Employees’ Compliance with ISP: A Socio-Technical Conceptual Model

Arman Falahati
McGill University
arman.falahati@mail.mcgill.ca

Liette Lapointe
McGill University
liette.lapointe@mcgill.ca

Anne Beaudry
Concordia University
anne.beaudry@concordia.ca

Abstract

Employees’ compliance with Information Systems Security Policies (ISP) is critical for protecting organizational data. Both the technical side and the social aspects of IT-use were shown to have significant influence on ISP-compliance. However, they have been mostly studied in isolation, despite the literature’s emphasis on the socio-technical nature of security. Also, while the technical side has been extensively explored, there is a scarcity of research on the social mechanisms that underlie ISP-compliance. Here, we aim at bridging the gap between the technical and social sides of compliance. We also build upon Social Impact Theory to provide a more nuanced understanding of the social influence on ISP-compliance. We suggest that transparency of use is associated with the three pivotal elements of social influence, namely, perceived strength, immediacy, and number of influencing sources, which trigger normative and informational forces towards compliance. The influence of organizational ISP-compliance culture is also discussed.

1. Introduction

The worldwide information security (InfoSec) market is forecasted to reach $170.4 billion in 2022. This comes as no surprise given the significant impacts that recent InfoSec breaches have had on individuals, organizations, and society [1]. Researchers have identified employees’ compliance with ISP as a critical determinant of organizational security [2], [3], [4]. Previous research also shows that the mere existence of an ISP in organizations does not necessarily translate into ISP-compliance [3], [5], [6]. In many organizations, the technical specifications of the work systems or the existing organizational routines fundamentally allow for both ISP-compliant and non-compliant use-behaviors. As a result, employees have the leeway to comply or not with ISP [3]. In this paper, we thus are addressing cases where the employees’ compliance with ISP is based on a meaningful level of volition and personal decision-making.

Prior studies have identified several factors that motivate and foster employees’ compliance with ISP in volitional contexts [2], [7], [8]. For example, it was shown that ISP-compliant behaviors can be promoted through employees’ perceived severity of penalties [9], policy awareness [10], and managerial support [11]. Similarly, the literature has emphasized the significance of social influence [12], [4] in this regard.

While the socio-technical nature of information technology (IT)-use [13], [14], security [15], and more specifically, ISP-compliance [16] calls for the simultaneous consideration of the social and technical sides of security, these two have been studied mostly in isolation [16], [17]. As Gwebu et al. [18, pp. 220] mentioned recently, “despite the significant advancements made in understanding the factors that drive employees’ compliance and non-compliance behaviors with information security policy, less is known about how different factors interact to impact such behaviors”.

In addition, many of the prior studies have either neglected the social mechanisms that underlie ISP-compliance [4] or remained limited to highly general and abstract concepts such as principle ethical climate [5] and subjective norms [7]. Therefore, there is still a need to pay closer attention to and provide a finer-grained understanding of the social side of security.

Hence, we seek to fill these gaps by answering the following general research question: *How do the technical aspect of IT and the social influence among users jointly influence ISP-compliance in organizations?* In this paper, we not only provide a finer-grained understanding of the social influence in ISP-compliance but also adopt a socio-technical perspective in an attempt to bridge the gap between the technical and the social sides of compliance.

Our review and synthesis of the literature present the current state of knowledge on both the social and the technical sides of ISP-compliance and guide our theoretical development. Our proposed conceptual model introduces a new category of ISP-compliance antecedents and suggests novel insights. Since research has also shown the importance of considering contextual factors such as the organizational security

URI: https://hdl.handle.net/10125/80180
978-0-9981331-5-7

culture when studying ISP compliance [19], in this paper, we also address the potential influence of the compliance culture of the organization. Our work also provides new avenues for future research to look at ISP-compliance from a socio-technical lens.

In this paper, we mainly focus on ISP-compliance. As such, our work does not seek to explain non- compliant use-behaviors, since non-compliance is not necessarily the flip side of compliance. Although research has shown that the relative influence of many antecedents stays consistent across both compliant and non-compliant behaviors [20], scholars such as Guo [21] contend that compliance and non-compliance are distinct behaviors, and thus, should be studied separately. For example, deterrence-based sanctions were shown to be strong predictors of compliance, but not necessarily of non-compliance [22].

2. Literature review

We reviewed 83 papers that focused on ISP compliance. In terms of review method, we followed [17]. In general, information system security refers to the protection of data and critical elements such as the software or hardware that use, store, and transmit information, against unauthorized access and use [23], [24]. A fundamental step towards ensuring security in organizations is developing appropriate ISPs and providing adequate training. ISP is a subset of organizational policies that explains specific and necessary security-related outlines, including but not limited to IT-use protocols and technical controls that aim at safeguarding organizational IT assets against security breaches [4], [25].

In the information system literature, security behaviors regard how employees use their organizational IT, security-wise [21]. More specifically, the term "security behavior" refers to those particular use behaviors that have certain security-related implications in terms of protecting or disregarding security. For example, turning off firewalls, disabling antiviruses, choosing hard-to-guess passwords, and following or neglecting access protocols when using the organizational network, are all examples of security-related behaviors.

2.1. ISP-compliance

ISP-compliance is defined as obeying the organizational ISP when utilizing the organizational IT [26], [27]. Based on our synthesis of the literature, we realized that the employees' decision to comply with ISP is shaped through a heuristic process that embeds three steps. First, the employe needs to acquire adequate awareness of the ISP and the associated use-behaviors via either of the personal, social, and organizational sources [28].

