2017

Understanding the Formation of Information Security Climate Perceptions: A Longitudinal Social Network Analysis

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

Karlheinz Kautz
RMIT University, karlheinz.kautz@rmit.edu.au

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

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

Understanding the Formation of Information Security Climate Perceptions: A Longitudinal Social Network Analysis

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

Karlheinz Kautz
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: karlheinz.kautz@rmit.edu.au

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

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

Abstract

This research employed a longitudinal social network analysis (SNA) method, called stochastic actor-oriented modelling (SAOM), to analyse the inter-relationship between the employees' socialisation and information security (InfoSec) climate perceptions which are the employees' perceptions of their colleagues and supervisors' InfoSec practices. Unlike prior studies, we conceptualised socialisation in the form of six networks: the provision of work advice and of organisational updates, the provision of personal advice, interpersonal trust in expertise, the provision of InfoSec advice, and support for InfoSec troubleshooting. The adoption of the SAOM method enabled not only analysis of why an employee chooses to interact with or to send a network tie to another employee, but also how an employee's perception of InfoSec climate is affected by the ties that they possess in the network. This research suggests new directions for InfoSec behavioural research based on the adoption of SNA methods to study InfoSec-related perceptions and behaviours, while findings about the selection and influence mechanisms offer theoretical insights and practical methods to enhance InfoSec in the workplace.

Keywords: information security, information security climate, information security management, social network analysis, stochastic actor-oriented modelling

1 Introduction

The behavioural information security (InfoSec) research field has recently focused on examining the impacts of the work environment on the employees' InfoSec perceptions and behaviours. For instance, Willison and Warkentin (2013) extended the Security Action Cycle by adding what they called "pre-kinetic events" that described the InfoSec environment's impacts on the development of InfoSec violations. Baskerville et al. (2014) analysed the InfoSec vulnerabilities in the workplace that could be exploited by the potential perpetrators to execute InfoSec violations. Situational support and peer-learning opportunities have been identified as important to the employees' compliance with InfoSec directives (Warkentin et al. 2011). The active provision of InfoSec advice among employees helps to reduce the time lost from re-inventing InfoSec solutions and enable the efficient allocation of resources to other InfoSec tasks of higher priorities (Safa et al. 2016).

Acquiring a holistic understanding about the social and environmental dynamics that constantly take place within the workplace, or how the employees' InfoSec perceptions shape their interactions and vice versa, can shed light on the opportunities and practices to improve organisational InfoSec. Conducting research to measure the effective delivery and utilisation of InfoSec advice and InfoSec troubleshooting would ideally require evaluating the changes before and after such delivery or utilisation. Recently InfoSec-related action research projects have been reported which involved monitoring throughout the research process and evaluating theoretically-grounded InfoSec implementation (e.g., Puhakainen and Siponen 2010). These studies focused on the changes in the employees' individual perceptions and behaviours, thereby overlooking the changes in the InfoSec environment that are external to the employees' cognition.

Our research objective is to explore and identify the employees' characteristics and their social interactions, also termed *socialisation*, that lead to the formation of an InfoSec climate, which is the employees' perceptions of their colleagues and supervisors' InfoSec practices (Chan et al. 2005; Goo et al. 2014). We employed a longitudinal social network analysis (SNA) method called stochastic actor-oriented modelling (SAOM) (Steglich et al. 2010) to investigate the changing inter-relationship between employees' perceptions of InfoSec climate and social interactions in a large organisation. Our study contributes to the current research gap in the behavioural InfoSec area, which has not yet empirically explored the impacts of individuals' interactions and relationships (in the form of social networks) on their InfoSec perceptions (Dang-Pham et al. 2017a). The adoption of the SNA method allows us to investigate the structural features and mechanisms of the InfoSec-related interactions and relations between employees (e.g., reciprocity, popularity, transitivity), which have traditionally been studied as individuals' perceptions (Sommestad et al. 2014). Conducting SNA further enables testing hypotheses that reflect existing explanations for the formation of InfoSec climate, by highlighting the interactional nature of socialisation (Schneider and Reichers 1983; Ashforth 1985). Unlike prior studies that conceptualised socialisation as the employees' cognitive perceptions (Chan et al. 2005; Goo et al. 2014), we analyse this concept as networks of employees' provisions of advice, support and interpersonal trust.

2 Literature review

2.1 Perceptions of InfoSec climate

The concept of InfoSec climate refers to the shared and collective InfoSec practices in a workplace that reflect how an organisation is treating InfoSec (Lowry and Moody 2013). The concept InfoSec climate was originally adapted from the work safety climate literature. It is defined as the employees' perceptions of the observed InfoSec environment, which consists of the observable InfoSec behaviours performed by their colleagues and supervisors (Chan et al. 2005; Dourish and Anderson 2006; Goo et al. 2014). Employees have their InfoSec perceptions and behaviours influenced by many factors in the work environment (see e.g., Padayachee 2012; Sommestad et al. 2014). InfoSec climate holds an important role since it fosters and maintains InfoSec compliance and InfoSec culture (Chan et al. 2005). InfoSec climate also promotes the provisions of InfoSec advice and the support for InfoSec troubleshooting in the workplace (Dang-Pham et al. 2017b). From a practical perspective, understanding the factors and mechanisms that lead to the formation of a positive InfoSec climate can contribute to the effective management of organisational InfoSec.

