Do individual employees' security compliance intentions relate to workgroup security effectiveness?

Chul Woo Yoo
Florida Atlantic University, chulwooy@buffalo.edu

Jahyun Goo
Florida Atlantic University, jgoo@fau.edu

H. Raghav Rao
The University of Texas at San Antonio, hr.rao@utsa.edu

Recommended Citation

Yoo, Chul Woo; Goo, Jahyun; and Rao, H. Raghav, "Do individual employees' security compliance intentions relate to workgroup security effectiveness?" (2022). *ICIS 2022 Proceedings*. 4.
https://aisel.aisnet.org/icis2022/security/security/4

Do individual employees' security compliance intentions relate to workgroup security effectiveness?

Short Paper

Chul Woo Yoo, Jahyun Goo
Florida Atlantic University
Boca Raton, FL33431 USA
yooc@fau.edu, jgoo@fau.edu

H. Raghav Rao
University of Texas at San Antonio
San Antonio, TX 78249 USA
hr.rao@utsa.edu

Abstract

This paper examines how individual security inputs i.e., security compliance intention and perceived security knowledge, are processed to produce workgroup information security effectiveness in the workgroup. Based on the input-process-output framework, we investigate the multi-level relationships between focal variables. For the analysis, multi-level structural equation model will be used. In particular, the study potentially contributes to the understanding of the security management by showing how individual compliance intention can be mediated by security knowledge coordination and how this mediation works conditionally based on empowering security leadership and perceived security knowledge. Further possible contributions are discussed in the paper.

Keywords: workgroup security, compliance, empowering leadership, knowledge coordination

Introduction

Extant literature on cybersecurity views information security (ISec) as an individual phenomenon under the implicit assumption that the organization's ISec success is determined by individual employees' security behaviors. As a result, a majority of behavioral ISec studies strive to direct an individual employee to comply with IS policies in an effort to protect the organization's information and technology resources. Against this backdrop, past research in the area of ISec has primarily focused on individuals' ISec behaviors or deviations and have therefore adopted individual compliance intention as a dependent variable (Cram et al. 2019). Perhaps, this would be right approach if the individual employee's intention is simply added to the performance of ISec management at the unit level.

However, because employees are often considered as weak links and at the same time, as key allies in strengthening ISec of an organization (Moody et al. 2018), this assertion may not be necessarily true when it comes to measuring the effectiveness of ISec at the workgroup level. Individual security intention, as the literature has identified (Chen et al. 2021; D'Arcy et al. 2014), would be highly likely to intertwine and interact with many other (supporting and hindering) factors in the workplace, that would have an impact on organizations' actual ISec effectiveness (Da Veiga and Eloff 2010). For example, although an individual employee can have compliance intention, when there is little support at the time that knowledge or accommodations are needed from colleagues or team leaders, then individual intention can be weakened, leading to ISec negligence. An examination of prior ISec literature reveals that, studies that have examined these important links between individual compliance intention and achievement of the ISec effectiveness at the group level are scarce.

Organizations are often concerned with the effectiveness of ISec and thus employ value-focused assessment through a set of ISec metrics integrating not just individual compliance behaviors but also a process executed at the workgroup level to attain desired ISec goals in an organization (Dhillon and Torkzadeh 2006). Given the importance of individual's ISec behaviors, it would be natural to expect that group processes would play a key role that consolidates members' individual inputs into collective performance (Marks et al. 2001). Johnston et al. (2019) and Yoo et al. (2020) have advanced this view suggesting the importance of workgroup characteristics in ISec management. However, there are few empirical follow-up studies regarding which group processes work and how they interact with each other for effective workgroup ISec. Specifically, little is known as to how security compliance intention can be materialized towards the ISec effectiveness in the workgroup. This, we believe, is a significant omission in the literature that calls for developing an understanding about the collective security practices of employees and the interactions therein in workgroups. In this paper, we suggest that empowering security leadership and ISec knowledge coordination would play instrumental roles in such context as they would guide individual employees towards ISec actions that best materialize individuals' heightened ISec compliance intentions in pursuit of the desired workgroup ISec effectiveness.

