Dec 12th, 12:00 AM

Investigating Employees' Proactive Extra-Role Information Security Behaviors through Security Mindfulness

Bowen Guan
University of Sydney, guanbwe@163.com

Carol Hsu
University of Sydney, Carol.hsu@sydney.edu.au

Investigating Employees' Proactive Extra-Role Information Security Behaviors through Security Mindfulness

Short Paper

Bowen Guan
University of Sydney Business School
Corner Abercrombie Street and,
Codrington St, Darlington NSW 2006
bowen.guan@sydney.edu.au

Carol Hsu
University of Sydney Business School
Corner Abercrombie Street and,
Codrington St, Darlington NSW 2006
carol.hsu@sydney.edu.au

Abstract

Connecting mindfulness with organizational information security (InfoSec) is an increasingly attractive research topic. This paper conceptualizes InfoSec mindfulness as a dynamic InfoSec-specific trait evident when handling organizational information assets. We articulate the motivational factors that contribute to InfoSec mindfulness and the effects of InfoSec mindfulness on employees' proactive extra-role information security behaviors (ISBs), which refers to self-initiated and future-oriented behaviors that go beyond an organization's information security policies (ISPs) and are independent on rewards or punishments. This paper provides significant theoretical contributions to InfoSec behavioral literature by conceptualizing InfoSec mindfulness and deepening the understanding of proactive extra-role ISBs. We also summarize our research methodology to develop the scale of InfoSec mindfulness and test its validity for our future study.

Keywords: InfoSec mindfulness, dynamic InfoSec-specific trait, proactive extra-role ISBs, organizational InfoSec governance

Introduction

Mindfulness is a psychological concept introduced by Langer (1989) as a watchful and vigilant state which is characterized by the refinement of existing categories, creation of new categories, and an increase in greater awareness of multiple perspectives. Prior studies also show that mindfulness enables individuals to detect changes in their environment and create new ways to understand the present and future opportunities for actions (Bishop et al. 2004; Langer and Moldoveanu 2000; Langer 1997). Given its proven benefits, information systems (IS) scholars have linked mindfulness with various IS contexts ranging from improving IT innovation (Fichman 2004; Swanson and Ramiller 2004), IS reliability (Butler and Gray 2006), IT management at the organizational (Wong et al. 2009), to promoting IT adoption at the individual level (Sun et al. 2016; Thatcher et al. 2018). Recently, connecting mindfulness with information security (InfoSec) management is becoming a topical issue in practice. Industrial reports suggested that security mindfulness practices can improve employees' abilities to pay attention to information processing and assess security threats before taking reactions (Warner 2022), thus, practicing cybersecurity mindfulness extended to the entire organization would be a crucial managerial strategy for organizational InfoSec (Feather 2020). Considering its significant role in defending against security attacks, there is a need to deepen our understanding of InfoSec behaviors from the perspective of InfoSec mindfulness. However, scholarly empirical research in this area to date remains limited and theoretical conceptualization of InfoSec mindfulness has yet to emerge.

Therefore, we aim to theoretically conceptualize InfoSec mindfulness and empirically examine its effect on individuals' InfoSec behaviors (ISBs). Drawn upon a hierarchy view of personality traits, we define *InfoSec mindfulness* as a dynamic InfoSec-specific trait, evident when handling organizational information assets, whereby an individual exhibits the ongoing scrutiny of existing organizational InfoSec policies (ISPs), an enriched awareness, and alertness to potential information security threats and risks. Distinct from InfoSec awareness which reflects an acceptance-based consciousness often raised through a regular and repeated rule-based training approach from organizations (Puhakainen and Siponen 2010; Siponen 2000), InfoSec mindfulness implicates a more proactive capability and overarching mental mindset, going beyond the fact of knowing or being aware. It is an introspection-based trait that can dynamically allocate one's attention to security attacks and forestall judgment of suspicious detail (Jensen et al. 2017). Specifically, an InfoSec mindful individual tends to be alert to any security threats and proactively perform recommended actions to successfully defend against such threats.

