Can Socialization Mitigate ISP Violation? Exploring the Link between Socialization Tactics, Employees' IT Role Congruence, and Non-Malicious ISP Violation

Early stage paper

Sessika Siregar
Yuan Ze University
s1049207@mail.yzu.edu.tw

Kuo-Chung Chang
Yuan Ze University
changkc@saturn.yzu.edu.tw

Yuan Li
University of Tennessee
yli213@utk.edu

ABSTRACT

Non-malicious violations of Information Security Policy (ISP) are common in organizations. Extending past literature, this study examines how employees' IT role congruence, defined as the degree of alignment between employees' expected IT role and their perceptions of the IT role that ISP requires them to fulfil, can influence their intention to violate ISP. The study also examines the effect of socialization tactics in organizations that may lead to IT role congruence. We suggest that collective, formal, sequential, fixed, serial, and investiture socialization tactics can contribute to IT role congruence (measured as lack of role orientation, ambiguity, conflict, and overload), and IT role congruence reduces non-malicious ISP violations. How the study may contribute to the ISP violations literature is discussed.

Keywords

ISP violations, IT role congruence, socialization tactics.

INTRODUCTION

Along with the increasing digitalization and interconnectedness of organizations in the recent era, the volume of information security incidents and the cost of addressing them have both grown. Although technological advances such as anti-virus, firewall, intrusion detection systems, cloud computing, artificial intelligence (AI), security automation, and encryption can be applied to reduce cybersecurity incidents, a secure information systems (IS) environment cannot be fully guaranteed without addressing the humans using the IS (Ifinedo 2012; Safa et al. 2016). Ponemon's Cost of Insider Threats Global Report found that the number of cybersecurity incidents caused by insider threats in the firms it surveyed has increased by 44% between 2020 and 2022 with a total annual cost of US$15.38 million (Ponemon 2022). Hackers continue to exploit human nature using social engineering techniques, and employees may unintentionally compromise security attribute of an information asset, for example by sending sensitive information to the wrong persons. To amend and improve employee security behavior, organizations formulate and employ information security policy (hereafter ISP), yet employees' violation of ISP remains a major barrier to the realization of secured IS (Kolkowska and Dhillon 2013; Myyry et al. 2009).

This study focuses specifically on non-malicious ISP violation intention, defined as the tendencies of employees to purposefully engage in actions that violate ISP, but without malicious intents to cause damage (Cox 2012; Guo et al. 2011). Several traits characterize non-malicious ISP violation. First, the violation is intentional and not accidental, implying that the employees make conscious decision to violate the ISP. Second, the violation is premeditated and voluntary, meaning employees violate ISP at their own will and they justify them through salient cues such as claiming that they don't have time to comply to ISP due to tight deadlines or denying responsibility to comply to ISP because the policy was unclear (Siponen and Vance 2010). Third, the employees do not have malicious intent in violating the ISP; they merely want to help themselves in taking back the benefits of accessibility, ease of use, and integration that were lost or interfered due to ISP (Chang and Seow 2019). For example, employees allow their colleagues to use their computing devices or log-in credentials despite awareness of possible security implications because it saves time and efforts in comparison to if they followed the ISP (Guo et al. 2011; Renaud 2011). Despite some recent interest in malicious security behavior (e.g.: Burns et al. (2022), Luo et al. (2020)), according to Ponemon (2022)'s report, employees' non-malicious behavior such as negligence remains a main cause to human-related security incidents in the past two years. Since non-malicious ISP violations are in general within organization's control (Homoliak et al. 2019; Prabhu and Thompson 2020), studying this types of ISP violations may help managers develop solutions to yield immediate outcomes.

Prior studies in non-malicious ISP violation find that employees generally violate ISP when they experience incongruence in their organizational roles (Barlow et al. 2018; Chang and Seow 2019; Chen et al. 2018; D'Arcy et al. 2014; Li et al. 2021; Shadbad and Biros 2021; Teh et al. 2015; Xue et al. 2021). When employees experience cognitive dissonance between possibly doing an action in their role that is wrong according to ISP but simultaneously right according to their role contexts, employees would change their different perceptions until they become congruent again (Barlow et al. 2018). These attempt to build role congruence manifests in role orientation, role ambiguity, role conflict, and role overload where employees significantly change their ISP-related role requirements, ignore or deny ISP knowledge, or downplay or deprioritize ISP. In this study, we extend previous studies by contending that it is this role congruence issue that determines whether employees would violate ISP or not at a given moment. We named this factor information technology (IT) role congruence to highlight that the congruence particularly relates to employees' perceived consistency between IT usage they expect in their work contexts (e.g.: use IT as tools to increase productivity) and the IT usage specified in ISP (e.g.: use IT while maintaining confidentiality). Addressing this IT role congruence through IT role orientation, IT role ambiguity, IT role conflict, and IT role overload will reduce the role stressors associated with ISP and increase commitment to ISP which are important to mitigate ISP violations (D'Arcy et al. 2014; King and Sethi 1998; Shadbad and Biros 2021).

While the different dimensions of role congruence have been studied in IT security research before, for example: D'Arcy et al. (2014) and Shadbad and Biros (2021), they have mainly focus on examining the impact of role-related constructs on ISP violations rather than the antecedents to these role-related constructs and mechanism to mitigate them. Organizational theories can provide valuable lights in this area. In particular, socialization theory has been argued to be instrumental in addressing role orientation, role ambiguity, role conflict, and role overload in organizational contexts (Allen 2006; Cable and Parsons 2001; Filstad 2011; Jones 1986; King and Sethi 1998). Socialization refers to the process through which an individual comes to appreciate the values, abilities, expected behaviors, and social knowledge essential for assuming an organizational role and for participating as an organizational member (Chao et al. 1994; Louis 1980). It identifies means through which firms influence employees’ adaption to new jobs or organizational roles. As ISP entails organizations’ expectations that their employees adopt new roles in using IT more securely than the past, socialization theory is therefore applicable in ISP violation contexts (Doherty et al. 2009; Hagen et al. 2008; Vance et al. 2013).

Socialization takes place through the use of socialization tactics, referring to the different means through which individuals learn the beliefs, values, orientations, behaviors, skills, and so forth necessary to fulfill their new roles and functions effectively within organization’s environment

(Ashforth and Saks 1996; Van Maanen and Schein 1979). Socialization tactics influence employees’ learning process, particularly newcomers that are faced with uncertainty or anxiety following a reality shock or surprise when their existing assumptions about how people interpret and respond to actions or events do not conform to those that exist in their novel contexts (Jones 1986). Through socialization tactics, employees acquire the attitudes, behavior, and knowledge required to participate as organizational member (Bauer and Green 1998; Cable and Parsons 2001; Van Maanen and Schein 1979). Employees come to possess particular role orientation and learn to cope with role ambiguity, role complexity, and role overload (Grant and Bush 1996; Van Maanen and Schein 1979). Thus, we anticipate that IT role congruence can be fostered via socialization tactics and ISP violation can consequently be mitigated as well.