Advancing this view, our study fills the gaps in the extant literature of ISec by explicitly and empirically examining the link between individual employees' security compliance intention and the effectiveness of ISec at the workgroup level. We view that group properties play a crucial role in materializing individual security compliance intentions into the desired effect in attaining the group's security goals and objectives. Taking a multilevel approach, we capture both group and individual properties in pursuit of ISec effectiveness. Specifically, using the input-process-output (IPO) model of workgroup effectiveness (Mathieu et al. 2008) as an overarching theoretical framework, we develop an integrated model that depicts Process (P) mediates inputs (I) of individual security compliance intention and perceived security knowledge to outputs (O) of workgroup ISec effectiveness (WISE). Specifically, we examine the effect of two mediator variables as process (P) – (a) empowering security leadership, a leadership style whereby power is shared with subordinates and that raise their level of intrinsic motivation in the workgroup, and (b) security knowledge coordination, an unfolding process of linked security knowledge and interrelated actions to realize a collective security performance when delivering the individual employees' security compliance intention to the workplace security effectiveness. The goal of the current study is to answer two questions: (1) How does individual employees' security compliance intention directly affect WISE? (2) How do group processes and mechanisms operationalized through empowering security leadership and security knowledge coordination mediate and moderated mediate the relationships between security compliance intention, perceived security knowledge and WISE? To answer these questions, we plan to conduct a field study in a large software development organization in South Korea. More details about the methods, analysis and expected contributions will be addressed and discussed in the last section.

Security Compliance Intention and Security Effectiveness

Since employees within an organization are often viewed as a cause of ISec (Moody et al. 2018), a plethora of ISec studies have mainly been motivated to direct the individual employees' security compliance behaviors in ways to mitigate the security risks (Cram et al. 2019). Consequently, the ISec literature in the past decade zeroed in on examining the individual employees' security compliance intention because criminological research widely accepts measures of intention as indicative of a motivation state or predisposition to commit an act (Pogarsky 2004). These studies basically assume that the individual employees' heightened security compliance intention would lead to positive security behaviors, which in turn determine an organization's ability to successfully manage ISec incidents (Moody et al. 2018; Yazdanmehr and Wang 2016; Yoo et al. 2018).

While enhancement of individual intentions is an essential starting point for directing individuals' security compliance behaviors, the use of intention as the dependent variable raises various questions. 1) does intention indicate actual behavior given the possibility of intention-behavior gap (Sheeran 2002), and 2) can individual security compliance intentions simply bring about ISec effectiveness in the course of performing individuals' jobs, for which concerted security response actions of groups of individual employees are often expected (Johnston et al. 2019). In order to answer this, we draw on previous studies that have pointed out the discrepancies between intention and actual behavior. For example, Sheeran et al. (2002) demonstrated through a meta-analysis that 72% of the variance of behavior has not been explained by intentions. Cram et al. (2019) pointed out the limitation of using intention in explaining ISec behaviors.

Consistent with this view, past ISec studies also hint that actual security behaviors are by no means guaranteed by security compliance intention due to the employees' deliberate violation or neutralization of information security policies (ISPs) when facing with the productivity concerns at work (Chen et al. 2021; D'Arcy et al. 2014). For instance, Gwebu et al. (2020) showed that deviating from the premise of deterrence theory, individual employees' violation of ISPs is not always best explained by fear of sanctions because employees may use rationalizations which allow them to minimize the perceived harm of their policy violations. It is further exacerbated by conflicting results about prior literature shows for the effectiveness of deterrent measures employed to overcome the problem of employees' negligent security compliance (Li et al. 2021). Such cases indicate that, although the literature has made excellent contributions to predicting an individual's security compliance intention, ISec studies with individual employee security compliance intention still demands an extension with approaches that empirically attest its clear linkage to the desired ISec effectiveness, i.e., the practical goals of ISec management (NIST 2008).

This paper argues that the relationship between individual security compliance intention and group security performance is more complex than a simple aggregation of individual security behaviors. This is in a similar vein to recent literature in ISec that has recognized the aforementioned discrepancies and limits of individual-level approach in ISec management. An increasing number of ISec researchers have begun adopting group-level perspectives to bridge the intention-behavior gap as well as addressing effectiveness of ISec at the workplace because the group-level ISec concerns with the ISec performance in the course of performing their jobs (Johnston et al. 2019; Kozlowski and Bell 2013; Yoo et al. 2020). Specifically, recent studies have identified a set of ecological and social properties of groups such as security collective efficacy (Johnston et al. 2019), security coordination (Yoo et al. 2020), empowering leadership (Srivastava et al. 2006) and extra role behaviors (Hsu et al. 2015) that are salient to the members' protective ISec actions (Boss et al. 2015) and responses (Hsu et al. 2012) for the ISec effectiveness of workgroup as a whole.