Given the nature of InfoSec mindfulness and its potential impacts on ISBs, we hold our particular interest in the role of InfoSec mindfulness in motivating employees' *proactive extra-role ISBs*, which refers to the self-initiated and future-oriented actions that are beyond the requirements of an organization's ISPs and independent on any rewards or punishments (Hsu et al. 2015; Lin and Wittmer 2017), and aim to enact positive changes for InfoSec protection. Security experts have emphasized that empowering proactive actions to identify existing and new InfoSec threats and initiatively eliminate them is of vital importance for organizational InfoSec governance (NCSAM 2021). Encouraging proactive approaches more than reactive tactics, can help actively identify unknown security risks, constantly monitor vulnerabilities in the network infrastructure, so as to ultimately address and mitigate any disruptions and threats in the first place (Mukherjee 2022). Consequently, motivating proactive extra-role ISBs seems to enable dramatically improvements for the whole InfoSec landscape and supplement to the defensive effects of organizational ISPs. However, less is known about what factors might contribute to employees' proactive extra-role ISBs.

To address this research gap, we consider InfoSec mindfulness as a significant motivator to employees' proactive extra-role ISBs. As Hsu et al. (2015) suggested, a mindful employee would be able to identify inappropriate part of an ISP or the vulnerability of a system and provide guidance to improve it. This implies an important research opportunity to link InfoSec mindfulness with proactive extra-role ISBs. We argue that InfoSec mindfulness can motivate employees to engage in proactive extra-role ISBs including proactively implementing ideas on improvements for organizational InfoSec management, and proactively handling security threats and solving problems.

Furthermore, we also consider investigating how an individual's InfoSec mindfulness would be raised. Drawn on Weick and his colleagues' work on high reliability of organizations (HROs) in which they identified several processes of fostering mindfulness to improve organizational reliability, such as preoccupation with failures, reluctance to simply interpretations, sensitivity to operations, and commitment to resilience, we believe that these factors can be contextualized in the InfoSec context as important motivators to InfoSec mindfulness, considering that the goal of achieving organizational InfoSec protection is kind of partial approach to reach high reliability, in that governing organizational InfoSec needs to increase the ability to handle security risks, which is very close to the aim of HROs that is to "mitigate the adverse potential of unexpected events" (Carlo et al. 2012, p. 1081). Notably, extant literature on InfoSec mindfulness remains conceptual level and empirical work on examining its antecedents and effects has yet to emerge. Therefore, we argue that when employees hold the capabilities of *preoccupation with InfoSec threats*, *reluctance to simplify InfoSec interpretations*, *sensitivity to InfoSec operations*, and *commitment to resilience from InfoSec attacks* when handling InfoSec threats, they would be mindful to proactively detect security risks, change and improve their security understanding, and positively seek new ways to protect individual and organizational information assets.

Overall, we put our research focus on theoretically conceptualizing InfoSec mindfulness and empirically examine its antecedents and impacts on employees' proactive extra-role ISBs. Next section will show detailed discussions on the conceptualization of InfoSec mindfulness and the theoretical foundations of our hypotheses, followed by the summarized research methodology and expected contributions and further research directions.

Theoretical Foundations

Conceptualizing InfoSec Mindfulness

Mindfulness refers to an individual's ongoing scrutiny and refinement of expectations "based on new experiences, appreciation of subtleties, and identification of novel aspects of context that can improve foresight and functioning" (Thatcher et al. 2018 concluded from Langer (1989), p. 832). In general, mindfulness involves "the ability to detect important aspects of the context and take timely appropriate action" (Butler and Gray 2006, p. 216). In psychology, mindfulness has been demonstrated to be positively related to stress reduction and mental health (Langer 1989), increased creativity and decreased burnout (Langer et al. 1988), learning (Langer 2000; Levinthal and Rerup 2006), group decision-making (Fiol and O'Connor 2003), organizational reliability (Weick et al. 1999), and the quality of organizational attention (Weick and Sutcliffe 2006).

Given its specific benefits, conceptualizing mindfulness into different IT-related context and examining its impacts has been prevalent in IS discipline. For example, Swanson and Ramiller (2004) defined *IT innovation mindfulness* broadly as the attention to IT innovation with reasoning grounded in organizational own facts and specifics. Thatcher et al. (2018) specifically conceptualized *IT mindfulness* from a three-level hierarchy (i.e., broad, stable, and dynamic) of personality trait, based on their consideration on its impacts on individual behaviors from two dimensions (i.e., breadth of impact and situational variance). With the focus on a specific situation of an immediate task to be completed with a given technology, their conceptualization of IT mindfulness captures "more malleable predispositions to act in specific situations" (in Thatcher et al. (2018) p. 834, concluded from Davis and Yi (2012)), which means that the effects of IT mindfulness on user behaviors are relatively enduring and malleable. Thus, they defined IT mindfulness as "a dynamic IT-specific trait evident when working with IT" (Thatcher et al. 2018, p. 832).