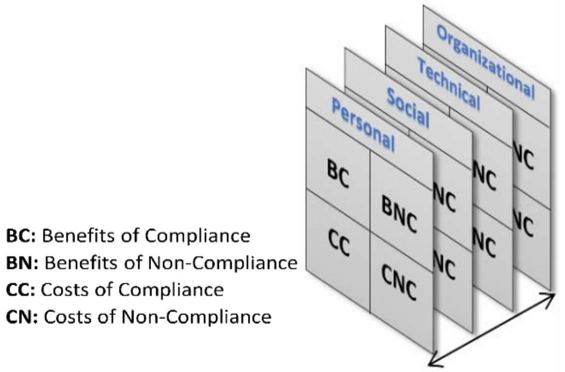

Organizational
Technical
Social
Personal
BC
BNC
CC
CNC
NC
NC
NC
NC
NC
NC
BC: Benefits of Compliance
BN: Benefits of Non-Compliance
CC: Costs of Compliance
CN: Costs of Non-Compliance

Figure 1. Sixteen points of cost-benefit evaluation

Second, and as presented in Figure 1, the decision to comply with ISP is shaped through the employee's evaluation of the costs and benefits of both compliance and non-compliance. The costs and benefits can be perceived as either personal and ethics-driven [5], [26], social and norm-driven [25], technical and design-driven [29], or related to organizational factors [30]. In addition, the evaluation regards both the significance and the probability of the costs and benefits in each case [9], [31], [32], [33], [34].

Third, the user needs to make sure that s/he fundamentally has the needed capabilities to comply with the ISP. The capability is not only associated with the users' ISP-related experience and awareness [35] but also embeds their security-related self-competency [25]. Following Bulgurcu et al. [26], we call this decision-making criterion perceived compliance self-efficacy.

A closer look into these three steps reveals that there is a social element embedded in most of them. For example, some are fundamentally based on the information cues provided by other users. Many also embed technical elements. For example, when evaluating costs of compliance at the technical level, several design-related factors were mentioned to be influential. In light of our research goals, we synthesized and summarized the literature on the social and technical aspects that have been shown to be influential on ISP compliance.

2.2. Social aspects of ISP-compliance

The social aspects of IT-use are known to have significant influence on how information systems are appropriated, specifically in the security context [36], [37]. Factors that are related to the social aspects of ISP-compliance mainly explain how employees influence their peers' compliance. In general, social influence is defined as an individual's feelings, thoughts, or behaviors being influenced by the real, implied, or imagined presence or actions of others [38], [39]. Specific to the context of ISP-compliance, two main groups of social influence are identified in the literature: normative and informational. While we acknowledge that other sources of influence may exist, the literature widely emphasizes the influence of colleague users [40].

2.2.1. Normative social influence. Normative social influence drives the user towards particular security behaviors by leveraging norm-centric social compliance or ethic-centric self-maintenance mechanisms [41], [42], [43]. Normative social influence is rooted in the user's inherent psychological needs, such as the need for attachment to peers [30] and self-approval [44]. Our review of the literature shows that this social influence can be of two kinds: influence on a user's personally accepted and internalized norms [5] and influence on a user's personally respected but not necessarily internalized norms [25].

2.2.2. Informational social influence. Informational social influence addresses the flow of knowledge and expertise among users [45] that informs, enables, and motivates an employee to perform or avoid particular security behaviors [43], [46]. Informational social influence takes place when people are influenced by other people's knowledge, expertise, and evidence [47]. The literature indicates that informational social influence can be of different kinds, including the influence on an employee's ISP awareness, ISP know-how [48], perception of ISP-legitimacy [34], understanding of compliance-related organizational rewards, non-compliance organizational penalties [33], and potential security threats [10].

2.3. Technical aspects of ISP-compliance

An important stream of research in information systems deals with the technical aspects of IT and has provided important insights into security. For example, it tries to produce new knowledge through the construction, technical manipulation, and evaluation of IT artifacts [49]. Research also involves the analysis of alternative designed artifacts to help understand and improve the users' behavior [50]. Here, the term "artifact" refers to a wide variety of concepts ranging from IT development methods, tools, techniques [51], and software, to use-processes, technical organizational interventions and methodologies that aim to enhance IT-use and organizational performance [49], [52].

Specific to security, prior research aims at creating, suggesting, and testing technological-engineering alternatives, and combining standards and procedures with particular configurations or maintenances of a system [27] to safeguard confidentiality, integrity, and availability of data [53]. Through our review of the literature, we identified three main types of technical approaches to enhancing ISP-compliance.

2.3.1. Restricting non-compliant use behaviors by adjusting security architecture. Researchers have suggested that organizations can enforce ISP-compliance by developing systems [or sub-systems] in a way that exclusively allows for compliant use. For example, specific technological alternatives were suggested for restricting employees' access to the organizational network [54] and data [55]. Similarly, research has suggested technical solutions for safeguarding the employees' access to outsourced and cloud services [56], [57] by using system designs that force a user to go through specific safety steps. In brief, it was shown that some technical designs are more effective in enforcing compliance. This category of solutions is not within the scope of our research as it does not embed volition and decision-making in the users' compliance with ISP.

2.3.2. Increasing the ease of secure use. A focal point of research in the technical side of security is enhancing ISP-compliance either by carefully directing the affordances of the system towards compliant use [58] or by lowering the user's needed information processing load for realizing compliant and non-compliant use and then, following the compliant ones [59]. For example, research has been dedicated to finding user-friendly and easy-to-understand interfaces that foster security [60]. In general, it was shown that there are particular system designs that make it simpler for the user to comprehend and adopt the compliant use behaviors. This category of solutions is also not within the boundaries of our paper as it mainly addresses individual-level factors in user-computer interactions, while our work addresses the social influence on ISP-compliance.