In particular, socialization tactics that are institutionalized by being collective, formal, sequential, fixed, serial, and investiture have been argued to reduces ambiguity and anxiety and encourage organizational members to passively accept preset organizational norms and maintain status quo (Cable and Parsons 2001; Jones 1986; Saks and Ashforth 1997). Meanwhile, socialization tactics that are individualized by being individual, informal, random, variable, disjunctive, and divestiture create ambiguity which encourage organizational members to challenge status quo and develop their own approaches to situations (Ashforth and Saks 1996; Cable and Parsons 2001; Jones 1986; Saks and Ashforth 1997). As ISP generally represents new organizational role that organizations want employees to fulfil, this research thus argues that socialization tactics can be valuable to explain and evaluate different mechanisms to which employees are socialized to their new security roles through ISP and how it may affect employees’ intention to violate or comply to ISP. Based on theoretical framework of socialization tactics literature, this study thus addresses two research questions:

1. Do employees’ IT role congruence relate to non-malicious ISP violation?
2. How do different socialization tactics relate to employees’ IT role congruence and ISP violation?

The rest of this early stage paper proceeds as follows. The next section provides a literature review and introduces the theoretical background of this study. Then, the research model and hypotheses are developed. This is followed by the design of methodology. Lastly, we discuss potential contributions of the study.

LITERATURE REVIEW AND THEORETICAL BACKGROUND

Studies on Non-Malicious ISP Violation

Existing research suggested that employees violate organizational ISP because they are negligent or ignorant of the policy (Siponen and Vance 2010), they prioritize job performance over ISP compliance (Guo et al. 2011), they feel that the ISP is an inconvenience (Renaud 2011), they are unhappy with the ISP (Hedström et al. 2013), they have poor understanding of the ISP (PwC 2015), or they experience security-related stress (D'Arcy et al. 2014; D'Arcy and Lowry 2019). A variety of theories have been used to advance knowledge on ISP violation, for example, criminological theories such as general deterrence theory, rational choice theory, and situational crime prevention theory; socio-cognitive models such as protection motivation theory; moral reasoning theories such as theory of cognitive moral development and theory of motivational types of values; training design theories such as the universal constructive instructional theory and the elaboration likelihood model; and also social cognitive theory and social bond theory (Cram et al. 2019; Ifinedo 2012; Lee and Lee 2002; Myyry et al. 2009; Pahnila et al. 2007; Puhakainen and Siponen 2010; Safa et al. 2016; Siponen et al. 2007; Straub and Welke 1998; Straub Jr 1990). The studies have provide various insights on what factors affect compliance to ISP and reduce ISP violation among employees, namely: attitude, normative beliefs, organizational support, personal norms and ethics, detection certainty, punishment expectancy, punishment severity, resource vulnerability, response cost, response efficacy, self-efficacy, security education, training, and awareness (SETA), and threat severity (Cram et al. 2019).

Nevertheless, researchers argue that the present literature are still plagued to a degree with suboptimal theoretical framing (Cram et al. 2019), particularly of theories in which inherent values of employees, such as attitudes, personal norms, ethics, and normative beliefs, are under-investigated. Prior studies find that employees violate ISP when they experience psychological, moral, or situational incongruence in their roles, resulting in security stress or lack of interest in learning or following ISP (Barlow et al. 2018; Chang and Seow 2019; Chen et al. 2018; D'Arcy et al. 2014; Li et al. 2021; Shadbad and Biros 2021; Teh et al. 2015; Xue et al. 2021). To function in their roles, employees navigate between role orientation, ambiguity, conflict, and overload to produce one relatively congruent perception of their role at a given moment. With regards to ISP enactment within firms, employees need to perceive congruence between the IT usage they expect in their working environment and the IT usage specified in security-focused ISP, because high IT role orientation, IT role ambiguity, IT role conflict, and IT role overload will increase employees' stresses towards ISP and reduce their commitment to ISP (King and Sethi 1998). IT role congruence is thus relevant to the issue of non-malicious ISP violation.

Employees' IT Role Congruence

Employees' IT role congruence relates to employees' perceived consistency between IT usage they expect in their work contexts (e.g.: use IT as tools to increase productivity) and the IT usage specified in ISP (e.g.: use IT while maintaining confidentiality). To guide decisions and actions, employees draw from their cognition and emotion. At the same time, organizational value systems provide cognitive guidelines that describe how organizational resources should be allocated and how employees should behave as organizational members. Two relevant cognitions can be consonant or dissonant to each other, dissonance however is psychologically uncomfortable for a person and would motivate a person to reduce the dissonance as well as avoid information that would likely increase the dissonance (Harmon-Jones and Mills 2019). If employees experience cognitive dissonance between possibly doing an action in their role that is wrong according to ISP but simultaneously right according to their role contexts (e.g.: to finish their works according to firms' demands), employees would change their different perceptions until they become congruent again for example by reducing or eliminating the perceived negative consequences from violating ISP (Barlow et al. 2018). A "role congruence" situation – in which employees' perception of IT usage in their work contexts (e.g.: as tools to increase productivity) matches their perception of IT usage specified in ISP (e.g.: maintain confidentiality) – is generally considered ideal for employees because it increases their positive attitudes and lessen their stresses or strains with regards to IT usage (Barlow et al. 2018; Kristof-Brown et al. 2005; Vogel et al. 2016),

ISP represents an established corporation policy that is contractually binding on employees. Thus, violating the policy can be seen as violation of social norms. However, employees may perceive ISP as faulty and make their violations justified (Siponen and Vance 2010). This clash between employees and ISP takes place because employees are accustomed to their work habits and values (Strong and Volkoff 2010) and expect IT usage to enhance job performance (Kolkowska and Decker 2012) through IT values such as accessibility (DeLone and McLean 1992), ease of use (DeLone and McLean 1992), and integration (Bailey and Pearson 1983). However, ISP are established for the realization of secured IS through IT security values of confidentiality, integrity, and availability (Andress 2014). This may entail restriction of information access (Hedström et al. 2013), control of employees' admission to organizational IS, and monitoring IS usage (Boss et al. 2009; Parsons et al. 2010). If employees experienced the lack of IT role congruence due to role orientation, role ambiguity, role conflict, or role overload, they will most likely adopt neutralization with their IT secure usage (Barlow et al. 2018; King and Sethi 1998). For example, if complying to ISP requires extra time and efforts from the employees and results on declining work quality, employees will likely view ISP as nuisance and threats to their productivity and convenience and thus violating them would be justified (Kolkowska and Dhillon 2013; Lowry and Moody 2013). Consequently, they will resort to violation behaviors to protect their previous IT role and regain what might be lost if they comply to the ISP and fulfill the new IT role (Hedström et al. 2013).