For our conceptualization of InfoSec mindfulness, we believe that a trait perspective should be more relevant as we shared similar considerations with the conceptualization of IT mindfulness, with the focus on the behavioral impacts of traits. Following the hierarchy view of personality trait, we define InfoSec mindfulness as a dynamic InfoSec-specific trait based on the following two reasons. First, it is a trait that has a narrower breadth of impacts on individual behaviors than that of a broad trait because this kind of trait captures the behavioral impacts within a specific InfoSec context (Davis and Yi 2012). Second, such impacts are somewhat malleable and relatively enduring (Thatcher et al. 2018) because it reflects not only predispositions to detect and prevent security threats but also a gradual accumulation of individual experiences of handling security threats. Thus, it might be changed and enhanced by InfoSec training programs.

Factors of Generating InfoSec Mindfulness

To further understand InfoSec mindfulness, we extended Weick and his colleagues' (1999, 2001, 2006) five processes of inducing mindfulness in HROs into our InfoSec context. In their work, their perspective on mindfulness "is grounded patterns of interrelation among processes of perception and cognition that induce a rich awareness of discriminatory detail and a capacity for action" (Weick and Sutcliffe, 2006, p. 515). Therefore, their definition of mindfulness represents "a rich awareness of discriminatory detail generated by organizational processes" (Weick and Sutcliffe, 2006, p. 516), including preoccupation with failures, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise. Notably, the concept of mindfulness in fostering high reliability for organizations is focused on "clear comprehension of emerging threats and on factors that interfere with such comprehension" (Weick and Sutcliffe, 2006, p. 516), derived from the quality of attention to mindful action by Wallance (1999, 2000). Weick and Sutcliffe (2006) suggested that the five specific processes can "lead to greater mindfulness through the processes' effects on the stability (see one thing fully) and vividness (see things clearly) of attention" (p. 519). When people pay more vivid attention to small failures (*preoccupation with failures*), retain their distinctiveness rather than lost in one category (*reluctance to simplify*), "remain aware of ongoing operations if they want to notice nuances that portend failure (*sensitivity to operations*), locate pathways to recovery (*commitment to resilience*) and rely on the expertise to implement those pathways (*deference to expertise*)" (p. 516), these processes would contribute to a rich awareness of discriminant detail and thus foster stubborn reliability.

In our InfoSec context, to enhance individuals' comprehension of organizational InfoSec governance and foster employees' ongoing scrutiny of InfoSec threats, is consistent with the goal of achieving organizational high reliability. Therefore, we assert that some of processes of inducing mindfulness for achieving high reliability can be used to explain the creation of InfoSec mindfulness in our InfoSec context. We contextualize four of the factors proposed by Weick and his colleagues (1999, 2006) into our InfoSec context and consider these as important triggers to employees' InfoSec mindfulness in order to proactively protect organizational InfoSec. Particularly, since *deference to expertise* involves "the migration of decisions to expertise resulting from the under-specification of structures" (Bulter and Gray 2006, p. 216), which reflects a kind of collective effort to reallocate "stable attention by routing decisions to experts who are best able to hold on to the intended object without distraction" (Weick and Sutcliffe 2006, p. 519), rather than through individuals' personal effort to solve the problem, this factor might not be appropriate for our research context. Therefore, we argue that in InfoSec context, preoccupation with InfoSec threats, reluctance to simplify InfoSec interpretations, sensitivity to InfoSec operations, and commitment to resilience from InfoSec attacks can help to foster InfoSec mindfulness.