2.2 InfoSec-related socialisation and the formation of InfoSec climate

Since prior studies in the behavioural InfoSec field have not yet empirically explained the formation of InfoSec climate, we consulted literature about the formation of organisational climates in general. Schneider and Reichers (1983) argued that the formation of organisational climates could be studied

under a structuralist perspective, a selection-attraction-attrition perspective, and an interactionist perspective. Specifically, the first and second perspective explain that organisational climates are formed by the objective characteristics of the workplace and the subjective similarities of the employees respectively, and the third perspective posits that organisational climates are formed as a result of the employees' interactions (Schneider and Reichers 1983). The interactionist perspective on the formation of organisational climates blends the objectivism and subjectivism of the former two perspectives to explain the changing nature of organisational climates (Ashforth 1985; Schneider and Reichers 1983).

Ashforth (1985) further argued that the employees' socialisation, which is brought about through their provisions of organisational resources in the workplace, facilitates the formation of organisational climate (Ashforth 1985); as such the employees' socialisation is facilitated by normative and informational influences which themselves form the organisational climate. Since employees have a constant need to make sense of their workplace, socialisation shapes and maintains the organisational climate by enabling the employees to reach a consensus on the meanings of organisational practices (Ashforth 1985; Schneider and Reichers 1983).

The employees' socialisation in the form of sense-making activities, such as provisions of work-related advice and interpersonal trust, helps to reduce uncertainty (i.e., lack of information) and to clarify ambiguity (i.e., too much overlapping information) (Saint-Charles and Mongeau 2009). In the InfoSec context, the socialisation among employees involves discussing, teaching, and learning about InfoSec-related matters (Chan et al. 2005; Goo et al. 2014). The InfoSec-related socialisation between the employees with their colleagues and supervisors raises awareness of the InfoSec practices deployed by their organisation, which contributes to a positive InfoSec climate (Chan et al. 2005). We therefore analysed socialisation in the form of six social networks. They are the social networks of provisions of work-related advice and organisational updates (combined as an "instrumental network"), of provision of personal advice and interpersonal trust in a colleague's expertise (combined as an "expressive network"), and the network of provision of InfoSec advice and of support for troubleshooting (combined as "InfoSec support network"). The instrumental and expressive networks represent the social interactions that exist in every organisation (Saint-Charles and Mongeau 2009; Tichy et al. 1979) as well as the socialisation that facilitates to the formation of organisational climates such as InfoSec climate (Ashforth 1985; Schneider and Reichers 1983). Likewise, the InfoSec support network specifically refers to the InfoSec-related socialisation which has an impact on InfoSec climate (Chan et al. 2005; Goo et al. 2014). This justifies the inclusion of these networks in this research.

Organisational networks consist of instrumental and expressive interactions (Borgatti et al. 2013; Ibarra and Andrews 1993; Saint-Charles and Mongeau 2009; Tichy et al. 1979). Researchers studied instrumental and expressive interactions as social networks of "seeking work-related advice" and "seeking personal advice" respectively (Ibarra and Andrews 1993). We added one network to each of these two types of networks which we labelled "seeking organisational updates" and "interpersonal trust in expertise". Since performing InfoSec behaviours requires reviewing relevant policies and directives, individuals who have first access to the latest organisational updates can be influential. The instrumental network in our study was thus defined as comprising the provisions of work-related advice and organisational updates. The expressive network in our study consisted of the socialisation that facilitated the provisions of personal advice and of interpersonal trust in expertise. Interpersonal trust is multi-faceted, which includes trusting a person's expertise and characteristics such as benevolence and integrity (McKnight 2002). While nominating a person to be capable of sharing and of discussing personal advice indicated the nominator's trust in the person's benevolent character, the "interpersonal trust in expertise" network that consisted of nominated people who were trusted for expertise covered the other facet of trust.

The InfoSec support network in our study referred to the provisions of InfoSec advice and the troubleshooting support among the employees. From the InfoSec climate perspective, these provisions of InfoSec advice and for troubleshooting presented the socialisation that involved the employees discussing InfoSec matters with each other (Chan et al. 2005; Goo et al. 2014). From the social influence perspective, being nominated as capable of providing InfoSec advice and support meant that the nominated person possessed expert power to influence others' behaviours (French and Raven 1959).

2.3 Theoretical model

Figure 1 presents the theoretical model that summarises the key components and their relationships in our study. With a basis in the reviewed literature, the theoretical model is explained as follows. First, the employees' socialisation which consists of the six social networks combined into three higher order networks (i.e., provisions of instrumental, expressive, and InfoSec support resources), is consistent with prior studies about sense-making activities (Ibarra and Andrews 1993; Saint-Charles and Mongeau

2009). The combination of these six networks was based on their relevant contents as described in the reviewed literature. Of these three networks, the social network about the provisions of InfoSec support (i.e., InfoSec advice and InfoSec troubleshooting) contributes the most to the employees' perceptions of InfoSec climate, which follows Chan et al.'s (2005) and Goo et al.'s (2014) discussion on the formation of InfoSec climate.