Advancing this view, this paper provides a bridge between individual-level and group-level security phenomena by examining the effect of group properties, alongside the individual-level factors, on ISec effectiveness. Specifically, the current study explicitly and empirically examines the link between individual employees' security compliance intention and workgroup ISec effectiveness. Drawing on input-process-output (IPO) model of workgroup effectiveness (Mathieu et al. 2008), we identify appropriate group properties and theorize their roles in the group-level process through which the individual employees security compliance intention translates into ISec effectiveness at the workgroup level.

Extended Input-Process-Output Framework

Since McGrath (1964) advanced an IPO framework for studying group effectiveness, group effectiveness studies have long advocated IPO frameworks (Mathieu et al. 2008). While the IPO model has served as a valuable guide for researchers over the years, it has also been modified and extended in several ways (Ilgen et al. 2005; Mathieu et al. 2008). Most adaptations to the IPO model have either rediscovered more subtle aspects of the model that have been overlooked or placed it in an existing complex work arrangement. To this end, Ilgen et al. (2005) have suggested that IPO models be expanded to consider "the broader range of variables that show important mediational influences with explanatory power for explaining variability in team performance and viability" (p. 520). Another extension of IPO framework has also been made to embrace the inherent multilevel nature of groups, in which individual members are nested in groups (Klein and Kozlowski 2000; Mathieu et al. 2008). Consistent with the extended view of the IPO framework, we adopt a multilevel model and propose individual security compliance intention as input, empowering leadership and security knowledge coordination as processes combining two categories of mediating mechanisms, and workgroup ISec effectiveness (WISE) as output at the group level.

Input in the IPO framework describes antecedent factors that enable and constrain members' interactions (Mathieu et al. 2008). In this study, we focus on the security compliance intention (SCI) and perceive security knowledge (PSK) of individual employees as an input. While the majority of past ISec research has primarily focused on understanding how such individual input of security compliance intention can be induced, it still has a way to go to match developments in the performance domain. Guided by NIST's practical concerns (NIST 2008), we attempt to answer the generic question of how mediating processes can explain the impact of SCI and PSK on ISec effectiveness and viability at the workgroup level, and what makes some workgroups more effective or more viable relative to others.

Process may present a broader range of variables that provide important mediational influences in group performance and viability (Ilgen et al. 2005). Thus, process in the extended IPO framework includes both classes of mediator variables – group processes and emergent states. Group processes refer to members' actions directed toward task accomplishment, coordinating team members, as well as monitoring and backing up their fellow team members whereas emergent states describe other mediating mechanisms conceived of as cognitive, motivational, or affective states (Marks et al. 2001). Although there are a fairly large set of emergent states and processes examined in the literature (Kozlowski and Bell 2013), we have identified security knowledge coordination (SKC) and empowering security leadership (ESL) as a key mediating process and emergent state mechanism that allow the current research model to be conceptually and empirically parsimonious and focused.

Lastly, output (O) includes results and by-products of group activity that are valued by one or more constituencies (Mathieu et al. 2008). They may broadly include performance (e.g., quality and quantity) and effectiveness (e.g., viability). As a collective agency in an organization, the workgroups are expected to effectively manage ISec incidents through collective actions of members within their workgroup boundaries (Zohar 2014). Thus, output in the current study corresponds to WISE as a measure for collective ISec effectiveness and shows the viability of attaining ISec goals set at the workgroup level.

Security Knowledge Coordination

In this study, we propose security knowledge coordination as an important component of group process for workgroups. The group performance literature has demonstrated that success of workgroup is not only a function of individual members' capabilities and available resources, but also the processes members use to interact with each other to accomplish the work (Barrick et al. 2007). Rather, the desired group performance is achieved when knowledge is effectively coordinated (Kanawattanachai and Yoo 2007; Rico et al. 2008). Knowledge coordination is thus identified as a critical group process because if not properly coordinated, the cognitive resources available within a group remains underutilized.