Preoccupation with InfoSec threats. In Weick and Sutcliffe (2006), *preoccupation with failures* involves "a search for incipient failures to the exclusion of all else" and the term *failures* is plural which reflects "there are multiple objects to monitor" (p. 519). It reflected converting errors and failures into the process of learning and improvement and required scattered, potentially unstable attention to multiple objects. Specifically, it can create mindfulness by helping employees avoid the "overconfidence, complacency, and inattention that can result when employees believe success has become commonplace and routine" (Bulter and Gray 2006, p. 216). In InfoSec context, it can be contextualized as preoccupation with InfoSec threats which means being capable to pay vivid attention to monitoring potential InfoSec threats and risks. We argue that employees who preoccupy with InfoSec threats tend to be in the belief that any small security breach can increase the possibility of a major InfoSec problem, thus, they would foster a closer attention to any security threats and treat them as the windows on protecting InfoSec for the whole organizations. Therefore, we propose that preoccupation with InfoSec threats can induce employees' InfoSec mindfulness.

Reluctance to simplify InfoSec interpretations. Weick and Sutcliffe (2006) indicated that *reluctance to simplify* can create the mindfulness manifested by maintaining divergent points of view when seeing problems and keeping healthy skepticism. It involves a desire to "continually see problems from different perspectives" (Bulter and Gray 2006, p. 216). In the context of mindful IT management, Wong et al. (2009) interpreted it as the attention to multiple perspectives when developing IT applications, embodied by understanding the complex environment and accessing different needs of different IT users. Here, we conceptualized this element as reluctance to simplify InfoSec interpretations which means unwillingness to overlook the details of diverse InfoSec threats and keep multiple perspectives while dealing with even small security warnings. It can induce InfoSec mindfulness by focusing on the details uncovered by an ongoing scrutiny of organizational ISPs. Therefore, we argue that reluctance to simplify InfoSec interpretations can create employees' InfoSec mindfulness.

Sensitivity to InfoSec operations. Being sensitive to operations implies an integrated overall picture of operations at any moment, which can improve the probabilities of the detection of small errors before they produce large failures (Butler and Gray 2006; Carlo et al. 2012; Weick et al. 1999). Weick and Sutcliffe (2006) proposed that both sensitivity to operations and reluctance to simplify involve an increased vivid attention to replace abstractions with current details, but sensitivity to operations emphases on paying attention to what is actually done (i.e., the current operations) rather than what should be done (i.e., those general policies and plans) (Butler and Gray 2006). In line with this notion, we propose that sensitivity to InfoSec operations focuses much more on continuously attentions to practical InfoSec operations than the prescribed organizational ISPs. Thus, it can help to capture potential security threats in everyday handling with organizational information assets and generate ongoing awareness of InfoSec. Therefore, we argue that sensitivity to InfoSec operations can also lead to InfoSec mindfulness.

Commitment to resilience from InfoSec attacks. Resilience refers to the "capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back" (Wildavsky 1991, p. 77). Commitment to resilience proposed by Weick et al. (1999) refers to a well-developed capability to "see the threatening details in even most complex environment" and of paying attention to "both error-prevention and error-containment" (p. 47). This element can generate mindfulness by paying vivid attention to whatever is at hand helpful to resume from the interruptions. In this research, we identified commitment

to resilience from InfoSec attacks as a tendency to cope with security attacks as they arise through security threats detection and security attacks containment. We argue that this would inform InfoSec mindfulness from the perspective of unanticipated security risks prevention. Therefore, commitment to resilience from InfoSec attacks can be an important motivational factor of InfoSec mindfulness. Overall, we propose our hypotheses:

H1: Preoccupation with InfoSec threats is positively related to InfoSec mindfulness.

H2: Reluctance to simplify InfoSec interpretations is positively related to InfoSec mindfulness.

H3: Sensitivity to InfoSec operations is positively related to InfoSec mindfulness.

H4: Commitment to resilience from InfoSec attacks is positively related to InfoSec mindfulness.

Proactive Extra-Role Information Security Behaviors (ISBs)

InfoSec behavioral research has distinguished desirable employees' ISBs as *in-role ISBs* and *extra-role ISBs*, which are mainly differ in whether behaviors go beyond an organization's ISP and employees' work role (Hsu et al. 2015; Turel et al. 2020). For example, ISPs compliance is an in-role behavior because it describes what employees should be doing within their work roles and responsibilities (D'Arcy and Lowry 2019; Herath and Rao 2009). By contrast, extra-role ISBs can be engaged without being motivated by any rewards or punishments of an ISP (Hsu et al. 2015). It can be manifested as a voluntary action that help others prevent security violations (i.e., helping) and an initiate intent to improve current organizational InfoSec (i.e., voicing) (Hsu et al. 2015).

