

Investigating Information Security Policy Noncompliance as a Local Phenomenon

Early-stage paper

Botong Xue

Kennesaw State University
bxue1@kennesaw.edu

Alaa Nehme

Mississippi State University
a.nehme@msstate.edu

Savishesh Malampallayil

SUNY Brockport
smalampallayil@brockport.edu

Abstract

Organizations often have information security policies (ISPs) in place that require employees to follow them. Despite decades of research on the topic, ISP noncompliance remains a problem. We take an alternative approach to examining the factors that underly ISP noncompliance. We argue that ISP noncompliance may be a local phenomenon, rather than a contextualized general phenomenon as treated by the extant literature. On that basis, we focus on identifying and examining the local (unique) factors that solely predict employees' ISP noncompliance and are not related to other non-ISP-related behaviors (or general organizational policy violations). To identify these factors, we adopt a sequential mixed-method research approach comprising a qualitative study (Study 1) and a quantitative cross-sectional survey (Study 2). In this research-in-progress paper, we present the results of Study 1, propose a research model based on these results, and detail our plan for conducting Study 2. We hope that this research will contribute to both the information security literature and management practice.

KEYWORDS

Information security policy noncompliance; environment security; helping others; work performance

Introduction

Employees' information security behavior has long been examined by scholars in the information systems security field. Organizational employees have been considered information security's weakest link since they have the most direct influence on organizations' security elements, including confidentiality, integrity, and availability. To regulate employees' information security behavior, organizations design and apply information security policies (ISPs), requiring employees to comply with them. ISP noncompliance (or violation) behaviors may include non-malicious violations (e.g., sharing passwords with colleagues), malicious behaviors (e.g., intentional data damage), and passive noncompliance actions (e.g., forgetting to backup data). Various studies have extensively investigated the factors that can effectively engender ISP compliance and deter ISP noncompliance, thereby enhancing our theoretical understanding of the phenomenon and recommending the respective "best" organizational practices (e.g., Aggarwal & Dhurkari, 2023; Cram et al., 2019). Particularly, scholars have investigated the antecedents of employees' ISP (non)compliance behaviors (and intentions thereof) through various theoretical perspectives. For example, previous studies have used deterrence theory (e.g., D'Arcy et al., 2009; D'arcy & Herath, 2011; Straub, 1990), fear appeal theory (e.g., Johnston et al., 2015; Johnston & Warkentin, 2010), neutralization theory (e.g., Siponen & Vance, 2010), and rationality-based theories (e.g., Bulgurcu et al., 2010), among others. Further, they have examined the role of organizational behavior factors in ISP noncompliance. These include leadership (e.g., Feng et al., 2019; Guhr et al., 2019; Xue et al., 2021), organizational culture / workgroup climate (e.g., Chan et al., 2005; Goo et al., 2014), job satisfaction (e.g., Bulgurcu et al., 2010; Chang et al., 2012), and organizational commitment (e.g., Liu et al., 2020; Safa et al., 2016), among others.

Despite these research efforts, ISP noncompliance behaviors continue to occur, negatively affecting organizational information assets (Verizon, 2024). A closer look at the existing literature indicates that it predominantly addresses ISP (non)compliance as a *contextualized general* phenomenon rather than a *localized* one. This broad (general) approach has led to adopting and testing theories that explain general behaviors across various organizational contexts, rather than ones that account for the unique aspects of ISP (non)compliance. For instance, studies testing deterrence theory within this literature show that the severity and certainty of sanctions deter ISP noncompliance. Further, studies testing neutralization theory indicate that employees engage in ISP noncompliance behaviors because they neutralize, or rationalize, them. However, these findings are broad and can be applied to (non)compliance behaviors with any type of organizational policies, not just ISPs. Such theories, while robust in their general applicability, often fail to account for the local specificities of ISP compliance, and as such may overlook context-specific factors (i.e., factors specific to ISP noncompliance). This has hindered the identification of distinct (or local) factors (and organizational factor structures) specific to ISP noncompliance, thereby compromising the “prescriptiveness” of the extant literature – as evidenced by ongoing ISP noncompliance incidents despite extensive research on the topic.