We define security knowledge as the ISec skills and know-how that an individual brings to the workgroup's task. Coordination refers to workgroup-situated interactions aimed at managing resources and knowledge dependencies. Thus, security knowledge coordination entails the workgroup's awareness of security knowledge location dispersed across the workgroup members with group-situated interactions implied for managing security knowledge dependencies and knowledge orchestration in order to effectively and timely respond to the tasks that require security attention (Gabelica et al. 2016). Having sufficient security knowledge is critical for mitigating ISec risks and managing overall organizational security effectiveness. Individual employees are typically considered as the principal agents who are expected to possess security knowledge and skills so that appropriate security measures should be exercised corresponding to specific security incidents and threats (Herath and Rao 2009). However, security knowledge coordination involves group processes, as workgroups are known as the foundation upon which its members' ISec collective actions are formed, and thereby realizing its members' security knowledge and skills into tangible results. To this regard, Johnston et al. (2019) empirically illustrated that the practices of using organizational memory, and collective induction/reflection in the workgroups positively related to workgroup's ISec response quality and are thus salient to workgroup' ISec effectiveness. Security knowledge coordination in workgroups, thus, engenders the efficient use of security knowledge that resides in workgroup members by preventing redundant deployment of security practices or reinvention of the security wheel. Although overarching organizational security policies and procedures control individual compliance intention, security knowledge coordination in the workgroup synchronizes individual members' security intent through the workgroup's own processes and enforcement, thereby collectively achieving workgroup information security effectiveness (WISE) (Yoo et al. 2020).

Empowering Leadership

Empowering leadership is defined in terms of behaviors whereby power is shared with subordinates and that raise their level of intrinsic motivation (Srivastava et al. 2006). Management literature has substantiated the role of empowering leadership in group process. Empowering leadership helps develop collaborative norms among members, enact subordinates to express opinions and ideas freely, promote collaborative decision making and collective information processing in workgroup (Lorinkova et al. 2013). We extend the literature and propose empowering leadership as a powerful mechanism by which workgroup members' involvement and motivation is leveraged to become more flexible and responsive to security knowledge coordination process. We agree that security knowledge coordination process within groups, although critical, may not come in handy without appropriate administrative support (Srivastava et al. 2006). Because information security is not a core task of non-security personnel, involvement in the coordinating process of security knowledge itself may come as an extra burden with concerns of productivity of business tasks in workgroup. However, as security breaches within the workgroup are getting more sophisticated and challenging for an individual member to handle, the leadership is expected to properly leverage members' security skills and expertise available within the group so as to remain effective in responding to those incidents (Johnston et al. 2019). To this regard, past studies provide a strong indication that empowering leadership would play a pivotal role in nurturing the knowledge coordination and sharing in the workgroups (Srivastava et al. 2006; Xue et al. 2011). Therefore, we believe that proper group process such as security knowledge coordination occurs when group empowerment is present.

Model and Hypotheses Development

Drawing on the IPO model, we have developed an integrated model to provide insights into the impacts of group process of empowering security leadership and security knowledge coordination on the relationship between individual security compliance intention (SCI) and perceived security knowledge on WISE. A central premise of the model is that the relationship between SCI and WISE should be mediated by security knowledge coordination, and this mediation is also conditioned on the presence of empowering security leadership in the workgroups. Lastly, this model tests the 3-way interaction effect of SCI, perceived security knowledge and empowering security leadership on security knowledge coordination. As such, the research model in Figure 1 depicts the cross-level relationships among variables at either individual or group levels.

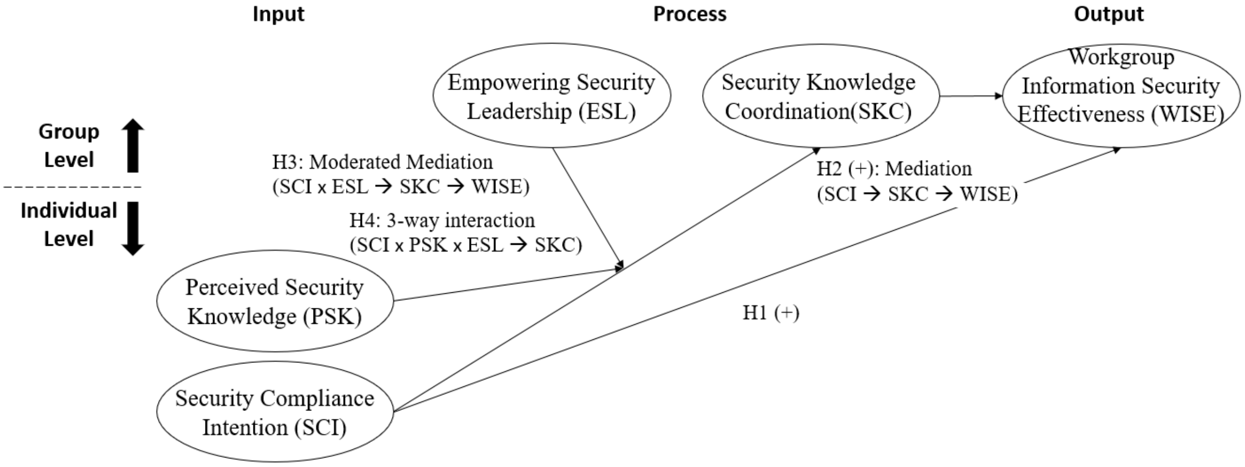
Input
Process
Output
Group Level
Individual Level
Empowering Security Leadership (ESL)
Security Knowledge Coordination(SKC)
Workgroup Information Security Effectiveness (WISE)
H3: Moderated Mediation (SCI x ESL → SKC → WISE)
H4: 3-way interaction (SCI x PSK x ESL → SKC)
H2 (+): Mediation (SCI → SKC → WISE)
H1 (+)
Perceived Security Knowledge (PSK)
Security Compliance Intention (SCI)