Thus, we defined employees' IT role congruence as the degree of alignment between their expected IT role and their perceptions of the IT role that ISP requires them to fulfil (Edwards and Cable 2009; Kristof-Brown et al. 2005). It involves the lack of role orientation, role ambiguity, role conflict, and role overload in IT usage after ISP introduction (D'Arcy et al. 2014; King and Sethi 1998; Shadbad and Biros 2021; Teh et al. 2015). Role orientation is defined as employees' perception that they can significantly change their role requirements with regards to IT secure usage (King and Sethi 1998). Role ambiguity is defined as employees' perceptions of uncertainty or lack of clarity about their jobs in relation to IT secure usage (Teh et al. 2015). Role conflict is defined as incompatible and inconsistent task requirements with regards to IT secure usage (Shadbad and Biros 2021). Role overload is defined as employees' perceptions of their incapability to handle all assigned tasks associated with IT secure usage (Shadbad and Biros 2021).

Role orientation, role ambiguity, role conflict, and role overload have been studied in IT security research, for example: D'Arcy et al. (2014), Teh et al. (2015), Barlow et al. (2018), and Shadbad and Biros (2021). D'Arcy et al. (2014) constructed security-related stress (SRS), a second-order construct comprised of security-related overload, complexity, and uncertainty and reported its positive relations to ISP violations through moral disengagement. Teh et al. (2015) reported positive relations between role conflict and ISP violation intention through neutralization techniques but found insignificant relations between role ambiguity and ISP violation intention through neutralization. Shadbad and Biros (2021) constructed role stress as a second-order construct rooted on role overload, role ambiguity, and role conflict and reported its positive link to ISP violations. Consequently, in this research we argue that IT role congruence will most likely has a negative relationship to ISP violation.

Socialization Tactics

Socialization tactics refer to the strategies that organizations employ to influence employees to assimilate their new organizational roles (Grant and Bush 1996; Van Maanen and Schein 1979). The most widely used conceptualization of socialization tactics is Van Maanen and Schein (1979) classification scheme, which distinguished six dimensions along which socialization tactics polarize: collective versus individual, formal versus informal, fixed versus variable, sequential versus random, serial versus disjunctive, and investiture versus divestiture. Collective tactic groups employees from different department together and provides them with common learning experiences, while individual tactic provides employees with unique set of learning experiences. Formal tactic takes employees outside of their work setting, while in informal tactic employees learn on the job. Fixed tactic lets employees know exactly the timetables associated with the stages in the process, while variable tactic provides no information to the employees on the stages.

Sequential tactic offers employees explicit guidelines about the sequence of activities they will go through, while in random tactic, employees do not know them. In serial tactic, experienced organizational members become role models for the employees, while disjunctive tactic requires employees to develop their own definitions of the situations with no role models. Lastly, in investiture tactic employees receive positive social support, while divestiture tactic implies employees receiving negative social communications until they begin to fulfill expectations.

Jones (1986) and subsequent research (e.g., Bauer and Green (1998)) further classify these socialization tactics to institutionalized and individualized tactics (Cable and Parsons 2001). Institutionalized tactics such as collective, formal, sequential, fixed, serial, and investiture tactics refers to structured program of socialization that reduces ambiguity and anxiety and encourages organizational members to passively accept preset organizational norms and maintain status quo (Cable and Parsons 2001; Jones 1986; Saks and Ashforth 1997). Meanwhile, individualized socialization tactics such as individual, informal, random, variable, disjunctive, and divestiture tactics refer to socialization program with relative absence of structure and high ambiguity that encourage organizational members to challenge status quo and develop their own approaches to situations (Ashforth and Saks 1996; Cable and Parsons 2001; Jones 1986; Saks and Ashforth 1997).

In the IS literature, socialization tactics have also been applied in several contexts. First, as one of organizational levers that management can exercise to prompt employees' intrinsic motivation to explore enterprise system features (Ke et al. 2012). Second, to understand the ways in which new IS personnel adjust to their roles as IS professionals (Choi et al. 2010; King and Sethi 1998). King and Sethi (1998) discovered that institutionalized socialization tactics lead to newcomers adopting knowledge, strategies, and missions already associated with a role than adopting innovative roles and to reduced role ambiguity and role conflict in new personnel. In their study on the impact of specific socialization tactics on newcomers' commitment to WikiProjects online groups, Choi et al. (2010) reported that in online groups, different socialization tactics have different effects on new members' motivation to contribute over time. Third, to understand knowledge transfer in enterprise system assimilation (Wang et al. 2015). Wang et al. (2015) found that socialization tactics strongly impact depth, breadth, and linkage of knowledge acquisition which in turn affect employees' habitual and extended use of the knowledge.

Previous studies have supported that certain institutionalized socialization tactics may increase congruence between employees' previous roles and their perceptions of the new roles better than others tactics (Cable and Parsons 2001). For example, sanctions have been argued to work better as a deterrent if they are rationalized and justified through cognitive education and persuasion which can be considered as formal and fixed tactics (Myyry et al. 2009; Puhakainen and Siponen 2010). Studies have also argued on the limitations of training and awareness programs in accomplishing full compliance (Mundie et al. 2013). Continuous ISP communication which can be considered as sequential and fixed instead of one-off efforts, have been suggested and found to be needed in addition to training to maximize ISP compliance (McLean 1992; Puhakainen and Siponen 2010). Visible top management and/or workgroup members' support of the ISP which can be considered as serial and investiture tactics has also been argued as important for ensuring employees' compliance to ISP (Perry 1985; Puhakainen and Siponen 2010). Socialization tactics thus provide a comprehensive framework explaining how organizations can impact the adjustment of employees to the new IT security role expected from them with the introduction of ISP (Grant and Bush 1996; King and Sethi 1998; Van Maanen and Schein 1979).