In this ongoing research, we study ISP noncompliance as a *local* phenomenon, as opposed to a contextualized general phenomenon. Our main objective is to identify the context-local factors of ISP noncompliance that do not also predict other (general) policy violation behaviors in organizations. Our overarching research question is:

(RQ) What are the localized factors that affect ISP noncompliance when studied as a local phenomenon, rather than a contextualized general phenomenon, as traditionally viewed and studied in the literature?

To answer our RQ, we employ a sequential mixed-method research design. In the first phase (Study 1), we explored the factors that locally and uniquely apply to ISP noncompliance by conducting a qualitative online survey with open-ended questions. Particularly, we qualitatively compared the factors that lead to ISP noncompliance against the ones that are general and lead to any type of policy noncompliance. On that basis, we then developed an empirical research model of ISP noncompliance as a local phenomenon. In the second phase (Study 2), we will conduct a quantitative study (an online cross-sectional survey) to test our proposed research model and hypotheses. This paper's contributions will lie in identifying the unique context-specific (localized) factors of ISP noncompliance, thereby providing the literature with a complementary view. Its practical implications will follow, uncovering new localized factors that can aid organizations enhance ISP compliance and deter ISP noncompliance.

literature & background

As a critical issue to modern organizations, employees' information security policy-related behavior has been investigated by several researchers in the past decades; such a topic has particularly had a rich history in information system security research. Spanning multiple decades, the organizational information security literature has primarily adopted theories from the fields of management, (health) psychology, criminology, sociology, and others, to explain human noncompliance behaviors. Following, the incorporated constructs that have been examined as factors that affect ISP noncompliance are from adopted theories emanating from reference disciplines. These adopted theories tested in the organization information security literature include but are not limited to Protection Motivation Theory (e.g., Johnston et al., 2015; Johnston & Warkentin, 2010), the Theory of Planned Behavior (e.g., Ifinedo, 2012; Sommestad et al., 2019), Deterrence Theory (e.g., D'Arcy et al., 2009; D'arcy & Herath, 2011; Johnston et al., 2015; Straub,

1990), Neutralization Theory (e.g., Barlow et al., 2018; D’Arcy & Teh, 2019; Siponen & Vance, 2010; Vance et al., 2020), and so on.

While these theories that have been borrowed and tested to predict ISP noncompliance have informed scholars’ and practitioners’ understanding of the phenomenon, having roots in other (i.e., non-IS) fields, they also naturally – in alignment with their original conceptualization – predict other general (i.e., non-ISP-related) misbehaviors. For example, Fear Appeal Theory, which is a theory originally from the field of healthcare, has been widely used to highlight the negative consequences of imminent *non-IS* threats through various types of persuasive messages, such as anti-smoking messages, safe-drive warnings, and other. General Deterrence Theory (GDT), another widely used theory used to investigate employees’ ISP-related behavior, has been adopted from the field of criminology; its constructs, including sanction certainty, severity, and celerity have been used to predict various *non-IS* misbehaviors, such as probation violations (Maxwell & Gray, 2000), tax noncompliance (Murphy, 2008), employee theft (Hollinger & Clark, 1983), and organizational deviance (Kura et al., 2015). Moral or ethics-related factors, which have been tested as important predictors of ISP-related behaviors (e.g., Xue et al., 2021), have also been used to predict non-security misbehaviors, such as corporate crimes (Paternoster & Simpson, 1996) and tax evasion (Wenzel, 2004). These examples extend to other adapted organizational and individual factors that predict employees’ ISP-related behaviors but are also highly related to other non-ISP-related misbehaviors.