Figure 1. The Research Model

Individual Security Compliance Intention

Behavioral ISec literature indirectly suggests that employees' security compliance intention (SCI) would help organizations maintain good ISec. We also view that SCI emanated from the personal determination and belief that an individual employee wants to protect the organizational ISec from possible threats by utilizing specific security technologies or procedures. In this study, SCI is defined as the extent to which an employee has a determination to comply with the security policy applicable to the workgroup that she belongs to. We think that an individual employee's compliance intention may lead to protecting information assets and technological resources shared in the workgroup although it is not her own individual assets because of employees' sense of belonging and responsibility shared through psychological ownership (Yoo et al. 2018). It can be truer when the workgroup is related to software development like this study. individual's threat inducing behavior (e.g., security non-compliance) can harm the whole project as a result. In addition, drawing on rational choice theory, Bulgurcu et al. (2010) showed that SCI is related to protecting the informational resources, resulting in safety of informational assets in the organization. Therefore, if there are employees who are willing to comply with organizational ISPs within a workgroup, we can assume that workgroup is likely to have good ISec effectiveness. Based on the discussion above, we postulate that SCI, although being at the individual level, may bring a positive effect on WISE.

H1 – Individual employees' security compliance intention in a workgroup is positively related to workgroup information security effectiveness.

Workgroup Security Knowledge Coordination

Given the workgroup's common conditions where members maintain a certain level of heterogeneity in skills, knowledge and experiences, the management literature suggests that heedful interactions that support the application of the skills and knowledge are important in group-level outcomes (Gupta et al. 1994; Nidumolu 1995). In this study, security knowledge coordination is defined as the extent to which the workgroup ensures the newly constructed necessary security policies and knowledge is put into practice in a coordinated way. We believe that knowledge coordination literature can be extended to our study context of workgroup security effectiveness. It could be interpreted that security knowledge coordination are fundamentally learning processes and is a function of learning mechanisms occurring when workgroup members interact and discuss their task and their workgroup. As Whitman and Mattord (2017) pointed out, collective ISec at the workgroup level security practices does not happen automatically in a workgroup without knowing workgroup-level processes. Coordinating the divergent security knowledge and skills within a workgroup would be important so that workgroup becomes an increasingly high-performing system (Zellmer-Bruhn and Gibson, 2006). In addition, in the interdependent nature of workgroup ISec, security knowledge coordination also functions as a complementary to individual security intention in a way to enhance the security effectiveness of workgroup. We posit that members' heightened security compliance intention can be translated into expected outcome when individual employees' security skills and knowledge are well coordinated for the workgroup ISec goals (Preacher et al. 2007). Thus, we posit:

H2 – Security knowledge coordination mediates the relationship between security compliance intention and workgroup information security effectiveness.