In this research, we focus on institutionalized socialization tactics as they reflect organizations' expectation from the introduction of ISP, which is to reduce ambiguity for employees of its information resources in interpreting and responding to information resources related events within the organizations in order to ensure the security of organizations' information resources. Table 1 presents a brief review of institutionalized ISP socialization tactics in existing IT literature.

Socialization tactics	Socialization tactics examples
Collective-individual	Discussion sessions among employees; online tutorial, e.g.: Cox et al. (2001)
	Contain promotional component (publications, advertising, and reaction to incidents), e.g.: Lafleur (1992)
Formal-informal	Contain interactive component (briefings, planning sessions, meetings, and training), e.g.: Lafleur (1992)
	Discussion of security through educational sessions, e.g.: Puhakainen and Siponen (2010)
Sequential-random	Checklist of do's and don'ts, e.g.: Cox et al. (2001)
	Various assets and security processes associated with each individual system should be identified and explicitly defined; manager responsible for each asset or security process should be agreed and the responsibility documented; authorization levels should be clearly defined and documented, e.g.: Kajava and Siponen (1996)
Fixed-variable	Segmenting employees' training needs according to his/her functional specialties as defined by his organizational role, e.g.: Wilson et al. (1998)
	Systematic and continuing training program, e.g.: Puhakainen and Siponen (2010)
Serial-disjunctive	A security board containing experts to organize security at corporate level in a top-down direction, e.g.: Kajava and Siponen (1996)
	The use of IS Security campaigns, e.g.: McLean (1992); Wood (1995); Proctor and Byrnes (2002); Rudolph (2012)
Investiture-divestiture	Rewards systems, e.g.: Mitnick and Simon (2003); Perry (1985)
	Visible support by top management, e.g.: Puhakainen and Siponen (2010)

Table 1. Institutionalized ISP Socialization Tactics

RESEARCH MODEL AND HYPOTHESES

We first study how socialization tactics help improve IT role congruence, then study how IT role congruence influences ISP violation intention. As introduced in the above section, socialization tactics contain six major dimensions. First, using collective socialization tactic means that the employees go through common socialization experiences with a group rather than learning the ISP individually. This tactic involves providing employees with common message and collective consciousness about the new roles and appropriate responses within IT usage as the ISP takes place to reduce role uncertainty and increase greater sense of shared values between employees rather than encouraging them to behave innovatively when using IT (Allen 2006; King and Sethi 1998). For example, rather than letting employees learn individually on how to execute the ISP, they are taught together with a focus on similar roles and common responsibilities with regards to IT usage. Employees' perception of their IT role would thus be more aligned with the rest of the organization towards those authorized by ISP rather than remain unchanged as before ISP. Thus, we predict:

H1a: Socialization tactics that are collective will be positively related to employees' IT role congruence.

Using formal tactics involves specifically arranging activities for employees to socialize them to the ISP rather than letting the employees learn the ISP whenever they can. Formal tactics increase the likelihood of employees to accept the re-definitions of their roles with regards to IT usage due to ISP and reduce the perception of flexibility to return to their old IT practices as they signals the higher importance firms place for employees to adapt to the new situations (Allen 2006; King and Sethi 1998). For example, employees are sent to one- or two-week classes to orient them to the new roles and expected responses with regards to IT usage as ISP is enacted. Consequently, employees would be more likely to align their previous perception of their IT roles (prior to the introduction of ISP) to those embedded in the ISP. Thus, we predict:

H1b: Socialization tactics that are formal will be positively related to employees' IT role congruence.

Using sequential tactics means that the employees are put through a coherent sequence of ISP socialization that build upon each other rather than being given jumbled ISP socialization experiences (Choi et al. 2010). When ISP socialization processes are sequential, employees would experience lesser uncertainties and have clearer routines and controls with regards to their new roles and expectations when using IT with the ISP (Allen 2006). It can thus reduce frustration and fatigue associated with adjusting to the new roles and actions expected of them with the introduction of ISP (D'Arcy and Lowry 2019). For example, employees are first introduced to ISP with regards to storage and device hygiene, then followed with email and messaging hygiene, then authentication and credential hygiene, transmission hygiene, and lastly social media hygiene (Vishwanath et al. 2020). As they are given relatively clear sequences to adjust to the new IT roles expected by the ISP instead of receiving them unclearly or in all-in-one sequence, employees are less likely to feel frustrated or tired with aligning their previous perception of IT roles to the new ones. Thus, we predict:

H1c: Socialization tactics that are sequential will be positively related to employees' IT role congruence.

Fixed socialization tactics involve providing employees with precise timing on the completion of each stage of the ISP socialization processes rather than letting them be in the dark. The tactics would thus reduce uncertainties and anxieties on employees on the timeline of their new expectations in IT usage and give them a better sense of control with regards to the timing of new ISP requirements (Allen 2006; D'Arcy and Lowry 2019). For example, ISP-related training sessions are made regularly (e.g., every 3 or 6 months) to remind employees of ISP requirements and introduce them to new requirements. Because they have clearer idea on the periods in which they are expected to re-align their perceived IT roles according to ISP, including if they move to different work positions, employees are less likely to feel uncertain or anxious on the process. Thus, we predict:

H1d: Socialization tactics that are fixed will be positively related to employees' IT role congruence.

Serial tactics involve providing employees with experienced mentors who will help them to learn the ISP rather than leaving them on their own (Choi et al. 2010). Serial tactics encourage employees to follow the footsteps of these mentors rather than developing employees' own approach on the situations (Allen 2006). They can thus reduce uncertainties with regards to the new roles and actions expected of them when using IT with the ISP because the employees can turn to these mentors to make sense of the new environment and to assist the employees if they face some issues with the new IT practices (Allen 2006). For example, managers offering detailed explanations and coaching on ISP to their subordinates to alleviate their doubts, concerns, and uncertainties on ISP (Feng et al. 2019). Encouraged by the mentors, employees are thereby more likely to align their previous perception of IT roles into those embedded in the ISP. Thus, we predict:

H1e: Socialization tactics that are serial will be positively related to employees' IT role congruence.

Using investiture tactics means that employees' existing skills and abilities are acknowledged and built rather than condemned (Choi et al. 2010). Investiture tactics involve endorsing the value of employees' characteristics and capabilities as something that the firms want to capitalize rather than change with negative feedback (King and Sethi 1998). Investiture tactics tend to better build sense of competence and confidence on employees than divestiture tactics (Allen 2006).