In sum, the theories, along with their constructs, that have been adopted to study ISP noncompliance in the literature are general in nature. They may be used to explain a wide range of “noncompliance” behaviors or misbehaviors. This has led the literature to study ISP compliance as a contextualized general phenomenon as opposed to a local phenomenon, which has its own

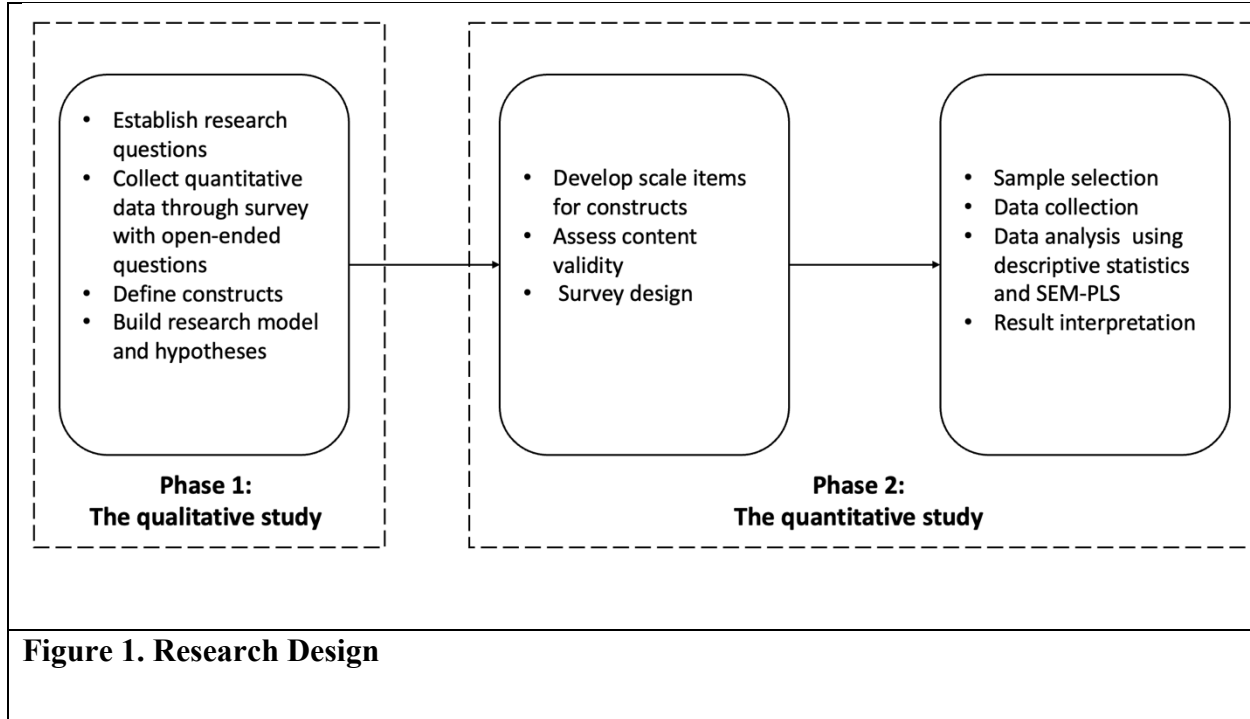
unique characteristics and factors. With ISP noncompliance persisting as a challenge in organizations, there is a pressing need to reassess the existing perspective. Specifically, we find a need to isolate the general factors that can explain both ISP and non-ISP violation behaviors – previously studied in the literature – while also identifying (and exploring) the unique factors that specifically predict ISP noncompliance. This approach allows for the study of ISP noncompliance as a localized phenomenon.

research approach

This ongoing research applies a multi-method multi-study design with two sequential phases (Figure 1): a qualitative phase (Study 1) and a quantitative phase (Study 2). This allows for developing deeper insights into the subject of interest field (Harrison & Reilly, 2011; Venkatesh et al., 2013, 2016). A multi-method design provides three benefits, including the ability to “address confirmatory and explanatory research questions,” the ability to “provide stronger inferences than a single method or worldview,” and the ability to “produce a greater assortment of divergent and/or complementary views” (Venkatesh et al., 2016). In the context of studying ISP noncompliance, it is especially useful to adopt the mixed-method research design since technologies and related security problems change frequently, making it difficult to draw insights from existing theoretical frameworks and perspectives. Further, using a mixed-methods design (with qualitative and quantitative studies) to study ISP noncompliance as a local phenomenon, as opposed to a general phenomenon as has been studied in the previous literature, is particularly useful as it allows for a comprehensive understanding of the nuanced and context-specific factors influencing X noncompliance. This approach enables the triangulation of data, providing richer insights and more robust conclusions that account for both the depth of individual experiences and the breadth of broader patterns.