Workgroup Empowering Security Leadership

An empowering leader who possesses these attributes is seen as a supportive leader who provides guidance to followers, develops the workgroup climate for teamwork, shows coaching behaviors, and recognizes the value of their input (Locke et al. 1997; Xue et al. 2011). In this study, we narrow down the scope of the original meaning of the construct, and apply it to the security management context in the workgroup. Empowering security leadership is defined as the extent to which the workgroup leader motivates workgroup members to be more participatory, shares the authority, and provides close coaching in the workgroup security management. Lorinkova et al. (2013) suggested that empowering leaders promote shared learning and the decision-making climate that results in emergence of collective processes, such as coordination in teams, enable teams to attain higher levels of performance in the long run. As such, workgroup leaders have an important role to play in actualizing workgroup's potential (Jung and Sosik 2002). It helps workgroup members to clarify the goals, share the necessary know-hows, exhibit their ability and pursue the collective performance (Locke et al. 1997). Consistent with the empowering leadership literature (Marks et al. 2001; Van Vugt et al. 2008) and following the view of the extended IPO model (Srivastava et al. 2006; Yoo et al. 2020), we think that empowering security leadership alone does not directly produce effectiveness of workgroup ISec. Instead, empowerment in a workgroup works with individual input to facilitate group-level processes and operate like conditions that make group processes happen (Mathieu et al. 2008). Specifically, empowering security leadership can specify a condition when the mediating path of SCI - security knowledge coordination - WISE holds. An empowering leader would give members a chance to voice their opinions and encourage them to express suggestions regarding a member's ISec issues. Given that members expect to receive fair recognition by an empowering leader for their contribution of their ISec, they are likely to be motivated to collaborate with others (Srivastava et al. 2006). This implies that empowering security leadership in a workgroup may pull a trigger of members' SCI to actual participation in security knowledge coordination, which in turn leads to the attainment of collective ISec goals. Based on the arguments above, we hypothesize:

H3 – Empowering security leadership moderates the mediation effect of security knowledge coordination on the relation between employees' security compliance intention and workgroup information security effectiveness.

In addition, we believe individuals' security knowledge level plays an important role in developing the security knowledge coordination which is the one of core processes in the model. For example, although when employee have strong compliance intention, she can have poor security knowledge, and vice versa.

Testing the 3-way interaction helps us to understand how employee with poor security knowledge with good intention can be benefited by the coordination or slow down the coordination or vice versa. In this study, we conceptualize this as perceived security knowledge. Perceived security knowledge is defined as the extent which an employee perceive she has good security knowledge regarding the workgroup security policy and management. Knowledge coordination literature illustrates that matured knowledge facilitates the knowledge coordination (Mathieu et al. 2008) and empowering leadership can be more effective with more knowledgeable members (Lorinkova et al. 2013). Based on the argument above, we posit:

> H4 – The 3-way interaction among security compliance intention, perceived security knowledge and empowering security leadership is associated with security knowledge coordination.

Methods

Data Collection

Data will be collected from one large security software development company in South Korea. There are several reasons why this targeted organization is appropriate for the data collection. First, there are many independent teams that develop different applications or modules for different projects in the organization. Hence, by focusing on these teams, we can measure members' perception about coordination and leadership within the teams properly. At the same time, according to the organizational security policies, each team pay much attention to security when the teams develop its projects. Therefore, security is not an unfamiliar or retrospective topic to most of potential respondents. It is rather an ongoing topic that needs employees' attention. We plan to collect the data from at least 50 different teams, 500 individual employees and 20 managers from this organization. Our research model investigates how workgroup processes, i.e., security knowledge coordination and empowering security leadership affect individual inputs, i.e., security compliance intention and perceived security knowledge. So we will collect the data of security compliance intention and perceived security knowledge first from the workgroup members. Then, the data of empowering security leadership and security knowledge coordination will be collected from the workgroup members. WISE will be measured by managers. The timespan between the first data collection and the second data collection will be three months, which is one of the common task cycles of the targeted organization. However, details can be changed based on the situation of the organization.

Measurements

Measurement items for the focal constructs are based on an extensive literature review of previous research. All predictor variables in the survey will be measured using multi-item scales with 5-point Likert rating systems. When possible, the measurement items of the constructs were adapted from existing scales in extant literature that have proven to be reliable. For example, to capture security compliance intention, we consulted Herath and Rao (2009), and Moody et al. (2018)'s works. However, the items were revised to reflect the workgroup context. For perceived security knowledge, we developed our own measurement to reflect three dimensions including ISP awareness, perceived depth of security knowledge, perceived timeliness of security knowledge. For empowering security leadership, Xue et al. (2011)' work was consulted. But items were also revised to reflect the security context. We used Yoo et al. (2020)'s work for security knowledge coordination. Lastly, for WISE, Hsu et al. (2015)'s work was consulted.

In addition, the referent-shift design was employed to ensure that our focal constructs properly capture group-level phenomena using group-referent items (Gully et al. 2002; Van Mierlo et al. 2009). As such, the group-referent items are intended to capture the respondents' perceptions of the group's traits or abilities, as opposed to the respondents' perceptions of their own. Specifically, following Hofmann (2004), the items of latent constructs are carefully written with collective terms, such as "our workgroup" instead of "I," to properly shift the referent point of construct from an individual orientation to a group orientation. Lastly, in regard to measurements of WISE, this study examines the manager's evaluation on workgroup's overall security performance. Measurement items will be provided based upon the request due to the page limit.