2.3.3. Keeping employees' use under surveillance by leveraging technical features. This type of control mechanism was also shown to have positive influence on ISP-compliance among employees [61]. One of the most widely implemented mechanisms in this regard is monitoring the user's use of the system. However, traditional monitoring mechanisms do have certain limitations, costs, and unwanted side effects [62], [63]. For example, the users may see it as a sign of mistrust and be offended. Others may find it as a serious cause of unnecessary stress at work [64].

Accordingly, research has suggested auditing as a more respectful and less stressful control mechanism. As explained by Jeon and Hovav [65], monitoring is the systematic process of tracking, watching, and recording the details of an employee's use, while auditing is the evaluation of an employee's use based on particular visible output. Clearly, the kernel of such control mechanisms is providing the knowledge of *who is doing what*, which we define in this research as transparency of use.

Research has also shown that the surveillance-based control mechanisms are only effective in promoting compliance when their existence is visible to the user [66]. This visibility is enabled via some levels of transparency in the systems, so the users will realize that their use-behaviors could be seen by others. Specific to security-related matters, Lindley [67] describes transparency as a tool of security regimes. Similarly, and as a key technical attribute of IS, being able to provide the knowledge of *who is doing what* was shown to be influential in directing security behaviors [68]. In addition, it was shown that when such transparency enables the accurate identification of the users at a given point of time, it helps to decrease insider non-compliant use [69]. Transparency of use is particularly relevant to our study as it has the potential to trigger security-related social influence among users.

3. Towards a socio-technical theory of ISP-compliance

The term socio-technical was originally developed based on the idea that in designing and implementing new work systems, providing a high-quality and satisfying work environment for employees is as important as the technological matters [70]. The idea of considering both the technical and human sides was then applied to different areas of information system research. Specific to security, it was shown that to protect organizational security, it is critical to understand the relationships between the technical aspects of IT and the human aspects of the users [71].

In the following section, we borrow insights from this perspective and suggest a new theoretical approach towards studying ISP-compliance. In this theoretical development, we address both the technical and social sides of security and show how a technical attribute of IT interacts with social mechanisms to enhance compliance. Next, we will explain in detail the two building blocks of our conceptual model: "Social Impact Theory" and "transparency of use".

3.1. Social side – Social Impact Theory

We build upon Social Impact Theory (SIT) [38] to provide a finer-grained understanding of the social influence on ISP-compliance. SIT provides a helpful framework for understanding how individuals are influenced by their social environment [39]. It suggests that individuals can be sources and targets of social influence. In this paper, we see the target of influence as an employee user, while the sources of influence are his/her colleagues. SIT states that an individual's feelings, attitudes, and behaviors can be affected by the presence of others. SIT also states that the intensity of the social influence on a target of influence depends on three pivotal attributes of the sources of influence: strength, immediacy, and number [38], [72].

Strength refers to the importance, salience, intensity, or social position of the sources of influence [42], [72]. Therefore, perceived *strength of the sources of influence* can be defined as the employee users' overall understanding of the importance, salience, intensity, or social position of their colleagues.

Immediacy refers to the temporal, social, or physical closeness between sources of influence and a target [42], [72]. Immediacy is usually perceived in the form of psychological closeness/distance [73], which is defined as one's perception that something or someone is close or far from the self [43], [73] either temporally, socially, or physically.

Last, *number* refers to the quantity of the sources of influence directed towards an individual target of influence [38], [42], [72]. In this study, we define the perceived number of the sources of influence as the employee user's understanding of the quantity of his/her colleagues.

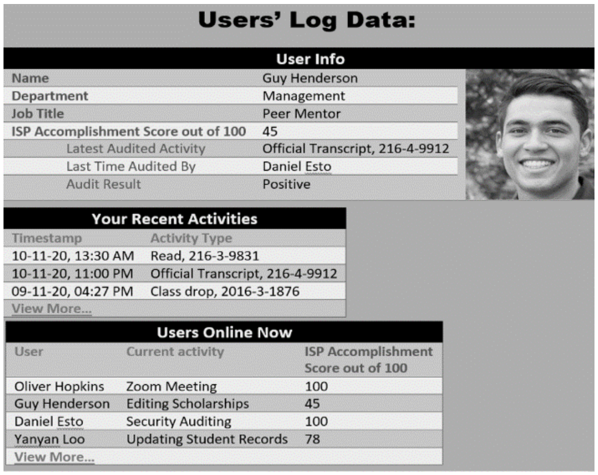
Previous research has shown how SIT can be used to explain users' intentions and behaviors, such as the visit and purchase intentions of eCommerce users [42] and the users' interactions in Facebook fan pages [72]. However, and despite its direct relevance for explaining security behaviors, to the best of our knowledge, no study to date has explicitly adopted this theoretical lens to study ISP-compliance.

3.2. Technical side – Transparency of use

In this paper, we also address the technical side of ISP-compliance and borrow insights from Vance et al. [68] to theorize how transparency of use, which is a technical design-oriented attribute, can trigger social influence on an employee user. *Transparency of use* is known to be one of the most important attributes of IT in terms of influencing the user's use-behaviors in general [74] and security behaviors in particular [68]. In the literature, transparency refers to the quality of having information open to others [75].

In this paper, we define transparency of use as an employee's perception of the degree to which the organizational IT allows to see who uses the system, how and for what purposes. To better clarify what details could become visible to the employees as a matter of higher transparency, we provide a sample interface in Figure 2.