As has been described previously, the main purpose of this research is identifying and examining the specific antecedents of employees' ISP noncompliance behaviors. However, since the literature adopts theories from other fields to study ISP noncompliance, thereby studying it as a contextualized general phenomenon, there is very limited research that examines specific local ISP noncompliance antecedents. Therefore, to better understand ISP noncompliance as a local phenomenon and to identify the local-specific antecedents of ISP noncompliance behavior, we followed a developmental process and conducted a qualitative study first from an interpretivist perspective with inductive reasoning. This necessitates not using a theory before data collection. Then, we plan to conduct a quantitative study by adopting a positivist perspective with deductive reasoning to test the research model and developed hypotheses. Overall, the multi-method design has two phases in this research and is influenced by the contextual research study guidelines (Hong et al., 2014). The first phase comprises a qualitative survey with open-ended questions answered by organizational employees. This phase allows for identifying the local antecedents of employees' information security policy noncompliance behavior and performing qualitative data analysis to help build our research model for the following quantitative study. The second phase comprises a quantitative cross-sectional survey for testing the research model and hypotheses.

In sum, our research follows a multi-method multi-study research design with two phases. The first phase (Study 1) comprises a qualitative study grounded in interpretivism and inductive reasoning. The second phase (Study 2) builds upon the findings of the first study and comprises a quantitative study grounded in positivism and deductive reasoning.



QUALITATIVE PHASE (STUDY 1)

In this phase, we conducted a qualitative study by using the online crowdsourcing platform, Prolific, for recruiting participants. We used Qualtrics to develop our qualitative questionnaire, which comprised open-ended questions. In this qualitative survey, we aimed to identify the local specific antecedents of ISP noncompliance. Thus, it was critical to also find out what factors contribute to violations of organizational policies not related to information security (InfoSec), along with the specific factors related to ISP noncompliance. To do so, we recruited full-time employees in the United States over 18 years old who had an ISP noncompliance experience, a non-InfoSec-related policy violation experience, or both. Specifically, we asked participants about their non-InfoSec-related policy violation experiences and ISP violation experiences separately; we inquired about the reasons for their violations. Examples of both non-InfoSec and InfoSec policy violations were provided at the beginning of the survey to mitigate any potential confusion.

Before participation, confidentiality, privacy, and voluntary participation were communicated and guaranteed in the study consent form to mitigate the response bias and improve response quality. An incentive was provided to each successful participant, and the amount was calculated based on the lowest labor cost in the United States and the estimated time needed to complete the survey.

The study was conducted in mid-August 2023, and 188 responses were received. After deleting responses that were incomplete, that had a short participation duration, and that had not met the participation requirements, 152 responses were retained for data analysis. Based on the 152 usable responses, we conducted a three-stage (initial, axial, selective coding) qualitative analysis (Corbin & Strauss, 2015) by following the grounded theory perspective, which has been previously used in many IS studies (e.g., Boudreau & Robey, 2005; Sarkar et al., 2020; Sarker & Sarker, 2009; Seidel et al., 2013, p. 201). Key codes, themes, and categories were captured during the analysis process, and the theoretical saturation was met when no new code and themes were captured (Charmaz, 2006).

At the end of our data analysis, we identified multiple antecedents of both sets of violation experiences – related to (1) non-InfoSec policies and to (2) InfoSec policies – discussed by the participants. Noteworthy is that all the identified antecedents are for previous violation behaviors, not violation intentions. As a result of the analysis, we captured insightful findings from examining the answers related to both sets of behaviors, ISP noncompliance and non-InfoSec policy violations. For example, most mentioned that their general (non-InfoSec related) policy violations included dress code violation (“I frequently violate my workplace dress code policy and show up wearing articles of clothing that are not “permitted...”), attendance policy violations (“I cut out of work 30 minutes early to go golfing with friends. I figured that since it was only 30 minutes it was not too big of a deal.”), and other work-related policy violations policy (e.g., outside-business