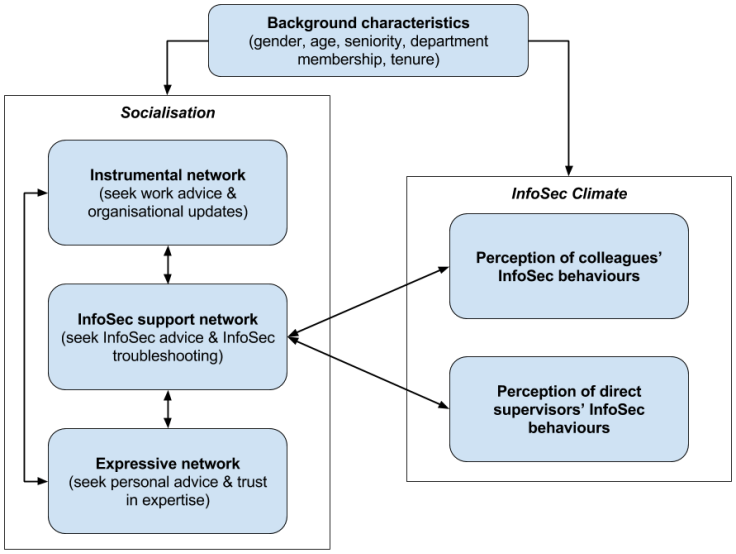

Figure 1. Theoretical model

We argue that the social networks representing the employees' socialisation impact each other, and the InfoSec support network influences the formation of InfoSec climate, which is reflected by the employees' perceptions of colleagues' and direct supervisors' InfoSec behaviours. The former argument is based on the concept of network multiplexity (Borgatti et al. 2013; Tichy et al. 1979) which posits that an individual may hold multiple roles, such as serving as the source of both instrumental and InfoSec support resources in the workplace. We describe the co-occurrence of the social networks in figure 1 by the bi-directional arrows among them.

The impact of the employees' perceptions of InfoSec climate on the InfoSec-related socialisation, specifically on the provision of InfoSec support, follows the principle of homophily. Homophily describes the human tendency to purposely associate with similar others, who share characteristics such as demographics, behaviours, or perceptions (Borgatti et al. 2013; McPherson et al. 2001). On this basis, we expect that employees who share similar levels of climate perceptions will intentionally choose to seek InfoSec support from each other, hence the bi-directional arrows between climate perceptions and InfoSec support network. Background characteristics such as age, gender, department membership, are included as control variables that impact both the employees' socialisation and climate perceptions.

3 Research method

SNA methods focus on analysing social interactions and relationships as network ties between actors (termed "nodes"), thus allow researchers to investigate in depth the social environment of individuals (Borgatti et al. 2013). Stochastic actor-oriented modelling (SAOM) is a predictive SNA method that provides the analytical capabilities to analyse longitudinal changes in the inter-relationship between nodal characteristics and network ties (Ripley et al. 2017). Snijders et al. (2010) provided a comprehensive and detailed introduction featuring the SAOM method, which involves specifying a model with parameters that evaluate the simultaneous changes in the employees' selection patterns of networks (i.e., the creation or maintenance of network ties over time) and the influence effects (i.e., the changes in the employees' InfoSec climate perceptions caused by the changing network ties).

As our research objective is to study the formation of InfoSec climate, which is the change of a workplace's InfoSec climate from one state to another; our research took place in a large construction enterprise in Vietnam (anonymised as "ABC"). We were approached by ABC to assist them with the diffusion of InfoSec advice and InfoSec troubleshooting in their workplace. We employed social network analysis (SNA) methods to identify the enterprise's InfoSec champions, who would be those employees to provide InfoSec advice and InfoSec troubleshooting support. These champions underwent a training

program and were asked to afterwards provide their new InfoSec knowledge to their colleagues in their departments.

3.1 Data collection

We collected our data in two waves. Data collection of wave 1 was performed before the provision of InfoSec advice and InfoSec troubleshooting by the champions, and wave 2 took place three months after the training and start of the diffusion actions. A questionnaire was designed to capture the six social networks of interest by asking the employees to nominate the colleagues who engaged with them in a network (refer to table 1 below). In a second part of the questionnaire we asked the employees to answer Likert scale questions that captured their climate perceptions of colleagues and supervisors' InfoSec behaviours.

Whole-network questionnaires demand information such as real names, which can pose as a source of common method bias and affect the response rate, since the employees may not want to be identified and evaluated for their responses (Borgatti et al. 2013; Podsakoff et al. 2003). To alleviate the issues related to anonymity, ABC's top management publicly announced in a memorandum of understanding that they did not have access to the collected data. To further minimise common method bias, remedies were employed such as mixing the order of questions to not relate to the same latent construct, and to include detailed definitions and examples to clarify any potentially vague questions (Podsakoff et al. 2003).