For the sake of clarity and precision, we define two types of transparency in this research. *Inbound transparency* refers to the quality that allows one's colleagues to see his/her use-behaviors. In contrast, *outbound transparency* refers to the quality that allows



Users' Log Data:

User Info

Name	Guy Henderson
Department	Management
Job Title	Peer Mentor
ISP Accomplishment Score out of 100	45
Latest Audited Activity	Official Transcript, 216-4-9912
Last Time Audited By	Daniel Esto
Audit Result	Positive

Your Recent Activities

Timestamp	Activity Type
10-11-20, 13:30 AM	Read, 216-3-9831
10-11-20, 11:00 PM	Official Transcript, 216-4-9912
09-11-20, 04:27 PM	Class drop, 2016-3-1876
View More...	

Users Online Now

User	Current activity	ISP Accomplishment Score out of 100
Oliver Hopkins	Zoom Meeting	100
Guy Henderson	Editing Scholarships	45
Daniel Esto	Security Auditing	100
Yanyan Loo	Updating Student Records	78
View More...		

Figure 2: A sample interface for higher transparency

a user to see his/her colleagues' use-behaviors. For example, in Figure 2, the tab "Users Online Now" enables the user Guy Henderson to see what his colleagues are doing. This enables outbound transparency. The fields "Latest Audited Activity" and "Last Time Audited by" show him that there are other users who are able to audit his use. Such fields enable inbound transparency.

3.3. Conceptual model

In this section, we propose a model (Figure 3) that first depicts the relationships between *normative* and *informational* social influence and a user's compliance with ISP. In this model, ISP compliance is defined as the degree to which a user abides by the organizational ISP when utilizing organizational IS. Then, we propose that the three abovementioned elements in social impact, perceived *strength*, *immediacy*, and *number* of the sources of influence, are associated with normative and informational social influence. Lastly, we delve into the relationships between *transparency of use*, and perceived strength, immediacy, and number.

3.3.1. Informational/normative social influence & ISP-compliance. Informational and normative social influence were shown to have impacts on conformity behaviors in general [76], [42]. Specific to the organizational context, it has been shown that the normative social influence will be reflected in the individuals' attempts to comply with the expectations of other employees [8] in order to achieve rewards, avoid punishments [42] or maintain a positive self-image [2].

Similarly, the influence of security-related knowledge acquired from other users has been shown to have positive impacts on a user's compliance with ISP [77]. As detailed in the literature review section, the three steps towards a user's decision to comply with ISP are fundamentally information-based, many of which come from other users. As such, we argue that both informational and normative social influence can then influence a user's compliance with ISP.

3.3.2. The user's perceptions of the sources of influence & informational/normative social influence. SIT holds that the perceived *strength*, *immediacy*, and *number* of sources of influence determine the level of social influence that those sources will have on a target of influence [38].

In regard to informational social influence, research has shown that people ascribe more technical and behavioral legitimacy to those sources of influence who are seen as more important and influential [78]. Moreover, the higher salience of particular sources of influence can naturally increase the chances for their actions to be seen by others, and as a result, learned and replicated. It has also been stated that immediacy triggers collaboration in groups [79], which can, in turn, translate into the existence of more chances for security-related technical and informational exchange [80]. As explained above, technical and informational exchange are the foundations of informational social influence.

Also, a higher number of sources of influence, as perceived by a user, can facilitate the learning process [81] via triggering particular social practices such as security-help-seeking [82] and knowledge sharing [83]. Similarly, the higher number provides more opportunities for the user to draw inferences based on the observation of others' behaviors [84]. In brief, the higher number of sources of influence usually means the availability of more resources for acquiring particular security-related information.

In regard to normative social influence, it has been stated that the strength of a source of influence increases his/her normative influence on others [85]. There is also evidence to suggest that perceived immediacy of potential sources of influence creates a sense of closeness and, as a result, influences social persuasion [86]. Specific to online interactions, it has been shown that those who are psychologically perceived to be closer to an individual will have higher impacts on him/her [86]. In contrast, the higher temporal distance between sources of influence and a target of influence was shown to be associated with lower social influence [86].

Similarly, it has been shown that the number of group members influences the number of social interactions that take place among them [87]. Each inter-personal interaction can potentially be a source of social normative influence. In sum, the higher number of peer users usually means the availability of more sources for understanding use-related norms.

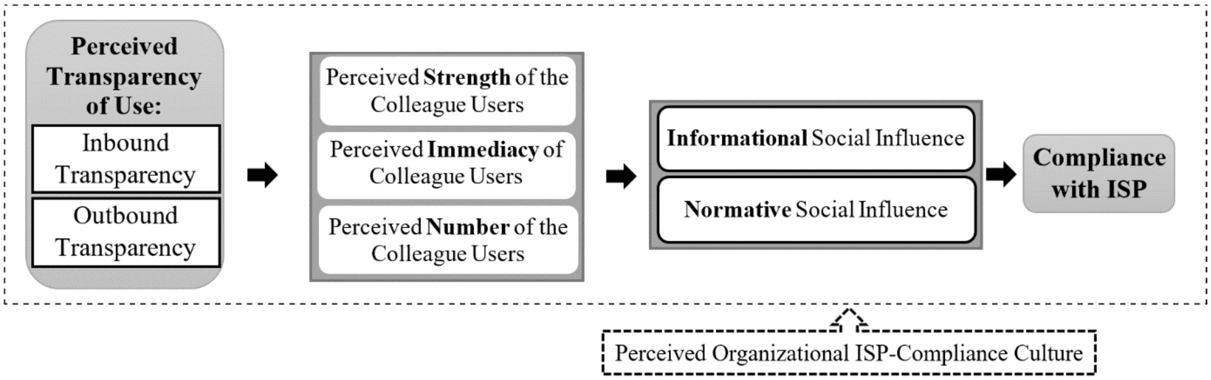

Perceived Transparency of Use:
Inbound Transparency
Outbound Transparency
Perceived Strength of the Colleague Users
Perceived Immediacy of Colleague Users
Perceived Number of the Colleague Users
Informational Social Influence
Normative Social Influence
Compliance with ISP
Perceived Organizational ISP-Compliance Culture

Figure 3: A socio-technical model of ISP compliance

Taken as a collective, we build upon SIT to suggest that there exist relationships between the three attributes of the sources of influence (strength, immediacy, and number), as perceived by the user, and the informational and normative social influence in regard to ISP-compliance.