Proactive behavior refers to a self-initiated and future-oriented action aiming to change and improve the situation or oneself (Crant 2000). It is classified by *proactive idea implementation*, which involves "an individual taking charge of an idea for improving the workplace, either by voicing the idea to others or by self-implementing the idea" (p. 637), and *proactive problem solving*, which refers to a self-starting and future-oriented action to prevent the reoccurrence of a problem or solving it in an unusual and nonstandard way (Parker et al. 2006). Prior studies examined several antecedents of proactive behavior, which are manifested by individual differences (including role breadth self-efficacy, proactive personality and job involvement) and contextual factors (such as job anonymous, management support and organizational culture) (Axtell and Parker 2003; Crant 2000; Frese and Fay 2001; Parker et al. 2006). Notably, Parker et al. (2006) revealed that proactive behavior is not confined to a particular contextual domain only. In the InfoSec context, Lin and Wittmer (2017) conceptualized proactive ISBs and linked it to individual creativity, group culture and decentralized IT governance. However, their research did not identify proactive ISBs separately from the idea-implementation and problem-solving dimensions and more potential factors that can influence proactive ISBs from the two dimensions deserve further investigations.

In addition, our literature review reveals that there exists conceptual overlap between extra-role ISBs and proactive ISBs in IS literature. On one hand, both in-role and extra-role behaviors can also be proactive, as proactive behaviors are identified by whether an employee "anticipates, plans for, and attempts to create a future outcome" (Grant & Ashford, 2008, p. 9). On the other hand, extra-role ISBs can be proactive or non-proactive (Abawajy 2014; Chen and Li 2019; Hsu et al. 2015; Li et al. 2017). For instance, Hsu et al. (2015) found that extra-role ISBs can also be motivated by formal control (such as specification, evaluation and reward) when interacting with social control (such as involvement, attachment, belief, and commitment), thus, these are not proactive. In this paper, we choose to focus on *proactive extra-role ISBs*, which have both characteristics of proactive and extra-role ISBs (i.e., 1) self-initiated and future-oriented and 2) without being motivated by rewards or punishments). Considering it is an increasingly important yet little-studied form of ISBs in InfoSec literature, we believe that identifying proactive extra-role ISBs theoretically and examining its motivational factors can deepen our understanding of employees ISBs from a more detailed perspective for InfoSec research.

Based on two types of proactive behaviors, we manifest proactive extra-role ISBs as *idea-implementation-oriented ISBs* (e.g., an employee implements a new idea or method for improving the rules of an ISP or refining systems) and *problem-solving-oriented ISBs* (e.g., an employee initiatively take charge of preventing security risks or addressing accidental security attacks). Employees who have an InfoSec mindfulness trait hold ongoing scrutiny of organizational InfoSec countermeasures. They are more likely to be able to identify the inappropriate parts of organizational ISPs or the vulnerability of a system (Hsu et

al. 2015). Therefore, we argue that the InfoSec mindful employees are able to initiate new ideas or methods to help improve organizational ISPs and information systems based on their accumulations of experience while handling with organizational information assets. On the other hand, InfoSec mindful employees also have an enriched awareness of organizational InfoSec practices and are sensitive to potential security attacks, hence, they tend to be good at addressing accidental security attack proactively when it happens or taking proactive measures to prevent future threats. As such, we believe that InfoSec mindfulness can lead employees to proactively react to current and future organizational InfoSec situation. Overall, we argue that InfoSec mindfulness can contribute to employees' proactive extra-role ISBs, manifested by positively influencing employees' idea-implementation-oriented ISBs and problem-solving-oriented ISBs. We propose our hypotheses as follows and the research model is shown in the Figure 1.

H5: InfoSec mindfulness will be positively associated with employees' idea-implementation-oriented proactive extra-role ISBs.

H6: InfoSec mindfulness will be positively associated with employees' problem-solving-oriented proactive extra-role ISBs.