Combined network	Network	Network question
Provisions of instrumental resources (involve provisions of resources that contribute to problem-solving and enhancing work processes)	Seek work advice	Who do you usually ask for advice (e.g. look for or improve solutions, get referrals or confirmation) about work?
	Seek organisational updates	From whom do you usually get the latest updates or changes (e.g. new policies, process, system) in ABC?
Provisions of InfoSec resources (an instrumental network which focuses on InfoSec advice and troubleshooting)	Seek InfoSec advice	Who would explain the importance of InfoSec to you, and/or teach you how to perform InfoSec behaviours, and/or use InfoSec technologies?
	Seek InfoSec troubleshooting	When you encountered an InfoSec problem e.g. lost or damaged data, computer virus infection etc., whom would you seek help from?
Provisions of expressive resources (involves interpersonal trust and affect)	Seek personal advice	When you want to discuss or ask for advice about personal life issues, whom would you talk to?
	Trust in expertise	Who do you think would be most able (because of education, experience, qualities) to take over your work if you were too busy or absent?

Table 1. Network questions

We used two sets of questions adapted from prior InfoSec climate studies (Chan et al. 2005; Goo et al. 2014) to capture the employees' climate perceptions of their colleagues and direct supervisors' InfoSec behaviours and we employed a seven-point scale to ask 10 questions about the level of InfoSec behaviours performed by the employees' colleagues and direct supervisors. Examples of the items are "How frequently do your direct supervisor(s) mention InfoSec matters to you and your co-workers?", "How often do your direct supervisor(s) require that you and your co-workers perform InfoSec behaviours?", and "How often do your co-workers perform InfoSec behaviours in their daily work?".

3.2 Data preparation

Missing data is problematic for longitudinal research and can result in biased findings without proper treatment (Ripley et al. 2017). Whole-network research design, which focuses on a bounded environment, can have missing data due to the respondents' refusal to participate in the survey or their exit of the bounded environment (Borgatti et al. 2013). Missing data in our study resulted from some participants' refusal to participate and due to the high turnover rate at ABC and in the construction industry in Vietnam. To ensure reliable analysis, we trimmed the dataset by selecting only the employees who casted their nominations in both waves. This resulted in a dataset which consisted of 151 employees.

We performed confirmatory factor analysis (Brown 2006) to specify and fit measurement models for the InfoSec climate perceptions of colleagues (COL) and supervisors' InfoSec behaviours (SUP). The two models were fitted under the assumption that perceptions in wave 1 influenced perceptions in wave 2. Since our Likert scale-based data violated the multivariate normality assumption, Maximum Likelihood estimation was deemed inappropriate and we relied on the Bollen-Stine bootstrapping method (Bollen and Stine 1992) to evaluate whether the model was specified correctly and fitted. Both models exhibited acceptable goodness-of-fit with Bollen-Stine bootstrap p-values equal to 0.357 (COL) and 0.669 (SUP). Table 2 shows that there were no issues with convergent validity.

Construct	Item	Loading–W1	α–W1	H–W1	Loading–W2	α–W2	H–W2
SUP	SUP1	0.94	0.94	0.95	0.90	0.95	0.95
	SUP2	0.94			0.95		
	SUP3	0.89			0.88		
	SUP4	0.83			0.90		
	SUP5	Dropped			Dropped		
COL	COL1	0.93	0.94	0.96	0.89	0.94	0.96
	COL2	0.93			0.92		
	COL3	0.71			0.69		
	COL4	0.83			0.92		
	COL5	0.93			0.94		
Acceptable criteria		**>±0.35**	**>0.70**	**>0.70**	**>±0.35**	**>0.70**	**>0.70**

Table 2. Convergent validity (W1=Wave 1; W2=Wave 2)

Factor score weights from the fitted measurement models were used to calculate composite scores of the latent constructs. Calculation of composite scores of latent constructs was necessary in our case since SAOM allows only single-item variables (Ripley et al. 2017). Further transformation included rounding the computed scores to integers, so to meet the other data requirement of the SAOM method that accepts only integer variables (Ripley et al. 2017).

3.3 Stochastic actor-oriented modelling process

Researchers performing SAOM develop and estimate mathematical models with parameters that describe two types of change mechanisms of the network. These mechanisms are about how a network tie is formed (i.e., why an actor choses to interact with or to send a tie to another one), and about how a characteristic of a node (e.g., perception of InfoSec climate) is affected by the ties that the node possesses (Ripley et al. 2017). Researchers refer to these two mechanisms as the "selection" and "influence" mechanisms respectively (Steglich et al. 2010). Table 3 summarises the parameters describing these mechanisms that were included in our model, which were consistent with our theoretical model illustrated in figure 1.

Besides the parameters which were included to model the inter-relationships between the networks and the employees' background characteristics, as well as the impacts of InfoSec support network on perceptions of InfoSec climate, we included parameters describing structural effects. These effects account for the formation of the network ties due to the structural features of the networks themselves. The inclusion of these effects contribute more explanations to the selection mechanisms of the networks, while increasing the model's goodness-of-fit (Ripley et al. 2017).