3.3.3. Perceived transparency of use & the user's perceptions of the sources of influence. In general, transparency of use provides more visibility and information about other users. This enables the users to better audit each other's use and detect potential security-related misbehaviors. Transparency of use also highlights the presence of authorities in the surrounding environment, which influences their salience as perceived by the user [72]. As a result, perceived transparency of use can be associated with the user's perceived *strength* of the sources of influence. In addition, higher perceived transparency can increase the perceived temporal immediacy by providing faster feedback and reactions. Similarly, the higher awareness of other users that transparency provides can increase perceived psychological closeness or perceived immediacy of the colleagues. Finally, transparency can make users feel exposed to more users, each of whom may be seen as an important source of influence. All in all, we can argue that transparency of use, both inbound and outbound, can be associated with the three attributes of the sources of influence as perceived by the employee user.

3.3.4. ISP-compliance culture.

In general, security culture is known as the set of values, gradually shaped by employees, which determine how people are expected to think and behave regarding security, specifically when using organizational ITs [88], [89]. Accordingly, ISP-compliance culture can be seen as a sub-category of the overall security culture, which gives a particular meaning and value to complying (or not) with the ISPs, as perceived by the employees, and represents the employees' overall stance towards complying with ISP [89], [90]. In this sense, the ISP-compliance culture can range from positive, where compliance is mostly expected, followed, and respected, to negative, where compliance with ISPs is not a respected norm among employees but is rather seen as unnecessary.

To this point, we have been working under the assumption that the general organizational culture is supportive of compliance, and also, such ISP-compliant behaviors are expected and well-respected by the majority of users. However, there exist other situations where ISP-compliance culture is not positive. In the presence of a negative ISP-compliance culture, there will not be adequate motivation towards compliant behaviors since they are not perceived as expected and respected [63]. Besides, compliant use behaviors will probably not be reinforced by the peers and may rather be seen as antisocial and against-the-norms behaviors.

For example, in the presence of a negative ISP-compliance culture, the employees may receive particular information from their colleagues on how to circumvent complying with ISPs. They may also be normatively encouraged to avoid the ISPs, and thereby, be better aligned with and loyal to their group. In brief, we argue that *organizational ISP-compliance culture* can alter the relationships proposed above. A positive culture enables positive informational and normative influence, and as such, amplifies compliance. In contrast, a negative culture can enable negative informational and normative influence or at least hinder the positive influence, which in turn can diminish the employee's compliance.

4. Conclusion

Our literature review revealed that past research has addressed both the technical and the social sides of ISP-compliance. However, the potential relationships between these two sides are rarely explored. To bridge this gap, we aim to merge the knowledge about both the technical and the social sides of security in our theoretical development. As a result, we are suggesting a model that uses a socio-technical lens for studying ISP-compliance, which is closer to reality and better aligned with the nature of security [58].

In addition, many of the previous studies look at the social influence factors in ISP-compliance merely as an independent variable and do not explore their antecedents (e.g., [4], [25], [48], [80]). In this paper, in order to provide a more in-depth understanding of social influence, we are using Social Impact Theory to study ISP-compliance, and we adapt it to this particular context. Our conceptual model suggests that, in regard to ISP-compliance, the level of social influence is associated with the strength, immediacy, and number of influencing sources.

The information system security literature has also suggested several mechanisms, e.g., constant monitoring and sanctions, for increasing ISP-compliance within organizations. However, many of these mechanisms are described as obtrusive, time-consuming, and heavy-handed when applied in organizations [62], [68]. Moreover, they were shown to have inconsistent results in the workplace [22] and have important side-effects such as causing low morale among employees or motivating strikes and further misbehaviors in organizations [12], [68]. Given the increasing reliance of organizations on remote work conditions, the effectiveness of some traditional control mechanisms is more questionable than ever before.

We thus suggest moving beyond the traditional approaches to better understand ISP-compliance and to identify additional ways by which it can be fostered. In this paper, we introduced a less invasive intervention [68] for motivating ISP-compliance within organizations. In our proposed model, we suggested that particular technical attributes of information systems, here, transparency of use, can help to encourage ISP-compliance by triggering certain social mechanisms among users without overemphasizing formal and relatively harsh control mechanisms. In addition, we proposed a finer-grained understanding of transparency of use in the context of security by introducing the concepts of inbound and outbound transparency. This helps better delineate the specific outcomes that are associated with the disclosure of different types of use-related data.

Our review of the literature will help security-management practitioners to better grasp the current state of knowledge regarding ISP-compliance within organizations. Our theoretical development also emphasizes the need for considering the social aspects of IT-use as an essential part of security management programs together with technical considerations.