Employees' positive evaluation of their personal skills, knowledge, or competency in fulfilling ISP requirements positively affects their intention to comply to ISP requirements (Bulgurcu et al. 2010). For example, their previous knowledge on IT usage are taken into consideration when designing ISP compliance training (Puhakainen and Siponen 2010). As the new IT roles embedded in ISP is perceived to align to employees' strengths, employees would more easily align their previous perceived IT roles to the new ones. Thus, we predict:

H1f: Socialization tactics that are investiture will be positively related to employees' IT role congruence.

When employees perceive that their present beliefs, values, orientations, behaviors, skills, and so forth necessary to fulfill their work roles and functions effectively within organization's environment aligned or exceed those of what organizations expect of them, they experience role congruence. ISP, however, entail new demands on employees in their usage of IT to perform daily works, as it may involves restriction of information access (Hedström et al. 2013), control of employees' admission to organization IS, monitoring of IS usage (Boss et al. 2009; Parsons et al. 2010), and so on that can cause role incongruence in employees with regards to IT usage in the work environment (D'Arcy and Lowry 2019). When employees are pulled between the pressure of completing their job efficiently on one side and security concerns as highlighted by ISP on the other side, the role incongruence, similar to cognitive dissonance, would more likely make them fall back to their previous IT usage routines which have been proven to fulfill their focal job tasks; this causes them to temporarily accept or self-justify their violation of ISP (Barlow et al. 2018; Hedström et al. 2013). Excess working load, security complexity, as well as uncertainties with job-related security requirements increase employees' role incongruence which can lead them to this non-malicious violation of ISP (D'Arcy et al. 2014; D'Arcy and Lowry 2019). However, if employees' perceived IT roles are aligned to the IT roles firm expects them to take (as embedded in the ISP), employees are more likely to maintain consistency in their thoughts and actions by not violating ISP. For example, managers designing employees' workload to be as manageable as possible with relations to IT usage or giving awards to employees that manage to comply with ISP regardless of excess work pressures (Posey et al. 2014).

H2: Employees' IT role congruence will be negatively related to ISP violation.

We include moral beliefs and self-control as control variables in the research model because they can affect employees' ISP violation behavior (Burns et al. 2022; Cram et al. 2019; Luo et al. 2020). We also include instrumental motives (financial benefits) and expressive motives (psychological contract violation) for insider computer abuse (ICA) as control variables in the model because they can also affect employees' ISP violation behavior as they encourage employees to violate ISP maliciously (Burns et al. 2022). They can thus be used to control malicious intention on the employees.

Figure 1 shows the research model of this study.

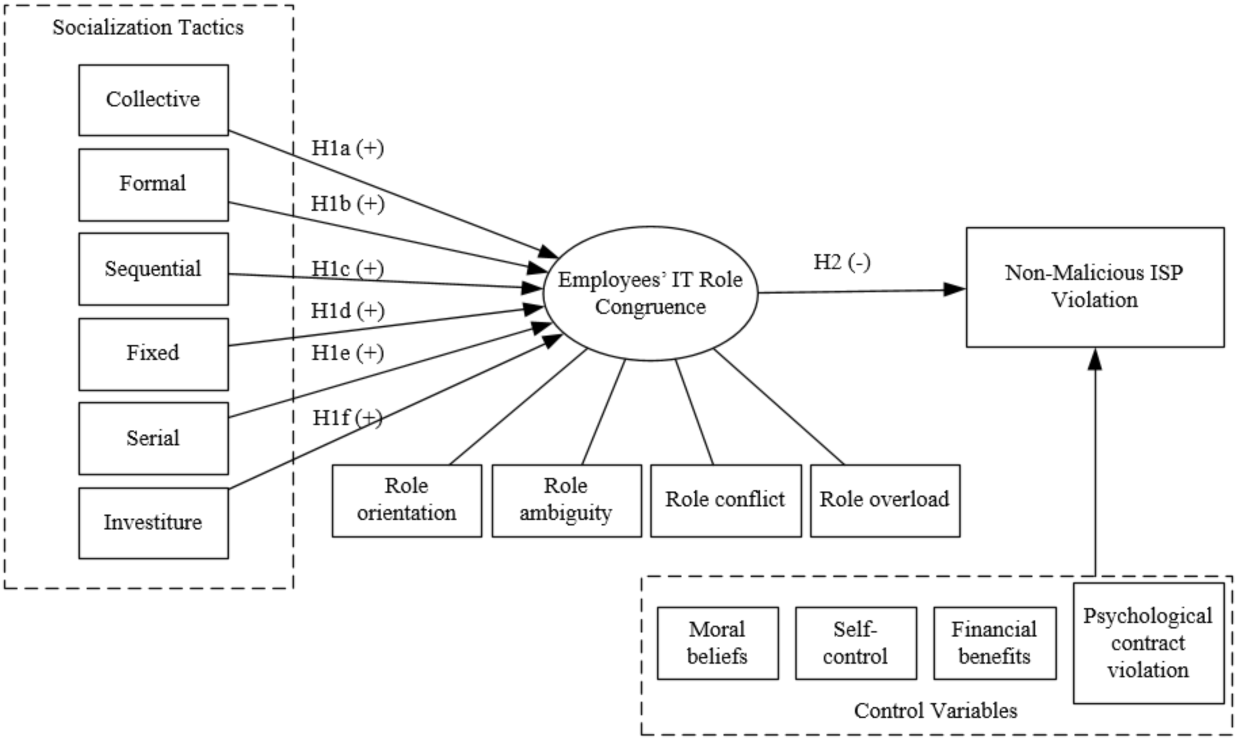

Figure 1. Research Model

METHODOLOGY

Sample and Procedure

The unit of analysis in this study is individual level. The key respondents will be employees working in various organizations that have ISP. Data is planned to be collected from Taiwan, Indonesia or Malaysia, and the US. This allows to test the generalizability of the model and to observe the possible effects of culture. The primary method of data collection will be survey.

Measures

The survey will consist of previously validated scales adapted to this study context. See Appendix A for an abridged list of the survey items.

Each construct of institutionalized socialization tactics will be measured using adaption of Jones (1986)'s Socialization Tactics Scale. Collective tactic will be measured using items such as: *In the* *last six months, I have been extensively involved with other employees in common ISP compliance training activities*. Formal tactic will be measured using items such as: *I have been through a set of ISP training experiences which are specifically designed to give employees a thorough knowledge of ISP compliance related skills*. Sequential tactic will be measured using items such as: *There is a clear pattern in the way one ISP compliance leads to other benefits in my organization*. Fixed tactic will be measured using items such as: *I can predict my future ISP compliance path in this organization by observing other people's experiences*. Serial tactic will be measured using items such as: *Organizational members experienced in ISP compliance see advising or training less experienced organizational members as one of their main job responsibilities in my organization*. Investiture tactic will be measured using items such as: *In my organization, I have been made to feel that my skills and abilities are very important in ISP compliance*.