Network mechanism	Effect described by parameter	Parameter	Description of effect
SELECTION	Structural effects on networks	rate	This parameter models the speed by which a network actor gets an opportunity to change their tie/perception.
		outdegree	This parameter models the tendency of a network actor to send an outgoing tie.
		gwespFF	This parameter models the nodes' tendency to close triads (i.e., set of three nodes) by establishing a direct connection with those who share the same partners.
		outActSqrt	This parameter models the dispersion in terms of out-degrees in the network.
		inPopSqrt	This parameter models the dispersion in terms of in-degrees in the network.
		reciprocity	This parameter models the tendency to reciprocate ties.
	Networks' effects on each other	cprod	This parameter models the tendency of two types of network co-occur with each other.
	Background characteristics' effects on networks	egoX altX	These parameters model the effect of a node's attribute on the occurrence of ties.
		sameX simX	These parameters model homophily for attributes of nodes i.e., nodes of same or similar attributes would be more likely to establish ties.
		linear shape	This parameter models the network actor's basic drive towards achieving a high value of the behaviour or perception's score.
		quadratic shape	This parameter models the feedback of the behaviour or perception on itself. This includes self-correcting (i.e., a negative estimate, which indicates the behaviour or perception's score is pulled to the average) or self-reinforcing (i.e., a positive estimate, which indicates the score is pushed to the extreme ends).
INFLUENCE	InfoSec support network's effect on perceptions of InfoSec climate	totAltW	This parameter models the influence effect on an individual's perception while accounting for the total number of neighbours (or connections) the influenced actor has. A positive estimate means that employees increased their climate perceptions when they were tied to others whose climate perceptions were at a high level. The letter "W" in the parameter's name indicates that this is the weighted (by the "same department" tie) version of the influence effect.
	Background characteristics' effects on perceptions of InfoSec climate	effFrom	This parameter models the effects of the employees' background characteristics (e.g., age, gender, seniority) on their perceptions of InfoSec climate.

Table 3. Parameters included in the stochastic actor-oriented model

4 Analysis and findings

We developed and estimated a large SAO model, which consisted of 96 parameters, by using the R statistical package called "RSiena" (Ripley et al. 2017). The same set of parameters describing "selection" mechanisms (e.g., rate, outdegree, crprod, sameX, etc.) was included for each of the three networks. Similarly, we included the same set of "influence" parameters (i.e., totAltW, effFrom) for the two perceptions of InfoSec climate. Table 4 summarises the results of our SAO model.

Due to the page limit, table 4 only reports the parameters that achieved statistical significance, as their parameter's estimate was twice as large as its standard error. The estimates reported in table 4 are log-odds ratios which can be converted into probabilities. For example, the estimate of effect #25 is 0.55, which describes the tendency of a network actor (named "A") to receive InfoSec support from other actors (named "B" or "C") with one of them holding the champion role. By taking the exponential of this estimate, it can be interpreted that for actor B and C, of whom B is the champion, the likelihood for A to receive InfoSec support from B (i.e., the champion) is 1.73 times higher than from C (i.e., the non-champion).

#	**Instrumental network**	**Estimate**	**Std. Error**
1	rate	7.09	-0.67
2	outdegree	-5.15	-0.74
3	reciprocity	0.84	-0.24
4	transitivity (gwespFF)	1.19	-0.23
5	gender alter (altX)	0.44	-0.13
6	gender ego (egoX)	-0.44	-0.15
7	same gender (sameX)	0.34	-0.12
8	same department (sameX)	0.94	-0.12
9	age alter (altX)	0.03	-0.01
10	seniority alter (altX)	0.50	-0.17
11	same seniority (sameX)	0.50	-0.18
12	expressive network (crprod)	1.90	-0.23
#	**Expressive network**	**Estimate**	**Std. Error**
13	rate	5.46	-0.55
14	outdegree	-4.20	-1.01
15	reciprocity	1.55	-0.19
16	transitivity (gwespFF)	1.04	-0.19
17	gender alter (altX)	0.56	-0.15
18	same gender (sameX)	0.66	-0.14
19	same department (sameX)	1.05	-0.14
20	instrumental network (crprod)	1.75	-0.33
#	**InfoSec support network**	**Estimate**	**Std. Error**
21	rate	8.29	-1.05
22	outdegree	-2.60	-1.05
23	same department (sameX)	1.22	-0.15
24	age alter (altX)	-0.03	-0.01
25	champion alter (altX)	0.55	-0.16
26	expressive network (crprod)	1.56	-0.40
27	instrumental network (crprod)	1.25	-0.37
#	**Perception of colleague's InfoSec behaviour**	**Estimate**	**Std. Error**
28	rate	2.07	-0.41
29	quadratic shape	-0.62	-0.19
30	effect of social influence on an individual's perception received from providers of InfoSec support in the same department (totAltW)	Score test[+++]	Score test [+++]
#	**Perception of direct supervisor's InfoSec behaviour**	**Estimate**	**Std. Error**
31	rate	2.74	-0.59
32	linear shape	2.57	-1.16
33	quadratic shape	-0.37	-0.11

