2015

Investigating the Formation of Information Security Climate Perceptions with Social Network Analysis: A Research Proposal

Duy Dang-Pham
RMIT University, duy.dang@rmit.edu.au

Siddhi Pittayachawan
RMIT University, siddhi.pittayachawan@rmit.edu.au

Vince Bruno
RMIT University, vince.bruno@rmit.edu.au

INVESTIGATING THE FORMATION OF INFORMATION SECURITY CLIMATE PERCEPTIONS WITH SOCIAL NETWORK ANALYSIS: A RESEARCH PROPOSAL

Duy Dang-Pham, School of Business IT and Logistics, RMIT University, Melbourne, Australia, duy.dang@rmit.edu.au

Siddhi Pittayachawan, School of Business IT and Logistics, RMIT University, Melbourne, Australia, siddhi.pittayachawan@rmit.edu.au

Vince Bruno, School of Business IT and Logistics, RMIT University, Melbourne, Australia, vince.bruno@rmit.edu.au

Abstract

Over the past years, a large amount of studies has advanced knowledge that explains how individuals react to information security cues and why they are motivated to perform secure practices. Nevertheless, those studies predominantly set their focus on the adoption of secure practices at an individual level; therefore they were unable to analyse such adoption at the higher level. As a consequence, the formation and dissemination processes of information security perceptions were overlooked despite their importance. Understanding those processes would inform methods to distribute effectively desirable information security perceptions within the workplace, while potentially explaining why in some cases implementation of information security measures was not successful at changing the employees' beliefs and behaviours. The first part of this paper reviews the concept of information security climate that emerge from the individual's interactions with the work environment, which has been under researched and investigated inconsistently. The second part begins with discussing the influence mechanisms that could disseminate information security climate perceptions, then suggests the adoption of social network analysis techniques to analyse those mechanisms. As a result, the paper forwards an integrated framework about information security climate perceptions, as well as proposes a research agenda for future investigations on how those perceptions could be formed and disseminated within the workplace.

Keywords: information security perception, information security climate, information security culture, information security management, social network analysis

1 INTRODUCTION

As information has always been regarded as a critical resource of organisational information systems over the last decades, the management of information's confidentiality, integrity and availability is no less vital. More importantly, effective information security management must address not only technological issues but also the socio-organisational factors including the human users. Consequently, it is important to understand how end users perceive and perform information security behaviours. An emerging number of studies have been investigating those perceptions and behaviours, consisting of how end users perceive and perform compliance (Herath and Rao 2009; Lee et al. 2008; Vance et al. 2012), proactive protection (Dang-Pham and Pittayachawan 2015; Liang and Xue 2010), as well as misbehaviours (Dang 2014; Siponen and Vance 2010). Nevertheless, there still exist certain limitations in the current body of knowledge, especially in information security behavioural field, that demand further investigations. The cognition and behaviours at the individual level have been predominantly studied despite information security is also about collective practices which characterise the interactions between employees (Dourish and Anderson 2006). For instance, delegations of trust and responsibility were found to occur in the workplace (Dourish et al. 2004). Most recently, Dang-Pham et al. (2014) argued that a majority of information security behavioural studies has been employing theories that focus on the individual's cognition and behaviours, thereby having their implications subject to satisfying the theoretical assumptions of these theories in practicality. As a result, these authors suggested investigating the phenomena at the collective level, particularly by analysing the interactions that exchange information about information security matters with social network analysis techniques.

The suggestion to investigate the interactions among individuals and their workplace subsequently links to the topic of information security climate, which is currently under researched and approached inconsistently despite their importance. For instance, gaining knowledge of such climate perceptions would inform how to develop information security environment and culture, especially when capturing and understanding organisational culture remains a daunting task to both internal and external members of the organisations (Lacey 2010). On the other hand, previous studies have determined the information security perceptions that could motivate compliant intention and actual secure behaviours, but little has been known regarding their formation and dissemination processes. We believe this knowledge gap could partly account for the unsuccessful implementations of information security, especially when all the training and resources have been delivered yet the employees fail to realise information security is prioritised in the workplace. While understanding how individuals react to information security cues and perform acceptable actions is crucial to designing measures and training programs, the same importance could be argued for investigating how to exploit those cues and measures to facilitate groups of information security-effective employees. This conceptual paper forwards a framework that describes information security climate perceptions, as well as their formation and dissemination processes.