Employees' IT role congruence will be measured with adaption of: King and Sethi (1998)'s five-item scale for role orientation; Teh et al. (2015)'s seven-item scale for role ambiguity; Teh et al. (2015)'s six-item scale for role conflict; and Shadbad and Biros (2021)'s five-item scale for role overload. Role orientation will be measured using items such as: *I have made attempt to redefine my role and change what I am required to do with regards to using IT securely*. Role ambiguity is measured using items such as: *I feel certain on how I will be evaluated in my secure IT usage*. Role conflict is measured using items such as: *I received incompatible requests on secure IT usage from two or more people*. Role overload is measured using items such as: *I often have to use IT more securely than I can handle*.

ISP violation will be measured using Johnston et al. (2016) scenario-based survey with respondents randomly being given one of three hypothetical vignettes involving an actor violating

ISP and then being asked the likelihood or chance that they would follow the actions of the hypothetical actor in violating ISP if they are under the same conditions. Additionally, to verify the robustness of the main claims in the model (i.e., socialization tactics improves IT role congruence that reduces ISP violations), we measure ISP compliance using a four-item scale from D'Arcy and Lowry (2019). The scale includes items such as: *Today at work, I have complied with the requirements of the ISP*.

Moral beliefs will be measured using D'Arcy and Lowry (2019)'s two-item scale: *I would find it morally unacceptable to violate my organization's ISP* and *It would be against my moral beliefs to violate my organization's ISP*. Meanwhile, self-control, instrumental and expressive motives for ICA will be measured based on Burns et al. (2022)'s study. Self-control will be measured using Tangney et al. (2004)'s reverse-worded six-item scale which include items such as: *I have a hard time breaking bad habits*. Instrumental motives for ICA will be measured using Posey et al. (2015)'s three-item scale to measure financial benefits which include items such as: *I could be rewarded financially for choosing to abuse my organization's computer systems*. Expressive motives for ICA will be measured using Robinson and Morrison (2000)'s six-item scale to measure psychological contract violation which include items such as: *I have not received everything promised to me in exchange for my contributions*. Additionally, we will also control for age, employees' position, and country as prior literature have found them to be related to ISP violation intention (Cram et al. 2019; Xue et al. 2021).

POTENTIAL CONTRIBUTIONS OF THE STUDY

While the study is currently in its early stage, we anticipate the following theoretical and practical contributions once it is finished. Theoretically, the study illustrates the critical roles that socialization tactics play in helping mitigate non-malicious ISP violations in organizations. While socialization has been examined in organizational and IS research, little is known about how it helps to mitigate ISP violations, particularly through its effect on boosting IT role congruence. We expect that our study would unveil their relationship and bring insight into how the different socialization tactics can lead to IT role congruence, which then mitigates ISP violations. This extends the socialization theory in ISP violation research. Secondly, the pivotal role of IT role congruence can be verified. While past research has examined IT role-related constructs such as role ambiguity, little is known about how role congruence would influence employees' attitude and behavior toward ISP. We suggest that role congruence plays a pivotal role in determining ISP violations, so that future research may focus on this construct and uncover other factors, in addition to socialization tactics, that may also lead to employees' IT role congruence.

Practically, the study may help organizations design mechanism to effectively socialize their employees to behaviors where ISP violations are avoided and commitment to ISP are increased. For example, we emphasize institutionalized socialization tactics (i.e., collective, formal, sequential, fixed, serial, and investiture) rather than individualized tactics, which offers guidelines to managers to design interventions based on these tactics. Also, the knowledge of the dimensions of IT role congruence may allow managers to assess their employees' perceptions in order to minimize the inconsistency in their perceptions.

REFERENCES

Allen, D.G. 2006. "Do Organizational Socialization Tactics Influence Newcomer Embeddedness and Turnover?," *Journal of management* (32:2), pp. 237-256.

Andress, J. 2014. "What Is Information Security?," *The Basics of Information Security, Elsevier*), pp. 1-22.

Ashforth, B.K., and Saks, A.M. 1996. "Socialization Tactics: Longitudinal Effects on Newcomer Adjustment," *Academy of management Journal* (39:1), pp. 149-178.

Bailey, J.E., and Pearson, S.W. 1983. "Development of a Tool for Measuring and Analyzing Computer User Satisfaction," *Management science* (29:5), pp. 530-545.

Barlow, J.B., Warkentin, M., Ormond, D., and 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), p. 3.

Bauer, T.N., and Green, S.G. 1998. "Testing the Combined Effects of Newcomer Information Seeking and Manager Behavior on Socialization," *Journal of Applied Psychology* (83:1), p. 72.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., and Boss, R.W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

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), pp. 523-548.

Burns, A., Roberts, T.L., Posey, C., Lowry, P.B., and Fuller, B. 2022. "Going Beyond Deterrence: A Middle-Range Theory of Motives and Controls for Insider Computer Abuse," *Information Systems Research*).

Cable, D.M., and Parsons, C.K. 2001. "Socialization Tactics and Person-Organization Fit," *Personnel Psychology* (54:1), pp. 1-23.

Chang, K.-C., and Seow, Y.M. 2019. "Protective Measures and Security Policy Non-Compliance Intention: It Vision Conflict as a Moderator," *Journal of Organizational and End User Computing (JOEUC)* (31:1), pp. 1-21.

Chao, G.T., O'Leary-Kelly, A.M., Wolf, S., Klein, H.J., and Gardner, P.D. 1994. "Organizational Socialization: Its Content and Consequences," *Journal of Applied psychology* (79:5), p. 730.

Chen, H., Chau, P.Y., and Li, W. 2018. "The Effects of Moral Disengagement and Organizational Ethical Climate on Insiders’ Information Security Policy Violation Behavior," *Information Technology & People*).

Choi, B., Alexander, K., Kraut, R.E., and Levine, J.M. 2010. "Socialization Tactics in Wikipedia and Their Effects," *Proceedings of the 2010 ACM conference on Computer supported cooperative work*, pp. 107-116.

Cox, A., Connolly, S., and Currall, J. 2001. "Raising Information Security Awareness in the Academic Setting," *Vine*).

Cox, J. 2012. "Information Systems User Security: A Structured Model of the Knowing–Doing Gap," *Computers in Human Behavior* (28:5), pp. 1849-1858.

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), pp. 525-554.

D'Arcy, J., Herath, T., and Shoss, M.K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of management information systems* (31:2), pp. 285-318.