- [+++]Score test was employed to examine this effect and the estimate was found positive and significant (Chi-square=9.2887; p-value=0.0023; one-sided statistic=3.0477)
- Statistically significant effects have estimates that are twice as large as their standard errors

Table 4. SAOM results

The parameter *rate* presents the number of opportunities for changing ties per actor in the network between the two data collection points (Ripley et al. 2017). The InfoSec support network had the largest number of change opportunities (effect #21). The more stable expressive (#13) and instrumental networks (#1) reflect the fact that without any major events, it would be reasonable to assume for the daily work routines in the company to remain unchanged.

In all examined networks, their *outdegree* parameters (#2, #14, #22) achieved statistical significance with negative values, which indicates these networks had sparse density or rare occurrence of network ties between employees. The *reciprocity* parameter, which describes the employees' tendency to

reciprocate ties, only achieved significance in the instrumental (#3) and expressive networks (#15) but not the InfoSec support network. The odds ratio of the *reciprocity* parameters for instrumental and expressive networks were 2.3 (exponential of 0.84) and 4.7 (exponential of 1.55) respectively. In other words, work advice and organisational updates were reciprocated 2.3 times more likely than only uni-directed, and 4.7 times more likely for the network about provisions of personal advice and trust in expertise.

Transitivity describes the tendency that a network actor would close the triads with two other actors, by establishing a direct connection with the others who were already indirectly connected via multiple intermediaries. The positive results of this parameter indicate that the instrumental and expressive networks were transitive. Transitivity occurred more in the instrumental and expressive networks (#4, #16), but not in the InfoSec support network.

The parameters about selection mechanisms identified the factors that influenced the employees' socialisation in the three examined networks. For each of the employee's background characteristics such as gender, age, and tenure, we estimated parameters that described the selection tendency of the senders (i.e., egoX parameters), receivers (i.e., altX parameters), and matching partners (i.e., sameX parameters)–see table 3 for the parameters' descriptions. Female employees tended to be sought for instrumental (#5) and expressive resources (#17) more than male employees. Employees of the same gender tended to seek work advice and updates (#7), and personal advice and trust in expertise (#18) from each other more. In contrast, gender did not explain the patterns of InfoSec support provision.

Older employees tended to be sought more for instrumental resources (#9), whereas younger employees were more likely to be sought for InfoSec support (#24). Seniority also played a role in determining the employees' nominations in the instrumental network. Employees who held more senior positions provided more work-related advice or organisational updates (#10), and the provision of those resources occurred more between those having the same seniority (#11). Sharing the same department membership resulted in the employees' nominations in the three networks (#8, #19, #23). Employees who served as InfoSec champions in ABC were 1.7 times more likely than non-champions to be sought for InfoSec support (#25). We included parameters that evaluated the employees' tendency to socialise with those whose InfoSec climate perceptions' scores were similar (i.e., the "simX" parameter for climate perceptions in table 3). The results of these parameters did not achieve statistical significance and were thus omitted from table 4. However, the insignificant findings indicated that the employees' decision to socialise with others in the instrumental, expressive, and InfoSec support networks, was not affected by their similar InfoSec climate perceptions.

We found the three types of socialisation co-occurred with each other; the employees' selection of colleagues to socialise with in one network affected their socialising choice in other networks. The instrumental and expressive networks tended to co-occur with each other (#12, #20). Employees were more likely to seek work advice or updates from those whom they trusted, and vice versa. Similarly, InfoSec support ties co-occurred with instrumental and expressive ties (#26, #27).

We also examined how the employees' InfoSec climate perceptions changed over time as a result of other factors' effects. None of the background characteristics affected the formation of InfoSec climate perceptions, as the parameters describing their effects did not achieve statistical significance and were thus omitted. Since we calculated the scores for the climate perceptions of colleagues' and direct supervisors' InfoSec behaviours, which ranged from 1 (weak climate) to 5 (strong climate), we were interested in examining the variation of those scores. A positive and significant linear shape for climate perception of supervisors' InfoSec behaviours (#32) indicated that this perception tended to achieve a higher score over time. The negative values of the quadratic shape parameter for both climate perceptions (#29, #33) suggested that the scores of these perceptions tended to increase when being low, and to decrease when being high. It reflected the tendencies of self-reinforcing and self-correcting, and the scores of climate perceptions tended to deviate around the average point within the range of 1 to 5, rather than moving towards either of the polarised ends. Our analysis suggested that the employees were inclined to adjust their climate perception of colleagues' InfoSec behaviours to match with those who were in the same department and capable of providing them with InfoSec support (#30). In contrast, the same influence effect (i.e., parameter "totAltX" in table 3) was not confirmed to impact the change in the employees' climate perceptions of their direct supervisors' InfoSec behaviours.