Further research will be needed to successfully direct and manage use behaviors. We hope that this paper will inspire further research on the socio-technical nature of ISP-compliance. For example, our conceptual model could serve as the basis of a research model to be tested and expanded in order to provide new insights in this regard. Moreover, future studies are invited to identify and explore other important technical factors and social mechanisms that interact to influence ISP-compliance within organizations.
Further research is also needed to check for the existence of a threshold in the level of transparency when higher transparency is proposed to be associated with higher security. This is important specifically when seeking an appropriate balance between security and privacy. There are cases where higher transparency endangers privacy [91], while in some other cases, transparency helps to maintain or enhance privacy [92], [93]. Last but not least, we recommend studying how organizational culture can be precisely tuned in order to foster positive security behaviors in organizations.

All in all, understanding the socio-technical triggers of ISP-compliance is critical for protecting security in organizations, and we hope that future studies will inform more effective mechanisms for motivating employees to comply.

5. References

[1] Sobers, J. R. "98 Must-Know Data Breach Statistics for 2021", Varonis, May 16, 2021. [Online]. Available: www.varonis.com/blog/data-breach-statistics/ [Accessed June 13, 2021].

[2] Moody, G., Siponen, M., Pahnila, S., “Toward a unified model of information security policy compliance”, MIS Quarterly, 2018. 42(1), pp. 285-A22.

[3] Palanisamy, R., Norman, A. A., & Kiah, M. L. M., “Compliance with Bring Your Own Device security policies in organizations: A systematic literature review”, Computers & Security, 2020. 98, pp. 101998.

[4] Yazdanmehr, A., Wang, J., & Yang, Z., “Peers matter: The moderating role of social influence on information security policy compliance”, Information Systems Journal, 2020. 30(5), pp. 791-844.

[5] Yazdanmehr, A., Wang, J., “Employees’ information security policy compliance: A norm activation perspective”, Decision Support Systems, 2016. 92, pp. 36-46.

[6] Li, H., Luo, R., & Chen. Y., “Understanding information security policy violation from a situational action perspective”, Journal of the Association for Information Systems, 2021. 22(3), pp. 739-772.

[7] Ifinedo, P., “Information systems security policy compliance: An empirical study of the effects of

socialization, influence, and cognition", Information & Management, 2014. 51(1), pp. 69-79.

[8] AlKalbani, A., Deng, H., & Kam, B., "The Influence of Organizational Enforcement on the Attitudes of Employees towards Information Security Compliance", Proceedings of the 10th International Conference on Information and Communication Systems, 2019. pp. 152-159.

[9] Siponen, M., Vance, A., "Neutralization: new insights into the problem of employee information systems security policy violations", MIS Quarterly, 2010. 34(3), pp. 487-502.

[10] Bélanger, F., Collignon, S., Enget, K., & Negangard, E., "Determinants of early conformance with information security policies", Information & Management, 2017. 54(7), pp. 887-901.

[11] Sharma, S., Warkentin, M., "Do I really belong?: Impact of employment status on information security policy compliance", Computers & Security, 2019. 87, pp. 101397.

[12] Lowry, P. B., Moody, G. D., "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies", Information Systems Journal, 2015. 25(5), pp. 433-463.

[13] Orlikowski, W. J., Scott, S. V., "Sociomateriality: challenging the separation of technology, work and organization", Academy of Management annals, 2008. 2(1), pp. 433-474.

[14] Benbya, H., Nan, N., Tanriverdi, H., & Yoo, Y., "Complexity and Information Systems Research in the Emerging Digital World", MIS Quarterly, 2020. 44(1), pp. 1-17.

[15] Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., & Surridge, M., "Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment", In Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, 2021. 3, pp. 266-274.

[16] Balozian, P., & Leidner, D., "Review of IS security policy compliance: Toward the building blocks of an IS security theory", ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 2017. 48(3), pp. 11-43.

[17] Falahati, A., Lapointe, L., "Compliance with IS Security-Policies: A Socio-Material Perspective Towards Security", In Proceedings of the Americas Conference on Information Systems (AMCIS), 2020. N. 9, pp. 1-11.

[18] Gwebu, K. L., Wang, J., & Hu, M. Y., "Information security policy non-compliance: An integrative social influence model", Information Systems Journal, 2020. 30(2), pp. 220-269.

[19] Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A., "Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance", Applied Sciences, 2021. 11(8), pp. 3383.

[20] Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J., "Variables influencing information security policy compliance", Information Management & Computer Security, 2014. 22(1), pp. 42-75.

[21] Guo, K. H., "Security-related behavior in using information systems in the workplace: A review and synthesis", Computers & Security, 2013 .32, pp. 242-251.

[22] D'Arcy, J., Herath, T., "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", European Journal of Information Systems, 2011. 20(6), pp. 643-658.

[23] Whitman, M. E., & Mattord, H. J., "Principles of information security", Boston, Ma, USA: Corse Technology, Cengage Learning, 2011.

[24] Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A., "The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth", International Journal of Contemporary Hospitality Management, 2012. 24(7), pp. 991-1010.

[25] D'Arcy, J., Lowry, P. B., "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study", Information Systems Journal, 2019. 29(1), pp. 43-69.

[26] Bulgurcu, B., Cavusoglu, H., & Benbasat, I., "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Quarterly, 2010. 34(3), pp. 523.

[27] Cram, W. A., Proudfoot, J. G., & D'Arcy, J., "Organizational information security policies: a review and research framework", European Journal of Information Systems, 2017. 26(6), pp. 605-641.

[28] Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J., "Building an awareness-centered information security policy compliance model", Industrial Management & Data Systems, 2019. 120(1), pp. 231-247.

[29] Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M., "Speak their language: Designing effective messages to improve employees' information security decision making", Decision Sciences, 2019. 50(2), pp. 245-284.