D'Arcy, J., and Lowry, P.B. 2019. "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43-69.

DeLone, W.H., and McLean, E.R. 1992. "Information Systems Success: The Quest for the Dependent Variable," *Information systems research* (3:1), pp. 60-95.

Doherty, N.F., Anastasakis, L., and Fulford, H. 2009. "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies," *International journal of information management* (29:6), pp. 449-457.

Edwards, J.R., and Cable, D.M. 2009. "The Value of Value Congruence," *Journal of applied psychology* (94:3), p. 654.

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), p. 2.

Filstad, C. 2011. "Organizational Commitment through Organizational Socialization Tactics," *Journal of Workplace Learning*).

Grant, E.S., and Bush, A.J. 1996. "Salesforce Socialization Tactics: Building Organizational Value Congruence," *Journal of Personal Selling & Sales Management* (16:3), pp. 17-32.

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), pp. 203-236.

Hagen, J.M., Albrechtsen, E., and Hovden, J. 2008. "Implementation and Effectiveness of Organizational Information Security Measures," *Information Management & Computer Security*).

Harmon-Jones, E., and Mills, J. 2019. "An Introduction to Cognitive Dissonance Theory and an Overview of Current Perspectives on the Theory,").

Hedström, K., Karlsson, F., and Kolkowska, E. 2013. "Social Action Theory for Understanding Information Security Non-Compliance in Hospitals: The Importance of User Rationale," *Information Management & Computer Security*).

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., and Ochoa, M. 2019. "Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *ACM Computing Surveys (CSUR)* (52:2), pp. 1-40.

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), pp. 83-95.

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), pp. 231-251.

Jones, G.R. 1986. "Socialization Tactics, Self-Efficacy, and Newcomers' Adjustments to Organizations," *Academy of Management journal* (29:2), pp. 262-279.

Kajava, J., and Siponen, M. 1996. "Security Management and Organizations-Bottom up or Top Down Approach," *Proceedings of Nordic Workshop on Secure Computer Systems*, pp. 1-12.

Ke, W., Tan, C.-H., Sia, C.-L., and Wei, K.-K. 2012. "Inducing Intrinsic Motivation to Explore the Enterprise System: The Supremacy of Organizational Levers," *Journal of Management Information Systems* (29:3), pp. 257-290.

King, R.C., and Sethi, V. 1998. "The Impact of Socialization on the Role Adjustment of Information Systems Professionals," *Journal of management information systems* (14:4), pp. 195-217.

Kolkowska, E., and Decker, B.D. 2012. "Analyzing Value Conflicts for a Work-Friendly Iss Policy Implementation," *IFIP International Information Security Conference*: Springer, pp. 339-351.

Kolkowska, E., and Dhillon, G. 2013. "Organizational Power and Information Security Rule Compliance," *Computers & Security* (33), pp. 3-11.

Kristof-Brown, A.L., Zimmerman, R.D., and Johnson, E.C. 2005. "Consequences of Individuals' Fits at Work: A Meta-Analysis of Person–Job, Person–Organization, Person–Group, and Person–Supervisor Fit," *Personnel psychology* (58:2), pp. 281-342.

Lafleur, L. 1992. "Training as Part of a Security Awareness Program," *Computer Control Quarterly* (10:4), pp. 4-11.

Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information management & computer security*).

Li, H., Luo, X.R., and Chen, Y. 2021. "Understanding Information Security Policy Violation from a Situational Action Perspective," *Journal of the Association for Information Systems* (22:3), p. 5.

Louis, M.R. 1980. "Surprise and Sense Making: What Newcomers Experience in Entering Unfamiliar Organizational Settings," *Administrative science quarterly*), pp. 226-251.

Lowry, P.B., and Moody, G.D. 2013. "Explaining Opposing Compliance Motivations Towards Organizational Information Security Policies," *2013 46th Hawaii International Conference on System Sciences*: IEEE, pp. 2998-3007.

Luo, X.R., Li, H., Hu, Q., and Xu, H. 2020. "Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective," *Journal of the Association for Information Systems* (21:6), p. 5.

McLean, K. 1992. "Information Security Awareness-Selling the Cause," *Proceedings of the IFIP TC11, Eigth International Conference on Information Security: IT Security: The Need for International Cooperation*, pp. 179-193.

Michailova, S., and Wilson, H.I. 2008. "Small Firm Internationalization through Experiential Learning: The Moderating Role of Socialization Tactics," *Journal of World Business* (43:2), pp. 243-254.

Mitnick, K.D., and Simon, W.L. 2003. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Mundie, D.A., Perl, S., and Huth, C.L. 2013. "Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions," *2013 third workshop on socio-technical aspects in security and trust*: IEEE, pp. 26-36.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Nguyen, T.N.T., Bui, T.H.T., and Nguyen, T.H.H. 2021. "Improving Employees’ Proactive Behaviors at Workplace: The Role of Organizational Socialization Tactics and Work Engagement," *Journal of Human Behavior in the Social Environment* (31:6), pp. 673-688.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.

Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. 2010. "Human Factors and Information Security: Individual, Culture and Security Environment," Defence Science and Technology Organisation Edinburgh (Australia) Command ….

Perry, W.E. 1985. *Management Strategies for Computer Security*. Butterworth-Heinemann.

Ponemon. 2022. "2022 Ponemon Cost of Insider Threats Global Report."

Posey, C., Roberts, T.L., and Lowry, P.B. 2015. "The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.

Posey, C., Roberts, T.L., Lowry, P.B., and Hightower, R.T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information

Security Professionals and Ordinary Organizational Insiders," *Information & management* (51:5), pp. 551-567.

Prabhu, S., and Thompson, N. 2020. "A Unified Classification Model of Insider Threats to Information Security," *31st Australasian Conference on Information Systems*.

Proctor, P.E., and Byrnes, C. 2002. *The Secured Enterprise: Protecting Your Information Assets*. Prentice Hall PTR.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS quarterly*), pp. 757-778.

PwC. 2015. "Global State of Information Security Survey."

Renaud, K. 2011. "Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?," *IEEE Security & Privacy* (10:3), pp. 57-63.

Robinson, S.L., and Morrison, E.W. 2000. "The Development of Psychological Contract Breach and Violation: A Longitudinal Study," *Journal of organizational Behavior* (21:5), pp. 525-546.

Rudolph, K. 2012. "Implementing a Security-Awareness Program," *Computer Security Handbook*), pp. 49.41-49.47.

Safa, N.S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *computers & security* (56), pp. 70-82.