2 INFORMATION SECURITY CLIMATE PERCEPTIONS

2.1 Valuations of information security-related workplace's attributes

The focal interest of this paper is about information security climate, or the individual's perceptions of information security matters that emerge from their interactions with the workplace's attributes. The seminal articles by James and colleagues (e.g. James and James 1989; James et al. 2008; Jones and James 1979) defined such perceptions as the individual's *valuation* of environmental attributes that result from their cognitive information processing. More importantly, valuation needs to be distinguished from descriptions that do not require much information processing such as observed technological complexity, formal regulations, and communication structures (James and James 1989). For example, co-worker socialisation could be observed as a *description* of the environment, but the friendliness of the workgroup is a *perceptual valuation*, or a climate perception, of such socialisation.

Currently there are few studies that examine information security climate perceptions. One of the first and widely cited studies investigated information security climate perceptions was by Chan et al. (2005). By comparing the similar natures, goals, and practices of workplace safety and information security, these researchers adapted the dimensions of safety climate to measure the construct of information security climate perceptions and determine its driving factors. These dimensions were included in their model as observed environment's descriptions. The climate perceptions being measured include the perceived standard of information security in the workplace, as well as how concerned the participants believed their management, supervisor, and co-workers would feel about information security. It is also worth emphasising that among these few studies about information security climate, only Chan et al. (2005) have explicitly separated the observed workplace's attributes from the climate perceptions. This helps to further clarify the descriptive and value-based meanings in the workplace as discussed by James and James (1989) and James et al. (2008).

Other research about information security climate perceptions includes the work of Jaafar and Ajis (2013) which employed the same three dimensions as Chan et al.'s (2005) study to measure a construct named "organisational climate" focusing on information security of the Malaysian Army. Unlike Chan et al. (2005), these authors posited direct impact of the workplace's descriptions on compliant behaviours rather than being mediated by climate perceptions. In this approach, the existence of the visible workplace's descriptions (e.g. observed management practices and co-workers socialisation) was emphasised rather than their perceived motivational meanings. Similarly, Goo et al. (2014) adapted the dimensions of safety climate to conceptualise information security climate as their focal construct. However, they neither clearly separated observed and perceived climate factors as done by Chan et al. (2005), nor tested for direct impacts on compliance like Jaafar and Ajis's (2013). Information security climate in their research was modelled as a mediating second-order construct formed by a mixture of perceptual and descriptive valuations of top management attention, security enforcement, awareness program, and policies. These valuations subsequently had their contributing effects tested on commitment, security avoidance, and compliant intention (Goo et al. 2014). In summary, the measurement items used in these two studies did not clearly distinguish between observable workplace's attributes (descriptions) and climate perceptions (valuations).

2.2 Climate perceptions from the information security culture's perspectives

It can be observed that the mentioned studies about information security climate perceptions commonly included factors that belong to the two core dimensions (i.e. leadership and workgroup) of molar (generic) psychological climate as described in the works of Jones and James (1979) and James et al. (2008). Nonetheless, the other generic dimensions such as job and role and organisational systems have not been included in the information security context. In fact, perception of job autonomy or work ownership is an important factor of organisational climate as viewed from both the generic (James et al. 2008; Jones and James 1979) and specific perspectives such as safety climate (Zohar 2008). Interestingly, some of those perceptions have been discussed in the literature about information security culture.

Organisational climate was regarded as a surfacing mean to gain deeper knowledge about the organisational culture (Härtel and Ashkanasy 2010). Information security culture has been analysed at four levels: artefacts (visible day-to-day behaviours), espoused values (formal values being promoted), shared tacit assumptions (underlying beliefs), and knowledge (Van Niekerk and Von Solms 2010; Da Veiga and Eloff 2010). In organisational climate's terms, it could be argued that the observed descriptions of the environment reflect what is measured at the artefact's level, whereas the valuations or climate perceptions would be the shared tacit assumptions as a result of the individual's information processing. Such matching relationship between climate and culture justifies the appropriateness of incorporating information security culture's factors into climate's model.

