Risk-Taking Orientation and Injury among Youth Workers: Examining the Social Influence of Supervisors, Coworkers, and Parents. *Journal of Applied Psychology*, 90(5), 1027.

Wiley, A., McCormac, A., and Calic, D. (2020). More Than the Individual: Examining the Relationship between Culture and Information Security Awareness. *Computers & Security*, 88, 101640.

Xue, Y., Bradley, J., and Liang, H. (2011). Team Climate, Empowering Leadership, and Knowledge Sharing. *Journal of Knowledge Management*, 15(2), 299-312.

Yazdanmehr, A., and Wang, J. (2021). Can Peers Help Reduce Violations of Information Security Policies? The Role of Peer Monitoring. *European Journal of Information Systems*, 1-21. doi.org/10.1080/0960085X.2021.1980444

Yoo, C. W., Goo, J., and Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly*, 44(2), 907-931.