Saks, A.M., and Ashforth, B.E. 1997. "Organizational Socialization: Making Sense of the Past and Present as a Prologue for the Future," *Journal of vocational Behavior* (51:2), pp. 234-279.

Sanclemente, F.J., Gamero, N., Medina, F.J., and Mendoza-Denton, R. 2022. "A Multilevel Model of Job Inclusion of Employees with Disabilities: The Role of Organizational Socialization Tactics, Coworkers Social Support and an Inclusive Team Context," *Applied Psychology*).

Selmer, J. 2001. "Antecedents of Expatriate/Local Relationships: Pre-Knowledge Vs Socialization Tactics," *International Journal of Human Resource Management* (12:6), pp. 916-925.

Shadbad, F.N., and Biros, D. 2021. "Understanding Employee Information Security Policy Compliance from Role Theory Perspective," *Journal of Computer Information Systems* (61:6), pp. 571-580.

Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," *IFIP International Information Security Conference*: Springer, pp. 133-144.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly*), pp. 487-502.

Straub, D.W., and Welke, R.J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS quarterly*), pp. 441-469.

Straub Jr, D.W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Strong, D.M., and Volkoff, O. 2010. "Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact," *MIS quarterly*), pp. 731-756.

Tangney, J.P., Boone, A.L., and Baumeister, R.F. 2004. "High Self-Control Predicts Good Adjustment, Less Pathology, Better Grades, and Interpersonal Success," *Journal of Personality* (72:2), pp. 271-324.

Teh, P.-L., Ahmed, P.K., and D'Arcy, J. 2015. "What Drives Information Security Policy Violations among Banking Employees?: Insights from Neutralization and Social Exchange Theory," *Journal of Global Information Management (JGIM)* (23:1), pp. 44-64.

Van Maanen, J.E., and Schein, E.H. 1979. "Toward a Theory of Organizational Socialization,").

Vance, A., Lowry, P.B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-290.

Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G., and Chin, J. 2020. "Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests," *Decision Support Systems* (128), p. 113160.

Vogel, R.M., Rodell, J.B., and Lynch, J.W. 2016. "Engaged and Productive Misfits: How Job Crafting and Leisure Activity Mitigate the Negative Effects of Value Incongruence," *Academy of Management Journal* (59:5), pp. 1561-1584.

Wang, W., Hu, Q., Liu, L., Feng, Y., and Yang, M. 2015. "Understanding Knowledge Transfer in Enterprise System Assimilation: The Critical Role of Socialization Tactics,").

Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D., and Ippolito, J.B. 1998. "Information Technology Security Training Requirements: A Role-and Performance-Based Model," National Institute of Standards and Technology.

Wood, C.C. 1995. "Information Security Awareness Raising Methods," *Computer Fraud & Security* (6:1995), pp. 13-15.

Xu, L., Cui, N., Qualls, W., and Zhang, L. 2017. "How Socialization Tactics Affect Supplier-Buyer Co-Development Performance in Exploratory and Exploitative Projects: The Mediating Effects of Cooperation and Collaboration," *Journal of Business Research* (78), pp. 242-251.

Xue, B., Xu, F., Luo, X., and Warkentin, M. 2021. "Ethical Leadership and Employee Information Security Policy (Isp) Violation: Exploring Dual-Mediation Paths," *Organizational Cybersecurity Journal: Practice, Process and People*).

APPENDIX A: EXAMPLE ITEMS

This table contains example items for measuring the research constructs and control variables.

Complete list of items will be presented at the workshop.

Collective tactic Based on Jones (1986)	In the last six months, I have been extensively involved with other employees in common, ISP compliance training activities
	Other employees have been instrumental in helping me to understand compliance to ISP
Formal tactic Based on Jones (1986)	I have been through a set of ISP training experiences which are specifically designed to give employees a thorough knowledge of ISP compliance related skills
	During my training for ISP compliance I was normally physically apart from regular employees
Sequential tactic Based on Jones (1986)	There is a clear pattern in the way one ISP compliance leads to other benefits in my organization
	Each stage of ISP compliance training process has, and will, expand and build upon information security knowledge gained during the preceding stages of the process
Fixed tactic Based on Jones (1986)	I can predict my future ISP compliance path in this organization by observing other people’s experiences

	I have a good knowledge of the time it will take me to go through the various stages of ISP compliance training process in my organization
Serial tactic Based on Jones (1986)	Organizational members experienced in ISP compliance see advising or training less experienced organizational members as one of their main job responsibilities in my organization
	I am gaining a clear understanding of my role in ISP compliance in my organization from observing my senior colleagues
Investiture tactic Based on Jones (1986)	In my organization, I have been made to feel that my skills and abilities are very important in ISP compliance
	Almost all of my colleagues have been personally supportive of me in complying to ISP
Role orientation Based on King and Sethi (1998)	I have made attempt to redefine my role and change what I am required to do with regards to using IT securely
	While I am satisfied with my overall secure IT usage responsibilities, I have altered the procedures of using IT to do my job
Role ambiguity Based on Teh et al. (2015)	I feel certain on how I will be evaluated in my secure IT usage
	I am told how well I am doing in using IT securely
Role conflict Based on Teh et al. (2015)	I received incompatible requests on secure IT usage from two or more people
	I use IT in ways that are sometimes accepted by one person but not by another
Role overload Shadbad and Biros (2021)	I often have to use IT more securely than I can handle
	I am often required to do difficult tasks with regards to using IT securely
ISP Violation Johnston et al. (2016)	Scenario-based survey with respondents randomly being given one of three hypothetical vignettes involving an actor violating ISP and then being asked the likelihood or chance that they would follow the actions of the hypothetical actor in violating ISP if they are under the same conditions
ISP compliance (Model robustness verification) D'Arcy and Lowry (2019)	Today at work, I have complied with the requirements of the ISP
	Today at work, I have protected information and technology resources according to the requirements of the ISP
Moral beliefs D'Arcy and Lowry (2019)	I would find it morally unacceptable to violate my organization's ISP
	It would be against my moral beliefs to violate my organization's ISP
Self-control Tangney et al. (2004)	I have a hard time breaking bad habits
	I say inappropriate things

Financial benefits Posey et al. (2015)	I could be rewarded financially for choosing to abuse my organization’s computer systems
	I believe others would be willing to reward me financially for intentionally abusing my organization’s information systems
Psychological contract violation Robinson and Morrison (2000)	I have not received everything promised to me in exchange for my contributions
	My employer has broken many of its promises to me even though I’ve upheld my side of the deal

Table A1. Examples of Survey Items