activities; “My company has a no outside business policy, but I do not entirely agree with it for small projects like this. Now every other weekend we do small construction gigs for extra cash.”; “Was caught driving an Uber on company time and making extra money.” “I violated a general NDA work policy when talking with friends.”). Among those violation behaviors, most were intentionally performed. The most discussed reasons for those violations were concluded to be: no supervision (“I violated it because leggings are more comfortable and my boss was not there that day.”), unclear policy (“The dress code only said that skirts or dresses must be an ‘appropriate length’ and did not specify a specific length”), and apathy (“I violate it because I don't care about a company that doesn't care for me beyond what I can provide that day. They will never notice.”)

In parallel, we identified ISP noncompliance behaviors from the data analysis as well. These included password sharing (“We shared the passwords for the main workstation with someone outside of our department as they would be working with us for a period of time.”), workplace network/equipment usage policy violations (“... streaming videos on YouTube through high-quality settings while working, breaking our “personal use” policy and effectively, hindering our other remote workers by causing a slowdown to a substantial amount of local clients working remotely.”), and email policy violations (“using their company email to send personal email correspondence to family friends and online businesses as well.”). We note that although most of the ISP violation behaviors were not performed with malicious intentions, this does not indicate that we only focused and contributed to non-malicious ISP violation behaviors. Rather, this reveals that non-malicious ISP violation behaviors were more common and easy to be performed in the day-to-day workplace.

After the ISP noncompliance behaviors were examined, we identified a variety of reasons underlying them, and conclusions were drawn by following the three-stage analysis method. At

the end of the analysis, we classified and labeled the reasons for both behaviors into categories with subcategories, such as system-related, workplace-related, supervision-related, personal factors, and so on, and each category and subcategory contained multiple reasons for policy violation behaviors. Next, we conducted a comparison between the underlying reasons of regular/general (i.e., non-InfoSec) policy violations and those of ISP violations. We noticed that several reasons were shared between the two sets of violation behaviors, such as lack of supervision, job dissatisfaction, and carelessness. As our aim was to identify the local (unique) factors that motivate ISP violation (or noncompliance) behaviors, we excluded all the shared reasons and identified the reasons that were unique to ISP noncompliance behavior; in other words, these reasons never mentioned by participants when discussing why they violated general non-InfoSec policies. At this stage, we identified four prominent unique reasons local to ISP noncompliance. We conceptualized them as constructs. These included perceived technological/systems environment security, perceived physical environment security, motivation to help others, and relative job performance utility. Table 1 lists the constructs with their sample reflective participant quotations.

ISP Violation Antecedents	Sample Quotations
Perceived technological/systems environment security	“The computer logs off within minutes automatically, but it is still policy to log out deliberately.”
Perceived physical environment security	“Our floor is secure so there is no chance of an unauthorized person getting into my computer since they are unable to get to my floor in the first place. So I do not feel the need to lock my computer each and every time that I walk away from my desk”, “...I locked my office door though so it did not cause any harm”, “I don’t normally lock my computer when I leave my desk. So while it’s against policy there is no one in the area to see my screen.”
Relative job performance utility	“... using personal email to quickly exchange the data would help them meet the deadline without further delays caused by the technical issues.”, “We use Google Drive to hold work documents and share them, we do this because it is easier to edit things in real time, and we don't have to keep emailing the document (which could also be hacked) or walking over the drives.”, “It was faster and easier especially considering the workload at the time.”
Motivation to help others	“One colleague was sharing her password with a couple of other colleagues so that they could help her complete her project.”, “ I shared a password with a colleague because they needed access to the service.”, “I was unable to open my Dropbox account to forward some document to another coworker. So, my nearby colleague overheard this and offered his password so that I can transfer the file.”

Table 1. Detailed quotations of ISP violation reasons

Hypotheses development

Based on the results of our qualitative data analysis and previous literature, we developed the following research model and hypotheses, which have been presented below (Figure 2).