Analysis

We will collect data at two different levels from two different sources. Although we design to use group-referent items to measure the group level phenomena, there may exist within-group difference in empowering leadership and security knowledge coordination. On the other hand, WISE is measured only for group. As a result, the research model will have a so-called bottom-up relationship between the independent variables and the dependent variable. We plan to use the multilevel structural equation modeling (MSEM) approach with Mplus to test hypotheses. This method is appropriate to test the latent variables with multi-level relationships in which the individual group member's perception about the group impacts group performance (Yoo et al. 2020). This method causes minimal statistical problems because it does not aggregate the individual-level predictors to the group-level or disaggregate the group-level outcome variables to the individual-level to fit in with a single-level regression. In addition, the approach of Kim and Hong (2020) will be used to test the multilevel moderated mediation for H3.

Expected Contributions

We want to hear more feedback from the ICIS. The data collection will start after more updates based on the feedback. However, the following contributions are expected. First, findings from a multi-level analysis via IPO framework will empirically show whether or not the ISec effectiveness at the workgroup can be realized as simple aggregate of employees' security compliance intention (SCI). This finding would be particularly meaningful when considering the fact that organization's effectiveness is achieved through efforts of hierarchical nesting and coupling of groups of employees. Second, the results of the mediation effect of SKC on the relationship between individual employees' SCI and workgroup ISec effectiveness will shed light on security knowledge sharing research by suggesting that SKC embedded in the group settings is a crucial process by which the individual compliance intention is manifested for workgroup's ISec effectiveness. Lastly, our test of the multi-level moderated mediation effect will clearly articulate that empowering leadership can play an important role in the relationship of SCI → SKC→ WISE. Although new to the ISec context, the role of empowering security leadership in the ISec context confirms its important virtue in managing groups, alongside the individual compliance, because it gives autonomy to workgroup members and makes them participative. For future studies, it is expected that this study will provide pivotal opportunities in investigating potential workgroup processes in the information security research.

References

Barrick, M. R., Bradley, B. H., Kristof-Brown, A. L., and Colbert, A. E. 2007. "The moderating role of top management team interdependence: Implications for real teams and working groups," *Academy of Management Journal* (50:3), pp 544-557.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Quarterly* (39:4), pp 837-864.

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.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., and Willison, R. 2021. "Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model," Information Systems Research (32:3), pp 1043-1065.

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).

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.

Da Veiga, A., and Eloff, J. H. 2010. "A framework and assessment instrument for information security culture," Computers & Security (29:2), pp 196-207.

Dhillon, G., and Torkzadeh, G. 2006. "Value-focused assessment of information system security in organizations," Information Systems Journal (16:3), pp 293-314.

Gabelica, C., Van den Bossche, P., Fiore, S. M., Segers, M., and Gijselaers, W. H. 2016. "Establishing team knowledge coordination from a learning perspective," Human Performance (29:1), pp 33-53.

Gully, S. M., Incalcaterra, K. A., Joshi, A., and Beaubien, J. M. 2002. "A meta-analysis of team-efficacy, potency, and performance: Interdependence and level of analysis as moderators of observed relationships," Journal of Applied Psychology (87:5), pp 819-832.

Gupta, P. P., Dirsmith, M. W., and Fogarty, T. J. 1994. "Coordination and Control in a Government Agency: Contingency and Institutional Theory Perspectives on Gao Audits," Administrative Science Quarterly (39:2), pp 264-284.

Gwebu, K. L., Wang, J., and Hu, M. Y. 2020. "Information security policy noncompliance: An integrative social influence model," Information Systems Journal (30:2), pp 220-269.

Herath, T., and Rao, H. R. 2009. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," Decision Support Systems (47:2), pp 154-165.

Hofmann, D. A. 2004. Issues in Multilevel Research: Theory Development, Measurement, and Analysis, (Wiley-Blackwell: Malden, MA.

Hsu, C., Lee, J.-N., and Straub, D. W. 2012. "Institutional influences on information systems security innovations," Information Systems Research (23:3), pp 918-939.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The role of extra-role behaviors and social controls in information security policy effectiveness," Information Systems Research (26:2), pp 282-300.

Ilgen, D. R., Hollenbeck, J. R., Johnson, M., and Jundt, D. 2005. "Teams in organizations: From input-process-output models to IMOI models," Annual Review of Psychology (56), pp 517-543.