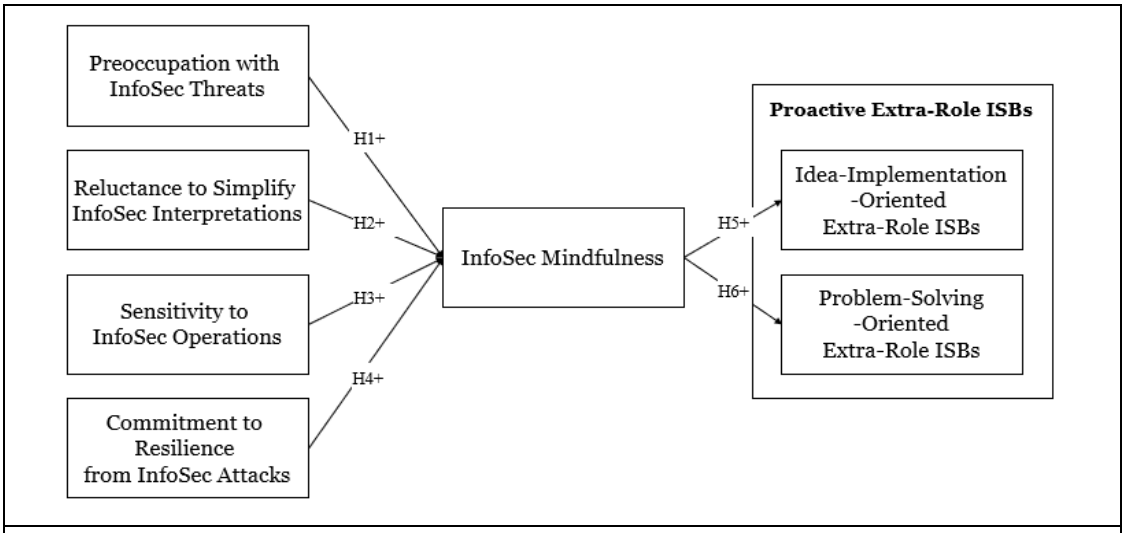

Figure 1. Research Model

Research Methodology

Our research design will include two sequential phases with the quantitative methodology. In the first phase, we aim to generate items of our InfoSec mindfulness scale and evaluate its validity and reliability through a pilot test. At the second phase, we will initiate our formal questionnaire through an online survey and test the hypothesized relationships in our research model.

Phase 1: InfoSec Mindfulness Scale Development and Validation

We will generate the items of our InfoSec mindfulness scale following a multistep procedure (Churchill 1979). First, based on Langer's archetypal mindfulness measurements and the other scales in InfoSec research (i.e. mindfulness in IT adoption scale (Sun et al. 2016) and IT mindfulness scale (Thatcher et al. 2018)), we will develop the items of InfoSec mindfulness by specifying InfoSec domain and include those items with slight differences in the meanings of the statements. To ensure content validity, we will develop several new items based on thoroughly reviewing the mindfulness literature to ensure all the categories of the construct are covered. And then, a card-sorting procedure (Moore and Benbasat 1991) will be conducted to map items to the categories and refine or delete some items to improve clarity. Second, we will conduct a pilot test to evaluate the reliability and validity of our InfoSec mindfulness scale. According to the results, we will modify and confirm the final measurements.

Following the same items development procedure, in terms of the antecedents of InfoSec mindfulness in our model, we will develop the items of these constructs based on the work from Carlo et al. (2012), which identified indicators for the dialectic of Weick and his colleagues' mindfulness processes (1999, 2001). The measurements of proactive extra-role ISBs will be adapted from measurements of proactive behaviors from Parker et al. (2006) and measurements of extra-role ISBs from Hsu et al. (2015). Eventually, we will conduct a pretest to examine the reliability, content, discriminant and convergent validity of the items of all the constructs.

Phase 2: Theoretical Hypotheses Testing

In phase 2, we will collect the data by surveying full-time employees across various industries, such as information technology, banking and finance, consulting, education, manufacturing and others, where the issue of information security has been highlighted. Respondents will be given points-based incentives for their participation. All respondents will be assured that their answers would remain confidential and be used for research purpose only. Besides questions which contain measurements of the constructs in our model, participants will also be asked about demographic information, including gender, age, education level and tenure within their organization. In addition, we will also use both a marker variable technique during our questionnaire design (Lindell and Whitney 2001) and a single-method factor analysis (Podsakoff et al. 2003) to reduce common method variance (CMV) and improve the quality of our data. The hypotheses testing will use the confirmatory factor analysis (CFA) via AMOS version 28.0.