In the first two hypotheses, we proposed a positive association between employees' perceptions about the environment security, including the systems environment security and physical working environment security, and ISP violation behavior. We particularly posit that the higher in security employees perceive their environment to, then the more likely they are to perform ISP violations. According to protection motivation theory, users evaluate the certainty of the threat along with the response costs and effectiveness before making the decision of protecting organizational assets. When the environment is perceived to be secure by employees, the risk and threat certainty would be perceived low in the meantime, which will lead to a lower intention to perform the protection/security behaviors. In the qualitative study, multiple participants mentioned that they violated ISPs simply because they believed that the working environment was well secured, with for example no one having access to the area, or with computers that automatically log off. This theoretically leads to perceptions of lower risk and threat certainty. Thus, we propose the following hypotheses:

H1: Perceived systems environment security is positively associated with ISP noncompliance.

H2: Perceived physical environment security is positively associated with ISP noncompliance.

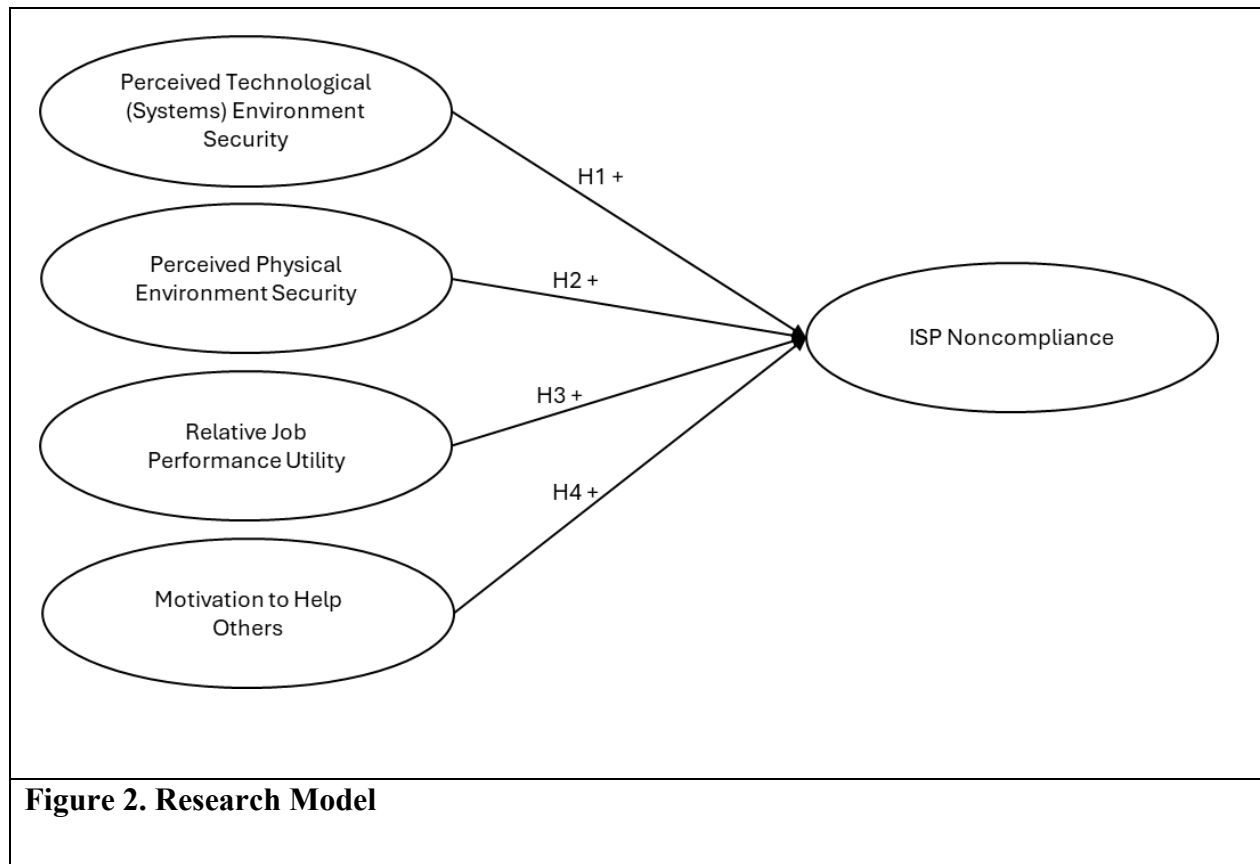
The third identified construct is relative job performance utility which refers to how much users expect the ISP violation (i.e., noncompliance action) helps them perform their job. In the qualitative study, multiple participants mentioned that they violated an ISP because the expected performance outcome will be significantly improved. As we know, employees' work performance is evaluated by task accomplishment and work outcomes instead of their security policy