From the literature discussing information security culture, we found Ruighaver et al.'s (2007) Organisational Security Culture Model fits well with our research's theme because it elaborates the holistic four-level structure and describes in-depth the dimensions of security culture from the employee's perspective. The model includes eight dimensions describing the intertwined aspects at organisation, workgroup, and individual levels, which together develop an information security

culture. To begin with, the first dimension of Ruighaver et al.'s (2007) model suggests that the employees perceive the importance of information security by observing top management's actions that are consistent with what being stated. The second dimension looks at whether information security is strategically planned in long-term or ad-hoc mitigations, in which the prior exhibits top management's serious commitment thus yields the perception that information security is of higher importance (Ruighaver et al. 2007). Such perception is consistent with prior research about safety climate, which Chan et al. (2005) argued to share common traits with information security. For instance, perceived importance of safety has been emphasised repeatedly in this line of research (e.g. Kuenzi and Schminke, 2009; Zohar, 2010). Similarly, perceived importance of information security was included as an indicator of security awareness in Albrechtsen and Hovden's (2010) study.

The third dimension of Ruighaver et al.'s (2007) model discusses the use of rewards in making the employees feel motivated to adopt and reflect on secure practices. This perception takes into account the definition of organisational climate, which describes climate in the form of behaviours that are observed as being rewarded and supported (Schneider et al. 2013). On the other hand, the perceptions of being trusted by the top management and assigned responsibility to handle information security matters (Ruighaver et al. 2007) reflect the core dimensions of generic psychological climate. In particular, these dimensions examine the characteristics of job autonomy and supervisors' trust in subordinates' performance and judgement (Jones and James 1979). Perceived responsibility was also listed as an indicator of Albrechtsen and Hovden's (2010) information security awareness.

The perception that information security is accepted as a part of daily operations could evaluate its actual priority over competing goals such as productivity. This evaluation is consistent with safety climate literatures, and especially emphasised by Zohar (2008, p. 377) that the true priority of safety is the ultimate target of safety climate perceptions. Likewise, Ruighaver et al. (2007) suggest acknowledgement of ownership and accountability (third and seventh dimensions), perceived balance between security and work constraints (fifth dimension), and observed collaborative efforts between organisational units (sixth dimension) to be capable of influencing this perception of priority. In contrast, the measurements of information security climate by Chan et al., (2005) and other similar research only capture the perceived concerns of the participant, their co-workers and management, but none of them actually discerned the priority of information security in work context. Provided that information security is often found neglected in exchange for achieving other priorities in daily operations (e.g. Siponen and Vance, 2010), it would be worthy to measure its perceived priority.

2.3 Appraisals of information security threats and coping solutions

As the scope of this research looks at information security climate perceptions, it is also necessary to consult studies about the perceptions of information security *per se* besides those that were explicitly described by climate literature to emerge from the observable workplace's attributes in relation to information security matters. Huang et al. (2010) defines information security perception as the individual's evaluation of security threats that determines one's behaviours. These authors factorised six factors which affect and characterise perception of information security risks, including knowledge, impact, severity, controllability, awareness, and possibility of threats. These six factors form the KISCAP model of information security perceptions (Huang et al. 2010). Moreover, they resemble the factors in Protection Motivation Theory (PMT) (Rogers 1975) model which has been empirically tested and extended by several prior research (e.g. Dang-Pham and Pittayachawan, 2015; Herath and Rao, 2009; Vance et al., 2012). For instance, previous studies adopting PMT commonly found that the cognitive appraisals of the threats (including perceived severity, vulnerability, and rewards) and the coping solutions (including self-efficacy, response cost and efficacy) would impact individual's compliant intention. While some factors in these two models are similar (e.g. severity, possibility/vulnerability, controllability/response efficacy), PMT provides a theoretical background to formally extend that information security perceptions also include the evaluation of the coping solutions rather than the threats alone.

While these perceptions' impacts on intention to perform secure behaviours have been consistently supported by empirical research, they were often tested as independent factors that are postulated by PMT (e.g. Herath and Rao, 2009; Lee et al., 2008; Vance et al., 2012). Until recently, these models

integrated with factors of other theories (Herath et al. 2012) and had their inter-relationships tested (Dang-Pham and Pittayachawan 2015), which findings provided more implications. Furthermore, it may be reasonable to group these perceptions in the same category of climate perceptions. Climate perceptions were described as the valuations that emerge from processing of the observable environment's description. Similarly, PMT's "response efficacy" factor that assesses one's perceived effectiveness of the coping solutions is actually a perceptual valuation of the observed security measures being implemented at the workplace. Another example, "perceived vulnerability" could also be evoked from observable climate descriptions such as security omissions or risky behaviours.