Conclusion, Expected Contributions and Further Research

This paper first conceptualizes InfoSec mindfulness in InfoSec behavioral literature and plans to empirically examine the factors that contribute to InfoSec mindfulness and the effects of InfoSec mindfulness on employees' proactive extra-role ISBs. We expect to make contributions to InfoSec literature in three main aspects. First, our research first theorizes InfoSec mindfulness as a dynamic InfoSec-specific trait within InfoSec context, and also articulates the motivational effects of preoccupation with InfoSec threats, reluctance to simplify InfoSec interpretations, sensitivity to InfoSec operations, and commitment to resilience from InfoSec attacks on InfoSec mindfulness. Second, we plan to develop and validate the scale of InfoSec mindfulness. We hope that this would be beneficial to encourage more InfoSec studies to empirically test the role of InfoSec mindfulness in various types of individuals' ISBs. Third, our study complements the existing behavioral InfoSec research by focusing on proactive extra-role ISBs and examining the motivational role InfoSec mindfulness played in both idea-implementation and problem-solving extra-role ISBs. This can also contribute to managerial practices for organizations to improve organizational InfoSec by stimulating employees' InfoSec mindfulness and encouraging their engagement in proactive extra-role ISBs.

References

Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods," Behaviour & information technology (33:3), pp. 237-248.

Axtell, C. M., and Parker, S. K. 2003. "Promoting Role Breadth Self-Efficacy through Involvement, Work Redesign and Training," Human relations (New York) (56:1), pp. 113-131.

Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., Segal, Z. V., Abbey, S., Speca, M., Velting, D., and Devins, G. 2004. "Mindfulness: A Proposed Operational Definition," Clinical psychology (New York, N.Y.) (11:3), pp. 230-241.

Butler, B. S., and Gray, P. H. 2006. "Reliability, Mindfulness, and Information Systems," MIS quarterly (30:2), pp. 211-224.

Carlo, J. L., Lyytinen, K., and Boland Jr, R. J. 2012. "Dialectics of Collective Minding: Contradictory Appropriations of Information Technology in a High-Risk Project," MIS quarterly (36:4), pp. 1081-1108.

Chen, H., and Li, W. 2019. "Understanding Commitment and Apathy in Is Security Extra-Role Behavior from a Person-Organization Fit Perspective," Behaviour & information technology (38:5), pp. 454-468.

Churchill, G. A. 1979. "A Paradigm for Developing Better Measures of Marketing Constructs," Journal of marketing research (16:1), pp. 64-73.

Crant, J. M. 2000. "Proactive Behavior in Organizations," Journal of Management (26:3), pp. 435-462.

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 (Oxford, England) (29:1), pp. 43-69.

Davis, J. M., and Yi, M. Y. 2012. "User Disposition and Extent of Web Utilization: A Trait Hierarchy Approach," International journal of human-computer studies (70:5), pp. 346-363.

Feather, N. 2020. "How to Practice Cybersecurity Mindfulness for Your Business," avaliable at: https://www.inc.com/neill-feather/how-to-practice-cybersecurity-mindfulness-for-your-business.html.

Fichman, R. 2004. "Going Beyond the Dominant Paradigm for Information Technology Innovation Research: Emerging Concepts and Methods," Journal of the Association for Information Systems (5:8), pp. 314-355.

Fiol, C. M., and O'Connor, E. J. 2003. "Waking Up! Mindfulness in the Face of Bandwagons," The Academy of Management Review (28:1), p. 54.

Frese, M., and Fay, D. 2001. "Personal Initiative: An Active Performance Concept for Work in the 21st Century," Research in organizational behavior (23), pp. 133-187.

Grant, A. M., and Ashford, S. J. 2008. "The Dynamics of Proactivity at Work," Research in organizational behavior (28), pp. 3-34.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," European journal of information systems (18:2), pp. 106-125.

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

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," Journal of Management Information Systems (34:2), pp. 597-626.

Langer, E., Heffernan, D., and Kiester, M. 1988. "Reducing Burnout in an Institutional Setting: An Experimental Investigation," Unpublished manuscript, Harvard University, Cambridge, MA).