5 Research implications

The primary objective of this research was to investigate the formation of the employees' perceptions of InfoSec climate, as a result of their social interactions or socialisation. Our finding that employees

tended to align their climate perceptions of colleagues' InfoSec behaviours with the perceptions of colleagues in the same department who provided them with InfoSec support, offers empirical evidence and supports the interactionist perspective's explanation for the formation of organisational climates (Schneider and Reichers 1983). The result further indicated that the number of IS support providers also impacted the social influence effect.

Our study offers practical recommendations about how to facilitate positive changes in an InfoSec environment by increasing the employees' socialisation. Specifically, the employees' department membership and age were identified to have strong impacts on the socialisation that involved the provision of InfoSec support among employees. The provision of InfoSec support was affected by organisational interactions such as the provisions of work advice and interpersonal trust. It should be noted that the effect of expressive ties (i.e., provisions of personal advice and interpersonal trust) on InfoSec socialisation was stronger than that of the instrumental ties (i.e., provisions of work advice and of organisational updates). Top management are advised to consider the employees' background characteristics (i.e., department membership, age, seniority) since they can affect the provisions of instrumental and expressive resources, which subsequently stimulate the provision of InfoSec support and lead to the formation of InfoSec climate.

As the provisions of work and personal advice were found to increase the provision of InfoSec support and InfoSec climate perceptions, organisations are advised to create socialising opportunities for their employees through initiatives such as job rotations, cross-functions projects, or mentoring systems. Top management also need to be aware of the employees' potential emergence as influential InfoSec support sources in the workplace. While these employees can be trained to provide other employees with InfoSec support of consistently high quality and contributed to the formation of a positive InfoSec climate, they can also diffuse unofficial and risky IS practices to their colleagues. To this end, our SAOM results serve as the criteria to identify these influential employees who act as the sources of InfoSec support in the workplace.

6 Future directions

While prior studies had analysed InfoSec climate and socialisation separately as the employees' perceptions (Chan et al. 2005; Dang-Pham et al. 2017b; Goo et al. 2014; Safa et al. 2016; Warkentin et al. 2011), the SAOM method is useful for examining both concepts simultaneously. Scholars in the behavioural InfoSec field had been exploring the intrinsic and extrinsic motivations that led to various InfoSec behaviours and perceptions. For instance, Protection Motivation Theory (Rogers 1975) has been widely applied to examine employees' perceptions of threat and coping measures, and the Theory of Planned Behaviour (Ajzen 2011) has been used to examine self-efficacy and perceived controllability, all of which were found to impact InfoSec behavioural decisions (Padayachee 2012; Sommestad et al. 2014). Moreover, various social processes were found to affect InfoSec behaviours, such as social learning (Warkentin et al. 2011) and social bonding (Cheng et al. 2013; Ifinedo 2014). It would be interesting to apply the SAOM method to explore how the employees' perceptions of threats, self-efficacy, or effectiveness of InfoSec protection are or can be shaped by other social interactions in the workplace.

Further network research ideas can be extended to address issues about InfoSec noncompliance and misbehaviours. For example, it was recently argued that InfoSec violations can be caused by employees who are disgruntled by their work environment (Willison and Warkentin 2013). Perception of injustice was also found to result in InfoSec misbehaviours (Posey et al. 2011). A longitudinal SNA method such as SAOM can be applied to identify factors that cause the employees' distress and thus might support the tendency to violate InfoSec policy, based on which appropriate and early countermeasures to prevent misbehaviours can be devised. Finally, we argue that it would be worth developing new theoretical frameworks that focus on explaining the temporal changes in InfoSec-related interactions, perceptions, and behaviours. Likewise, we need theories that use network-related components, such as employees' positions in networks and network structures, to explain InfoSec behaviours and perceptions.

7 Conclusion

Current studies in the behavioural InfoSec field have highlighted the importance of investigating how the socio-organisational factors can benefit or threaten organisational InfoSec, since such knowledge is critical for formulating practical strategies and measures for InfoSec success. Nevertheless, current research in the field has focused on the individual cognitive processes of employees, which determine how they perform InfoSec behaviours (see Padayachee (2012) and Sommestad et al. (2014) for reviews of existing studies), thereby overlooking the interactions and relationships between the employees.

The adoption of SNA methods enables the investigation of these interactions and relationships that shape the employees' InfoSec environment, such as their perceptions of InfoSec climate (Chan et al. 2005; Goo et al. 2014). Our research employed a longitudinal SNA method to examine the formation of InfoSec climate, as reflected by the inter-relationship of the employees' socialisation and their InfoSec climate perceptions. Our analysis found that employees' background characteristics (e.g., same department membership, age, gender, seniority) and their provisions of work advice, organisational updates, personal advice, and their trust in expertise, can increase the InfoSec-related socialisation that involves exchanging InfoSec support. This InfoSec-related socialisation contributes to the formation of InfoSec climate by stimulating the employees' decision to match their perceptions of colleagues' InfoSec behaviours. We advise top management to make use of the employees' background characteristics and of workplace interactions to develop a positive InfoSec climate and to increase the employees' socialisation about InfoSec matters. As SNA methods have not yet widely been adopted in the behavioural InfoSec field, we look forward to seeing more network research in this field.