In summary, we extracted and consolidated in Table 1 perceptions of workplace's descriptions from three research domains including information security climate, culture, and appraisals of threats and coping solutions. Among these, some factors appear to hold similar meanings but were named differently. In addition, a majority of factors in relation to the appraisals of leadership, workgroup, threats, and coping solutions were empirically assessed for impacts on intention to perform secure practices. On the other hand, perceptions of job and role, as well as those emerged from qualitative studies of information security culture still have their effects untested. Nonetheless, the list below is unable to cover all the important perceptions, provided that the area of information security climate perceptions is under researched.

Dimensions	**Information security climate perceptions**	**Elaborations**
Leadership	Information security goal emphasis	Employees perceive that top management and supervisor are committed to information security; visions and practices are consistent
	Top-down trust	Perceptions of being trusted by supervisors to handle information security matters
	Top management's supports	Employees perceive that top management's supports are available and responsive
Job & role	Information security importance	Employees perceive that secure behaviour and compliance make meaningful contribution to the organisation
	Information security responsibility	Employees perceive that they are responsible for security
	Information security's design efficiency	Perceptions of the balance or conflict between information security and other operations
Workgroup	Workgroup cooperation in information security	Perceptions of co-workers' active socialisation and genuine concerns about information security
	Consistent information security practices	Employees perceive that secure practices are accepted and prioritised consistently within business units and organisation
Organisational systems	Rewards for information security behaviour	Perceptions of information security behaviour being rewarded tangibly and intangibly (i.e. recognition) in the workplace
	Information security planning and effectiveness	Employees perceive that the implemented information security controls are effective in protecting information and at high standard

Table 1. Information security climate perceptions and dimensions

Previous studies have identified perceptions of information security-related workplace's attributes and determined their effects on intention to perform secure practices. However, we contend achieving that knowledge is only the initial step in the development of a secure workplace. To facilitate and maintain an information security environment, we need to understand how the perceptions of those descriptions would be brought about and disseminated among the employees. As a consequence, this involves identifying the formation and dissemination processes of information security climate perceptions.

3 THE FORMATION OF IS CLIMATE PERCEPTIONS

Social influence is argued to make individuals adopt the behaviours, beliefs, and attitudes of the surrounding others (Leenders 2002). Different types of social influence have been discussed by Cialdini and Goldstein (2004). Past studies have identified two core processes of social influence which include communication and comparison. Specifically, communication characterises the direct persuasion between two or more individuals that shapes their perceptions and behaviours. On the other hand, comparison takes place when one looks at peers, whose roles are similar, and acts accordingly as they establish their social identity (Burt 1987; Leenders 2002). These two processes have had their impacts on the changes of perceptions and behaviours tested as cohesion and structural equivalence, which were described respectively in Social Contagion Theory (SCT) by Burt (1987).

The theoretical constructs of communication and comparison, namely *cohesion* and *structural equivalence*, are included in many models of social network studies that analyse the connections and interactions of the network's actors. In particular, cohesion looks at the direct interactions among the individuals, whereas structural equivalence focuses on the similar position and communication patterns that individuals possess in the social networks (Burt 1987). A number of social network studies employed SCT has offered insightful findings about unethical behaviours (Brass et al. 1998), risk perceptions (Scherer and Cho 2003), and interpersonal trust (Ferrin et al. 2006). Similarly, information security is considered collective information practices that are based on morality, trust, and risk (Dourish and Anderson 2006). In addition, Dang-Pham et al. (2014) also suggested future studies to apply social network analysis techniques to investigate the diffusion of information security misbehaviours. As a consequence, it would be appropriate to include the concepts of cohesion and structural equivalence to study the formation of information security climate perceptions.

As a major component of the proposed framework, the influence mechanisms that contribute to the formation and dissemination of information security climate perceptions need to be specified. On one hand, the features of the social network and their effects on interpersonal influences have been established by empirical studies. For instance, Zohar and Tenne-Gazit (2008) found both densities of communication and friendship networks (i.e. how well-connected they are) to have significant impacts on safety climate strength. Moreover, Zohar (2010) called for future adoption of social network analysis techniques to investigate the sense-making processes related to organisational climate, but there is still a lack of climate researches that do so.

On the other hand, the types of employees' interactions and relationships (termed *ties* in social network analysis) in relation to their information security perceptions remain under researched. While there is not a definite list of ties in organisational context, relevant ties could be identified from the existing literatures. For example, delegating responsibility for information security was found as an interaction between end users in organisational context (Dourish et al. 2004). In such cases, it is possible that an individual's perception of security risk may be cohesively influenced by receiving direct delegation of responsibility to handle security matters from the others, or a group of people who often delegate security may have similar perception of risk as a result of their structural equivalence. Moreover, information security induction and training could be examined as exchanging advice.