compliance (Guo et al., 2011). In other words, when information security requirements conflict with work performance, considering the difficulties of following ISPs and the responsibilities of their work, employees will bypass the required security measurement and put their work performance as their first priority. Hence, we propose that:

H3: Relative job performance utility is positively associated with ISP noncompliance.

The last antecedent we identified is employees' motivation to help others in the workplace. Among the participants, multiple of them mentioned that they violated the ISP, especially the password-sharing behavior because their colleagues needed help to finish the assigned work. In previous research, the topic of sharing passwords with colleagues as a helping behavior has been discussed from the model belief perspective (Li et al., 2021). When making a choosing between helping others and violating the security policy, moral beliefs play a significant role (Iwai & de França Carvalho, 2022; Li et al., 2021). Hence, we posit that people who have a higher motivation to help others are more likely to violate information security policies, possibly due to a stronger moral identity. Therefore, we propose that:

H4: The motivation to help others is positively associated with ISP noncompliance.



Research plan

Quantitative phase (Study 2): Cross-sectional survey

We will empirically test our research model and hypotheses by conducting an online cross-sectional survey. Participants will be US-based full-time employees due to our research context and will be recruited by using the online crowdsourcing service, Prolific. The measurement scale of constructs will be adapted or adopted from previously published research. After the data is collected, both the measurement model and structural model will be tested sequentially. Common method bias will be assessed and controlled-for before and after the data collection (Podsakoff et al., 2003).

Conclusion

In this ongoing research project, we study ISP noncompliance as a local phenomenon rather than a contextualized general phenomenon, as the extant literature has viewed it. Thereby, we focus on identifying the factors that are uniquely associated with employees' information security policy noncompliance by conducting sequential mixed-method research. As one of the early studies that pay attention to this research issue, we not only provide a complimentary view of investigating employees' ISP-related behaviors but also will make practical recommendations related to security management.

REFERENCES

- Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy non-compliance behavior: A meta-analysis. *Computers & Security*, 124, 102991. <https://doi.org/10.1016/j.cose.2022.102991>
- Barlow, J., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, 19(8). <https://aisel.aisnet.org/jais/vol19/iss8/3>
- Boudreau, M.-C., & Robey, D. (2005). Enacting Integrated Information Technology: A Human Agency Perspective. *Organization Science*, 16(1), 3–18. <https://doi.org/10.1287/orsc.1040.0103>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Chan, M., Woon, I., & 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. <https://doi.org/10.1080/15536548.2005.10855772>
- Chang, A. J.-T., Wu, C.-Y., & Liu, H.-W. (2012). The effects of job satisfaction and organization commitment on information security policy adoption and compliance. *2012 IEEE International Conference on Management of Innovation & Technology (ICMIT)*, 442–446. <https://doi.org/10.1109/ICMIT.2012.6225846>
- Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE.