[30] Choi, M., Song, J., "Social control through deterrence on the compliance with information security policy", Soft Computing, 2018. 22(20), pp. 6765-6772.

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

[32] Aurigemma, S., "A composite framework for behavioral compliance with information security policies", Journal of Organizational and End User Computing, 2013. 25(3), pp. 32–5.

[33] Tsohou, A., Holtkamp, P., "Are users competent to comply with information security policies? An analysis of professional competence models", Information Technology & People, 2018. 31(5), pp. 1047-1068.

[34] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X., "Investigating the impact of cybersecurity policy

awareness on employees' cybersecurity behavior", International Journal of Information Management, 2019. 45, pp. 13-24.

[35] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C., "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", Computers & Security, 2014. 42, pp. 165-176.

[36] Yue, W. T., Wang, Q. H., & Hui, K. L., "See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums", MIS Quarterly, 2019. 43(1), pp. 73-95.

[37] Barton, K. A., Tejay, G., Lane, M., & Terrell, S., "Information system security commitment: A study of external influences on senior management", Computers & Security, 2016. 59, pp. 9-25.

[38] Latané, B., "The psychology of social impact", American Psychologist, 1981. 36(4), pp. 343-356.

[39] Chang, J. H., Zhu, Y. Q., Wang, S. H., & Li, Y. J., "Would you change your mind? An empirical study of social impact theory on Facebook", Telematics and Informatics", 2018. 35(1), pp. 282-292.

[40] Doherty, N. F., Tajuddin, S. T., "Towards a user-centric theory of value-driven information security compliance", Information Technology & People, 2018. 31 (2), pp. 348-367.

[41] Burnkrant, R. E., Cousineau, A., Informational and normative social influence in buyer behavior", Journal of Consumer Research, 1975. 2(3), pp. 206-215.

[42] Kwahk, K. Y., Ge, X., "The effects of social media on e-commerce: A perspective of social impact theory", Proceedings of the 45th Hawaii International Conference on System Sciences, 2012. pp. 1814-1823.

[43] Fu, J. S., Shumate, M., & Contractor, N., "Organizational and individual innovation decisions in an interorganizational system: Social influence and decision-making authority", Journal of Communication, 2020. 70(4), pp. 497-521.

[44] Cialdini, R. B., Goldstein, N. J., "Social influence: Compliance and conformity", Annual Review of Psychology, 2004. 55, pp. 591-621.

[45] Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M., "Deterrence and prevention-based model to mitigate information security insider threats in organizations" Future Generation Computer Systems, 2019. 97, pp. 587-597.

[46] Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A., "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, 2018. 19(8), pp. 689-715.

[47] Bearden, W. O., Netemeyer, R. G., & Teel, J. E., "Measurement of consumer susceptibility to interpersonal influence", Journal of Consumer Research, 1989. 15(4), pp. 473-481.

[48] Kim, S. S., Kim, Y. J., "The effect of compliance knowledge and compliance support systems on information security compliance behavior", Journal of Knowledge Management, 2017. 21(4), pp. 986-1010.

[49] Kuechler, W., Vaishnavi, V., "A framework for theory development in design science research: multiple perspectives", Journal of the Association for Information Systems, 2012. 13(6), pp. 396-423.

[50] Gregor, S., Hevner, A. R., "Introduction to the special issue on design science", Inf Syst E-Bus Manage, 2011. 9, pp. 1-9.

[51] Venable, J., "The role of theory and theorising in design science research" Proceedings of the 1st International Conference on Design Science in Information Systems and Technology, 2006. pp. 1-18.

[52] March, S. T., Storey, V. C., "Design science in the information systems discipline: an introduction to the special issue on design science research", MIS Quarterly, 2008. 32(4), pp. 725-730.

[53] Jahid, S., Nilizadeh, S., Mittal, P., Borisov, N., & Kapadia, A., "DECENT: A decentralized architecture for enforcing privacy in online social networks", Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops, 2012. pp. 326-332.

[54] Maes, S. H., U.S. Patent No. 8,688,813, Washington, DC: U.S. Patent and Trademark Office, 2014.

[55] Leventhal, J. C., Cummins, J. A., Schwartz, P. H., Martin, D. K., & Tierney, W. M., "Designing a system for patients controlling providers' access to their electronic health records: organizational and technical challenges". Journal of General Internal Medicine, 2015. 30(1), pp. 17-24.

[56] Wang, H., Yi, X., Bertino, E., & Sun, L., "Protecting outsourced data in cloud computing through access management", Concurrency and Computation: Practice and Experience, 2016. 28(3), pp. 600-615.

[57] Novkovic, G., Korkut, T., "Software and Data Regulatory Compliance in the Cloud", Software Quality Professional, 2017. 20(1), pp. 4-13.

[58] Van Slyke, C., & Belanger, F., "Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective", Computers & Security, 2020. 99, pp. 102064.

[59] Balfanz, D., Durfee, G., Smetters, D. K., & Grinter, R. E., "In search of usable security: Five lessons from the field", IEEE Security & Privacy, 2004. 2(5), pp. 19-24.

[60] Nwokedi, U. O., Onyimbo, B. A., & Rad, B. B., "Usability and security in user interface design: a systematic literature review", International Journal of Information Technology and Computer Science, 2016. 8(5), pp. 72-80.

[61] D'Arcy, J., Greene, G., "Security culture and the employment relationship as drivers of employees' security compliance", Information Management & Computer Security, 2014. 22(5), pp. 474-489.