Another source that can potentially provide influential interactions and relations is the literature in change management domain. When a new information security policy or process is introduced, it would change daily operations in different aspects. In that case, effective change management techniques are desired to achieve end user's acceptance of information security. The principles of successful change communication have been extensively researched. For example, in addition to workplace interactions, the formal and informal relations that are characterised by the actors' line and collegial authority (e.g. opinion leader) were argued to hold vital implications in implementing changes (e.g. Stiglitz and Fitoussi 1996). Nevertheless, Ibarra and Andrews (1993) found that it may depend on the firm's characteristics that instrumental (e.g. advice) and expressive (e.g. friendship) networks would have different predicting effects on work-related perceptions. As a result, the researchers must thoughtfully select to investigate the interactions that match with the employees' information security perceptions of interest, which some can be more related to work duty (e.g. perceived responsibility) or personal preferences (e.g. co-worker cooperation).

4 PROPOSED RESEARCH FRAMEWORK

By reviewing literatures about information security climate (Chan et al. 2005; Goo et al. 2014; Jaafar and Ajis 2013), culture (Ruighaver et al. 2007), and information security perceptions *per se* (e.g. Dang-Pham and Pittayachawan 2015; Herath and Rao 2009; Huang et al. 2010; Vance et al. 2012), we extracted and consolidated relevant perceptions of information security matters that reflect the valuations of workplace's descriptions. Nonetheless, very few studies to date have investigated the formation and dissemination processes of those climate perceptions. In other words, previous studies have identified the workplace's attributes that would yield desirable effects when being implemented, but they have yet to empirically determine the mechanisms to make use of these attributes and motivate collective compliant behaviours. The recent work of Dang-Pham et al. (2014) proposes adopting social network analysis techniques to analyse the dissemination of information security misbehaviour, but has yet discussed the theoretical foundations of such methodological approach.

This research also suggests adopting social network analysis techniques to examine the interactions that form and disseminate information security climate perceptions. Furthermore, we add Social Contagion Theory (Burt 1987) postulating two forms of social influence (i.e. cohesion and structural equivalence) that could serve as the mechanisms to explain the formation of information security climate perceptions. Furthermore, social network approach also suggests the structural attributes of social networks to have impacts on the dissemination of information and beliefs (Borgatti et al. 2013; Dang-Pham et al. 2014). Based on the theories and empirical findings presented so far and summarised in Table 1, the links between the influence mechanisms, information security climate perceptions, and compliant intention could be reasonably established. The integration of these three components forms our proposed framework and is illustrated in Figure 1 below.