Langer, E., and Moldoveanu, M. 2000. "The Construct of Mindfulness," Journal of Social Issues (56), pp. 1-9.

Langer, E. J. 1989. Mindfulness. Reading, Mass: Addison-Wesley Pub. Co.

Langer, E. J. 1997. The Power of Mindful Learning. Reading, Mass: Addison-Wesley.

Langer, E. J. 2000. "Mindful Learning," Current Directions in Psychological Science (9:6), pp. 220-223.

Levinthal, D., and Rerup, C. 2006. "Crossing an Apparent Chasm: Bridging Mindful and Less-Mindful Perspectives on Organizational Learning," Organization science (Providence, R.I.) (17:4), pp. 502-513.

Li, Y., Stafford, T., Fuller, B., and Ellis, S. 2017. "Beyond Compliance: Empowering Employees' Extra-Role Security Behaviors in Dynamic Environments ". The 23rd Americas conference on information systems, 2017, Boston, MA, USA.

Lin, C., and Wittmer, J. L. S. 2017. "Proactive Information Security Behavior and Individual Creativity: Effects of Group Culture and Decentralized It Governance," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1-6.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," Journal of applied psychology (86:1), pp. 114-121.

Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," Information systems research (2:3), pp. 192-222.

Mukherjee, A. 2022. "Proactive Cybersecurity-What Is It, and Why You Need It." available at: https://www.threatintelligence.com/blog/what-is-proactive-cybersecurity.

NCSAM. 2021. "Cybersecurity Awareness Month 2021 Results Report." available at: https://staysafeonline.org/programs/about-cybersecurity-awareness-month/.

Parker, S. K., Williams, H. M., and Turner, N. 2006. "Modeling the Antecedents of Proactive Behavior at Work," Journal of applied psychology (91:3), pp. 636-652.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," Journal of applied psychology (88:5), pp. 879-903.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," MIS Quarterly (34:4), pp. 757-778.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," Information management & computer security (8:1), pp. 31-41.

Sun, H., Fang, Y., and Zou, H. M. 2016. "Choosing a Fit Technology: Understanding Mindfulness in Technology Adoption and Continuance," Journal of the Association for Information Systems (17:6), pp. 377-412.
Swanson, E. B., and Ramiller, N. C. 2004. "Innovating Mindfully with Information Technology," MIS quarterly (28:4), pp. 553-583.
Thatcher, J. B., Wright, R. T., Sun, H., Zagenczyk, T. J., and Klein, R. 2018. "Mindfulness in Information Technology Use: Definitions, Distinctions, and a New Measure," MIS Q. (42:3), pp. 831–848.
Turel, O., Xu, Z., and Guo, K. 2020. "Organizational Citizenship Behavior Regarding Security: Leadership Approach Perspective," The Journal of computer information systems (60:1), pp. 61-75.
Wallace, B. A. 1999. "The Buddhist Tradition of Samatha: Methods for Refining and Examining Consciousness," Journal of consciousness studies (6:2-3), pp. 175-187.
Wallace, B. A. 2004. The Taboo of Subjectivity: Toward a New Science of Consciousness. Oxford University Press.
Warner, L. 2022. "Stopping Cybercrime with a Deep Breath: How Mindfulness Protects against Social Engineering Techniques," avaliable at: https://ampcreative.com/combat-cybercrime-and-phishing-with-mindfulness/ (accessed on February 25 2022).
Weick, K. E., and Sutcliffe, K. M. 2001. Managing the Unexpected: Assuring High Performance in an Age of Complexity. San Francisco, CA, US: Jossey-Bass.
Weick, K. E., and Sutcliffe, K. M. 2006. "Mindfulness and the Quality of Organizational Attention," Organization science (Providence, R.I.) (17:4), pp. 514-524.
Weick, K. E., Sutcliffe, K. M., and David, O. 1999. "Organizing for High Reliability: Processes of Collective Mindfulness," Research in Organizational Behavior (21), pp. 88-123.
Wong, C. W. Y., Lai, K.-h., and Teo, T. S. H. 2009. "Institutional Pressures and Mindful It Management: The Case of a Container Terminal in China," Information & Management (46:8), pp. 434-441.