[62] Jiang, H., Tsohou, A., Siponen, M., & Li, Y. "Examining the side effects of organizational Internet monitoring on employees", Internet Research, 2020. 30(6), pp. 1613-1630.

[63] Topa, I., Karyda, M., "Analyzing security behaviour determinants for enhancing ISP compliance and security management", Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS), 2016. pp. 1-13.

[64] Lee, C., Lee, C. C., & Kim, S., "Understanding information security stress: Focusing on the type of information security compliance activity", Computers & Security, 2016. 59, pp. 60-70.

[65] Jeon, S., Hovav, A., "Empowerment or control: Reconsidering employee security policy compliance in terms of authorization", Proceedings of the 48th Hawaii International Conference on System Sciences, 2015. pp. 3473-3482.

[66] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W., "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", European Journal of Information Systems, 2009. 18(2), pp. 151-164.

[67] Lindley, D., "Promoting peace with information: Transparency as a tool of security regimes", Princeton University Press, 2021.

[68] Vance, A., Lowry, P. B., & Eggett, D. L., "Increasing accountability through the user interface design artifacts: A new approach to addressing the problem of access-policy violations", MIS Quarterly, 2015. 39(2), pp. 345-366.

[69] Alotibi, G., Clarke, N., Fudong, L., & Furnell, S. "The feasibility of using behavioural profiling technique for mitigating insider threats", Computer Science & Information Technology, 2019. pp. 59-71.

[70] Mumford, E. "The story of socio-technical design: Reflections on its successes, failures and potential", Information systems journal, 2006. 16(4), pp. 317-342.

[71] Malatji, M., Von Solms, S., & Marnewick, A. "Socio-technical systems cybersecurity framework", Information & Computer Security, 2019. 27(2), pp. 233-272

[72] Perez-Vega, R., Waite, K., & O'Gorman, K., "Social impact theory: an examination of how immediacy operates as an influence upon social media interaction in Facebook fan pages", The Marketing Review, 2016. 16(3), pp. 299-321.

[73] Trope, Y., Liberman, N., "Construal-level theory of psychological distance", Psychological Review, 2010. 117(2), pp. 440-463.

[74] Leonardi, P. M., "Social media, knowledge sharing, and innovation: Toward a theory of communication visibility", Information Systems Research, 2014. 25(4), pp. 796-816.

[75] Cappelli, C., Cunha, H., Gonzalez-Baixauli, B., & do Prado Leite, J. C. S., "Transparency versus security: early analysis of antagonistic requirements", Proceedings of ACM symposium on applied computing, 2010. pp. 298-305.

[76] Deutsch, M., Gerard, H. B., "A study of normative and informational social influences upon individual judgment", The journal of abnormal and social psychology, 1955. 51(3), pp. 629-636.

[77] Stafford, T., Deitz, G., & Li, Y., "The role of internal audit and user training in information security policy compliance", Managerial Auditing Journal, 2018. 33(4), pp. 410-424.

[78] Mugny, G., Souchet, L., Codaccioni, C., & Quiamzade, A., "Social representations and social influence", Psychologie Francaise, 2008. 53(2), pp. 223-237.

[79] Woods, R. H., & Baker, J. D., "Interaction and immediacy in online learning", The International Review of Research in Open and Distributed Learning, 2004. 5(2), pp. 1-13.

[80] Safa, N. S., Von Solms, R., & Furnell, S., "Information security policy compliance model in organizations" computers & security, 2016. 56, pp. 70-82.

[81] Bose, M., Ye, L., "Cross-cultural perspective of situated learning and coping: understanding psychological closeness as mediator", Journal of Consumer Marketing, 2019. 37(1), pp. 10-20.

[82] Chen, Y., Zahedi, F. M., "Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China", MIS Quarterly, 2016. 40(1), pp. 205-222.

[83] Safa, N. S., & Von Solms, R., "An information security knowledge sharing model in organizations", Computers in Human Behavior, 2016. 57, pp. 442-451.

[84] Chu, S. C., Kim, Y., "Determinants of consumer engagement in electronic word-of-mouth (eWOM) in social networking sites", International Journal of Advertising, 2011. 30(1), pp. 47-75.

[85] Harkins, S. G., Latané, B., "Population and political participation: A social impact analysis of voter responsibility", Group Dynamics: Theory, Research, and Practice, 1998. 2(3), pp. 192-207.

[86] Miller, M. D., Brunner, C. C., "Social impact in technologically-mediated communication: An examination of online influence", Computers in Human Behavior, 2008. 24(6), pp. 2972-2991.

[87] Fay, N., Garrod, S., & Carletta, J., "Group discussion as interactive dialogue or as serial monologue: The influence of group size", Psychological science, 2000. 11(6), pp. 481-486.

[88] Schlienger, T., Teufel, S. "Information security culture", Security in the Information Society, 2002. 86, pp. 191-201.

[89] Wen, S. F., Kianpour, M., & Kowalski, S., "An empirical study of security culture in open-source software communities", Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2019. pp. 863-870.

[90] Otieno, E. O., Wausi, A. N., & Kahonge, A. M., "Exploring the Factors That Contribute Towards Information Security Policy Compliance Culture", Information and Knowledge Management, 2020. 10(5), pp. 39-49.

[91] Bernstein, E. S. "The transparency paradox: A role for privacy in organizational learning and operational control", Administrative Science Quarterly, 2012. 57(2), pp. 181-216.

[92] Seneviratne, O., Kagal, L., "Enabling privacy through transparency", Proceedings of IEEE International Conference on Privacy, Security and Trust, 2014. pp. 121-128.

[93] Belonick, P. "Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment", Stanford Technology Law Review, 2020. 23(1), pp. 114-181.