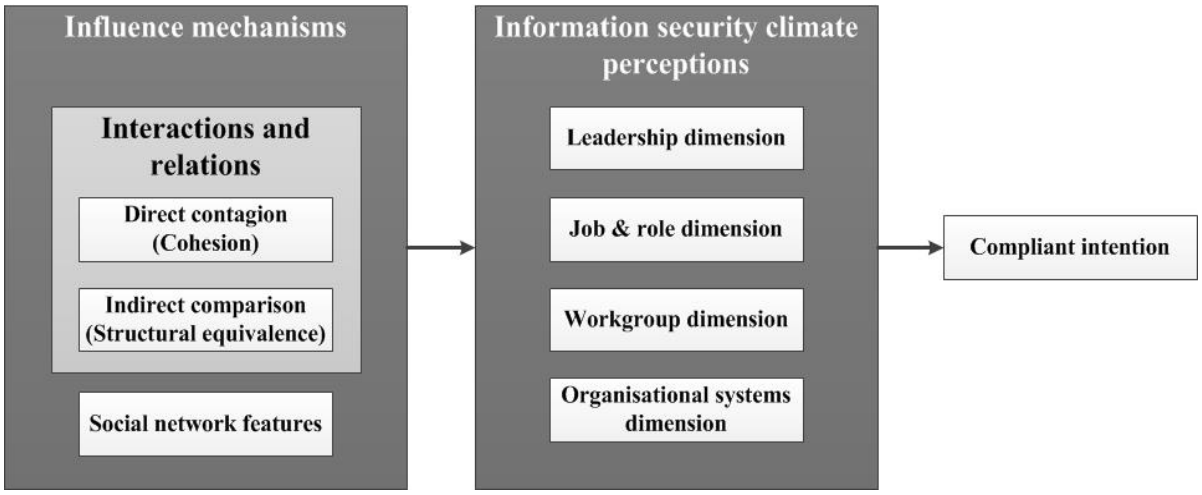

Figure 1. Proposed research framework

5 FUTURE RESEARCH DIRECTIONS

Given the topics that we have discussed are mostly under-researched, there is a need to firstly explore the relevant concepts that are potential for future studies. Besides conducting systematic literature reviews, fieldwork investigations are desired for identifying those concepts. More specifically, ethnographic methods and case studies are recommended because they can investigate in-depth the information security climate perceptions, as well as the influence mechanisms that emerge from the people's observation of information security matters in their local workplace whose nature is context-dependent and intimately meaningful to individuals. The detailed literature review in this paper (as summarised in Table 1) provides the relevant factors to be explored empirically in actual contexts with the suggested methods.

After determining the research environment and identifying the relevant concepts in that context, the researchers can specify a research model and its hypotheses based on our proposed framework. The next step involves testing the hypotheses or relationships between the identified factors with social network analysis techniques. Such techniques were suggested because they allow the researchers to flexibly investigate the phenomena at different levels, particularly the mechanisms of information exchange and influence among the individuals (Borgatti et al. 2013). Detailing the step-by-step hypotheses testing procedures requires lengthy discussions that have been better explained in other methodological studies, thus is purposely omitted from this paper. Given the limited space and the scope that focuses more on the theoretical framework, we briefly describe the hypotheses tests below.

As consistent with the levels of analysis, there are three types of hypotheses that can be tested: monadic (i.e. about actor's attributes), dyadic (i.e. about relational features of pairs of actors), and mixed monadic/dyadic hypotheses (Borgatti et al. 2013). An example of a monadic hypothesis could be about testing whether the number of information resources that an individual has access to would influence their information security climate perceptions. The particular relationship between "social network features" factor and "information security climate perceptions" in Figure 1 particularly refers to monadic hypotheses. With this knowledge, practitioners can adjust the positions of the individuals in the workplace's social network, or exploit the existing information brokers to evenly distribute information about security matters to everyone. A dyadic hypothesis example could be about using a relation or interaction (e.g. friendship) to predict another (e.g. delegating responsibility) between pairs of individuals. The findings resulted from these tests are especially useful for selecting the channels to foster information security learning and establishing communities of practice in the workplace.

On the other hand, the mixed monadic/dyadic hypotheses describe the diffusion and selection processes in the social networks. Unlike monadic hypotheses which could be tested by traditional methods such as generalised linear models without much difficulty, working with dyadic and mixed hypotheses demand more considerations (Butts 2008). It is then recommended to perform permutation tests such as QAP regression procedures that are available in the software package UCINET so to avoid such violation (as detailed in Borgatti et al. 2013). To test for social influence's effects such as cohesive contagion of information security climate perceptions, one may have an advice matrix (i.e. who receives direct advice from whom) regressed on another matrix of similarities in perception. The relationship between "interactions and relations" and "information security climate perceptions" as depicted in Figure 1 refers to these mixed hypotheses (i.e. predicting diffusion of perceptions).

6 CONCLUSION

Over the past years, studies in information security behavioural field have advanced knowledge of the contributing factors that motivate employees' compliant intention and behaviours. Among them, information security climate perceptions, or the valuations of the workplace's attributes in relation to information security matters, have been under researched and investigated inconsistently despite their importance. More specifically, understanding the employees' information security perceptions that emerge from their work environment would assist organisations in building a secure workplace and an information security culture in long term. More importantly, the predominant focus on the cognitions at the individual level appears to have overlooked the mechanisms that actually deliver the motivations to the individuals. This knowledge gap would prevent practitioners from effectively and efficiently raising information security awareness in the workplace, as well as explain why security violations still persist despite the existence of information security controls and training.

In response to the those issues, this conceptual paper proposes a research framework that describes the formulation and dissemination processes of information security climate perceptions by reviewing literatures from multiple domains. Relevant information security climate perceptions were consolidated and outlined in the first part of our paper, while the second part presents the influence mechanisms that could disseminate those perceptions. To provide further assistance, we briefly recommended the research methods that could be employed in future research. The recommendations include the use of social network analysis techniques being introduced as a novel and appropriate approach for investigating information security behavioural topics.