8 References

Ajzen, I. 2011. "Theory of planned behavior," in *Handbook of Theories of Social Psychology: Volume One*, pp 438.

Ashforth, B. 1985. "Climate formation: Issues and extensions," *Academy of management review*, (10:4), pp 837–847.

Baskerville, R. L., Park, E., and Kim, J. 2014. "An emote opportunity model of computer abuse," *Information Technology & People*, (27.2), pp 1–31.

Bollen, K. A., and Stine, R. A. 1992. "Bootstrapping Goodness-of-Fit Measures in Structural Equation Models," *Sociological Methods & Research*, (21:2), pp 205–229 (doi: 10.1177/0049124192021002004).

Borgatti, S. P., Everett, M. G., and Johnson, J. C. 2013. *Analyzing Social Networks*, Sage Publications Ltd.

Brown, T. A. 2006. *Confirmatory Factor Analysis for Applied Research*, The Guilford Press.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of information security at the workplace: linking information security climate to compliant behavior," in *Perceptions of Information Privacy and Security*, (Vol. 1), pp 18–41.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security*, (39), Elsevier Ltd, pp 447–459.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2017a. "Applications of social network analysis in behavioural information security research: concepts and empirical analysis," *Computers & Security*, (68), Elsevier Ltd, pp 1–15 (doi: 10.1016/j.cose.2017.03.010).

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2017b. "Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace," *Information & Management*, (54:5), pp 625–637 (doi: 10.1016/j.im.2016.12.003).

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

French, J. R. P., and Raven, B. 1959. "The bases of social power," in *Studies in Social Power*, pp 150–167.

Goo, J., Yim, M., and 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), pp 1–24.

Ibarra, H., and Andrews, S. B. 1993. "Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions," *Administrative Science Quarterly*, (38:2), p. 277 (doi: 10.2307/2393414).

Ifinedo, P. 2014. "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Information and Management*, (51:1), Elsevier B.V., pp 69–79 (doi: 10.1016/j.im.2013.10.001).

Lowry, P. B., and Moody, G. D. 2013. "Explaining Opposing Compliance Motivations towards Organizational Information Security Policies," *2013 46th Hawaii International Conference on System Sciences*, Ieee, pp 2998–3007 (doi: 10.1109/HICSS.2013.5).

McKnight, D. H. 2002. "Developing and Validating Trust Measures for E-commerce: An Integrative Typology," *Information Systems Research*, (13:3), pp 334–359 (doi: 10.1287/isre.13.3.334.81).

McPherson, M., Smith-Lovin, L., and Cook, J. M. 2001. "Birds of a Feather: Homophily in Social Networks," *Annual Review of Sociology*, (27:2001), pp 415–444 (doi: 10.1146/annurev.soc.27.1.415).

Padayachee, K. 2012. "Taxonomy of compliant information security behavior," *Computers & Security*, (31:5), pp 673–680 (doi: http://dx.doi.org/10.1016/j.cose.2012.04.004).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *The Journal of applied psychology*, (88:5), pp 879–903 (doi: 10.1037/0021-9010.88.5.879).

Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. "When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse," *Journal of Information System Security*, (7:1), pp 24–47.

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

Ripley, R. M., Snijders, T. A. B., and Preciado, P. 2017. "Manual for RSiena," (available at http://www.stats.ox.ac.uk/~snijders/siena/RSiena_Manual.pdf).

Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, (91), pp 93–114.

Safa, N. S., Solms, R. Von, and Von Solms, R. 2016. "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, (57), Elsevier Ltd, pp 442–451 (doi: 10.1016/j.chb.2015.12.037).

Saint-Charles, J., and Mongeau, P. 2009. "Different relationships for coping with ambiguity and uncertainty in organizations," *Social Networks*, (31:1), pp 33–39 (doi: 10.1016/j.socnet.2008.09.001).

Schneider, B., and Reichers, A. 1983. "On the etiology of climates," *Personnel psychology*, (1934), pp 19–40.

Snijders, T. A. B., van de Bunt, G. G., and Steglich, C. E. G. 2010. "Introduction to stochastic actor-based models for network dynamics," *Social Networks*, (32:1), pp 44–60 (doi: 10.1016/j.socnet.2009.02.004).

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Information Management & Computer Security*, (22:1), pp 42–75 (doi: 10.1108/IMCS-08-2012-0045).

Steglich, C., Snijders, T. A. B., and Pearson, M. 2010. "Dynamic Networks And Behavior: Seperating Selection From Influence," *Sociological Methodology*, (8), pp 329–393 (doi: 10.1111/j.1467-9531.2010.01225.x).

Tichy, N. M., Tushman, M. L., and Fombrun, C. 1979. "Social Network Analysis for Organizations," *The Academy of Management Review*, (4:4), pp 507–519 (doi: 10.2307/257851).

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, (20:3), Nature Publishing Group, pp 267–284 (doi: 10.1057/ejis.2010.72).

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly*, (37:1), pp 1–20.