Johnston, A., Di Gangi, P., Howard, J., and Worrell, J. 2019. "It takes a village: understanding the collective security efficacy of employee groups," Journal of the Association for Information Systems (20:3), pp 186-212.

Jung, D. I., and Sosik, J. J. 2002. "Transformational leadership in work groups the role of empowerment, cohesiveness, and collective-efficacy on perceived group performance," Small Group Research (33:3), pp 313-336.

Kanawattanachai, P., and Yoo, Y. 2007. "The impact of knowledge coordination on virtual team performance over time," MIS Quarterly (31:4), pp 783-808.

Kim, S., and Hong, S. 2020. "Comparing methods for multilevel moderated mediation: A decomposed-first strategy," Structural Equation Modeling: A Multidisciplinary Journal (27:5), pp 661-677.

Klein, K. J., and Kozlowski, S. W. 2000. Multilevel theory, research, and methods in organizations: Foundations, extensions, and new directions, (Jossey-Bass: San Francisco, CA.

Kozlowski, S. W. J., and Bell, B. S. 2013. Work Groups and Teams in Organizations: Review Update, (Wiley: Hoboken, NJ.

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.

Locke, E. A., Alavi, M., and Wagner III, J. A. 1997. Participation in decision making: An information exchange perspective, (JAI Press: Greenwich, CT.

Lorinkova, N. M., Pearsall, M. J., and Sims, H. P. 2013. "Examining the differential longitudinal performance of directive versus empowering leadership in teams," Academy of Management Journal (56:2), pp 573-596.

Marks, M. A., Mathieu, J. E., and Zaccaro, S. J. 2001. "A temporally based framework and taxonomy of team processes," Academy of Management Review (26:3), pp 356-376.

Mathieu, J., Maynard, M. T., Rapp, T., and Gilson, L. 2008. "Team effectiveness 1997-2007: A review of recent advancements and a glimpse into the future," Journal of Management (34:3), pp 410-476.

McGrath, J. E. 1964. Social psychology: A brief introduction, (Holt, Rinehart & Winston: New York, NY.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a unified model of information security policy compliance," MIS Quarterly (42:1), pp 285-311.

Nidumolu, S. 1995. "The effect of coordination and uncertainty on software project performance: Residual performance risk as an intervening variable," Information Systems Research (6:3), pp 191-219.

NIST 2008. "Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Revision 1," National Institute of Standards and Technology, Gaithersburg, MD.

Pogarsky, G. 2004. "Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity," Criminology (42:1), pp 111-136.

Preacher, K. J., Rucker, D. D., and Hayes, A. F. 2007. "Addressing moderated mediation hypotheses: Theory, methods, and prescriptions," Multivariate Behavioral Research (42:1), pp 185-227.

Rico, R., Sánchez-Manzanares, M., Gil, F., and Gibson, C. 2008. "Team implicit coordination processes: A team knowledge–based approach," Academy of Management Review (33:1), pp 163-184.

Sheeran, P. 2002. "Intention—behavior relations: A conceptual and empirical review," European review of social psychology (12:1), pp 1-36.

Srivastava, A., Bartol, K. M., and Locke, E. A. 2006. "Empowering leadership in management teams: Effects on knowledge sharing, efficacy, and performance," Academy of Management Journal (49:6), pp 1239-1251.

Van Mierlo, H., Vermunt, J. K., and Rutte, C. G. 2009. "Composing group-level constructs from individual-level survey data," Organizational Research Methods (12:2), pp 368-392.

Van Vugt, M., Hogan, R., and Kaiser, R. B. 2008. "Leadership, followership, and evolution: Some lessons from the past," American Psychologist (63:3), p 182.

Whitman, M. E., and Mattord, H. J. 2017. Principles of Information Security, (6th ed.) Cengage: Boston, MA.

Xue, Y., Bradley, J., and Liang, H. 2011. "Team climate, empowering leadership, and knowledge sharing," Journal of Knowledge Management (15:2), pp 299-312.

Yazdanmehr, A., and Wang, J. 2016. "Employees' information security policy compliance: A norm activation perspective," Decision Support Systems (92), pp 36-46.

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

Yoo, C. W., Sanders, G. L., and Cerveny, R. P. 2018. "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance," Decision Support Systems (108:1), pp 107-118.

Zohar, D. 2014. "Safety Climate: Conceptualization, Measurement, and Improvement," in The Oxford Handbook of Organizational Climate and Culture, Oxford University Press: Oxford, UK, pp. 317-334.