References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29 (4), 432-445.

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2013). Analyzing Social Networks. Sage Publications Ltd.

Brass, D., Butterfield, K., & Skaggs, B. (1998). Relationships and unethical behavior: A social network perspective. Academy of Management Review, 23 (1), 14-31.

Burt, R. (1987). Social contagion and innovation: Cohesion versus structural equivalence. American Journal of Sociology, 92 (6), 1287-1335.

Butts, C. T. (2008). Social network analysis: A methodological introduction. Asian Journal of Social Psychology, 11, 13-41.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. In Perceptions of Information Privacy and Security, 18-41.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: compliance and conformity. Annual Review of Psychology, 55 (1974), 591-621.

Da Veiga, a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29 (2), 196-207. doi:10.1016/j.cose.2009.09.002

Dang, D. P. T. (2014). Predicting insider's malicious security behaviours: a General Strain Theory-based conceptual model. In 2014 International Conference on Information Resources Management (Conf-IRM 2014). Ho Chi Minh City, Vietnam.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. Computers & Security, 48, 281-297.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2014). Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach. In 25th Australasian Conference on Information Systems (ACIS). Auckland, New Zealand.

Dourish, P., & Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. Human-Computer Interaction, 21 (3), 319-342.

Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing, 8 (6), 391-401.

Ferrin, D. L., Dirks, K. T., & Shah, P. P. (2006). Direct and indirect effects of third-party relationships on interpersonal trust. The Journal of Applied Psychology, 91 (4), 870-883.

Goo, J., Yim, M., & Kim, D. (2014). A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. IEEE Transactions on Professional Communication, 57 (4), 1-24.

Härtel, C. E., & Ashkanasy, N. M. (2010). Healthy human cultures as positive work environments. In Handbook of organizational culture and climate.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18 (2), 106-125.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29 (3), 221-232.

Ibarra, H., & Andrews, S. B. (1993). Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions. Administrative Science Quarterly, 38 (2), 277-303.

Jaafar, N. I., & Ajis, A. (2013). Organizational Climate and Individual Factors Effects on Information Security Faculty of Business and Accountancy. International Journal of Business and Social Science, 4 (10), 118-130.

James, L. a., & James, L. R. (1989). Integrating work environment perceptions: Explorations into the measurement of meaning. Journal of Applied Psychology, 74 (5), 739-751.

James, L. R., Choi, C. C., Ko, C.-H. E., McNeil, P. K., Minton, M. K., Wright, M. A., & Kim, K. (2008). Organizational and psychological climate: A review of theory and research. European Journal of Work and Organizational Psychology, 17 (1), 5-32.
Jones, A., & James, L. (1979). Psychological climate: Dimensions and relationships of individual and aggregated work environment perceptions. Organizational Behavior and Human Performance, 201-250.
Kuenzi, M., & Schminke, M. (2009). Assembling Fragments Into a Lens: A Review, Critique, and Proposed Research Agenda for the Organizational Work Climate Literature. Journal of Management, 35 (3), 634-717.
Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security, 18 (1), 4-13.
Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27 (5), 445-454.
Leenders, R. T. A. J. (2002). Modeling social influence through network autocorrelation: constructing the weight matrix. Social Networks, 24 (1), 21-47.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. Journal of the Association for Information Systems, 11 (7), 394-413.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 93-114.
Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26 (1), 56-62.
Scherer, C. W., & Cho, H. (2003). A Social Network Contagion Theory of Risk Perception. Risk Analysis, 23 (2), 261-267.
Schneider, B., Ehrhart, M. G., & Macey, W. H. (2013). Organizational climate and culture. Annual Review of Psychology, 64-88.
Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34 (3), 487-502.
Stiglitz, J. E., & Fitoussi, J. (1996). A management communication strategy for change. Journal of Organizational Change Management, 9 (2), 32-46.
Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29 (4), 476-486.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49 (3-4), 190-198.
Zohar, D. (2008). Safety climate and beyond: A multi-level multi-climate framework. Safety Science, 46 (3), 376-387.
Zohar, D. (2010). Thirty years of safety climate research: reflections and future directions. Accident Analysis and Prevention, 42 (5), 1517-1522.
Zohar, D., & Tenne-Gazit, O. (2008). Transformational leadership and group interaction as climate antecedents: a social network analysis. The Journal of Applied Psychology, 93 (4), 744-757.