- Corbin, J., & Strauss, A. (2015). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications.
- Cram, W. A., D'Arcy, J., & 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., & 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(6), 643–658.
- D'Arcy, J., Hovav, A., & 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.
- D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), 103151.
- Feng, G., Zhu, J., Wang, N., & 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). <https://doi.org/10.17705/1jais.00581>
- Goo, J., Yim, M.-S., & Kim, D. J. (2014). A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *IEEE Transactions on Professional Communication*, 57(4), 286–308. <https://doi.org/10.1109/TPC.2014.2374011>
- Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, 29(2), 340–362. <https://doi.org/10.1111/isj.12202>
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28(2), 203–236. <https://doi.org/10.2753/MIS0742-1222280208>
- Harrison, R. L., & Reilly, T. M. (2011). Mixed methods designs in marketing research. *Qualitative Market Research: An International Journal*, 14(1), 7–26. <https://doi.org/10.1108/13522751111099300>
- Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft*. *Social Forces*, 62(2), 398–418. <https://doi.org/10.1093/sf/62.2.398>
- Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research. *Information Systems Research*, 25(1), 111–136. <https://doi.org/10.1287/isre.2013.0501>
- Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Iwai, T., & de França Carvalho, J. V. (2022). Would you help me again? The role of moral identity, helping motivation and quality of gratitude expressions in future helping intentions. *Personality and Individual Differences*, 196, 111719. <https://doi.org/10.1016/j.paid.2022.111719>

- Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549–566. <https://doi.org/10.2307/25750691>
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113–134. <https://doi.org/10.25300/MISQ/2015/39.1.06>
- Kura, K. M., Shamsudin, F. Mohd., & Chauhan, A. (2015). Does Self-Regulatory Efficacy Matter? Effects of Punishment Certainty and Punishment Severity on Organizational Deviance. *Sage Open*, 5(2), 2158244015591822. <https://doi.org/10.1177/2158244015591822>
- Li, H., Luo, X., & Chen, Y. (2021). Understanding Information Security Policy Violation from a Situational Action Perspective. *Journal of the Association for Information Systems*, 22(3). <https://doi.org/10.17705/1jais.00678>
- 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. <https://doi.org/10.1016/j.ijinfomgt.2020.102152>
- Maxwell, S. R., & Gray, M. K. (2000). Deterrence: Testing the Effects of Perceived Sanction Certainty on Probation Violations. *Sociological Inquiry*, 70(2), 117–136. <https://doi.org/10.1111/j.1475-682X.2000.tb00901.x>
- Murphy, K. (2008). Enforcing Tax Compliance: To Punish or Persuade? *Economic Analysis and Policy*, 38(1), 113–135. [https://doi.org/10.1016/S0313-5926\(08\)50009-9](https://doi.org/10.1016/S0313-5926(08)50009-9)
- Paternoster, R., & Simpson, S. (1996). Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review*, 30(3), 549–583. <https://doi.org/10.2307/3054128>
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70–82. <https://doi.org/10.1016/j.cose.2015.10.006>
- Sarkar, S., Vance, A., Ramesh, B., Demestihis, M., & 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. <https://doi.org/10.1287/isre.2020.0941>
- Sarker, S., & Sarker, S. (2009). Exploring Agility in Distributed Information Systems Development Teams: An Interpretive Study in an Offshoring Context. *Information Systems Research*, 20(3), 440–461. <https://doi.org/10.1287/isre.1090.0241>
- Seidel, S., Recker, J., & vom Brocke, J. (2013). Sensemaking and Sustainable Practicing: Functional Affordances of Information Systems in Green Transformations. *MIS Quarterly*, 37(4), 1275–1299.
- Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487–502. <https://doi.org/10.2307/25750688>
- Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 59(4), 344–353. <https://doi.org/10.1080/08874417.2017.1368421>

- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276.
- Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Information & Management*, 57(4), 103212. <https://doi.org/10.1016/j.im.2019.103212>
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*, 37(1), 21–54.
- Venkatesh, V., Brown, S., & Sullivan, Y. (2016). Guidelines for Conducting Mixed-methods Research: An Extension and Illustration. *Journal of the Association for Information Systems*, 17(7). <https://doi.org/10.17705/1jais.00433>
- Verizon. (2024). *2024 Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>
- Wenzel, M. (2004). An analysis of norm processes in tax compliance. *Journal of Economic Psychology*, 25(2), 213–228. [https://doi.org/10.1016/S0167-4870\(02\)00168-X](https://doi.org/10.1016/S0167-4870(02)00168-X)
- Xue, B., Xu, F., Luo, X., & Warkentin, M. (2021). Ethical leadership and employee information security policy (ISP) violation: Exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1), 5–23. <https://doi.org/10.1108/OCJ-02-2021-0002>