# Explaining the Development of Information Security Climate and an Information Security Support Network: A Longitudinal Social Network Analysis

**Duy Dang-Pham**
School of Science and Technology
RMIT Vietnam
School of Business IT and Logistics
RMIT University
duy.dangphamthien@rmit.edu.vn

**Karlheinz Kautz**
School of Business IT and Logistics
RMIT University

**Siddhi Pittayachawan**
School of Business IT and Logistics
RMIT University

**Vince Bruno**
School of Business IT and Logistics
RMIT University

## Abstract:

Behavioural information security (InfoSec) research has studied InfoSec at workplaces through the employees' perceptions of InfoSec climate, which is determined by observable InfoSec practices performed by their colleagues and direct supervisors. Prior studies have identified the antecedents of a positive InfoSec climate, in particular socialisation through the employees' discussions of InfoSec-related matters to explain the formation of InfoSec climate based on the employees' individual cognition. We conceptualise six forms of socialisation as six networks, which comprise employees' provisions of (1) work advice, (2) organisational updates, (3) personal advice, (4) trust for expertise, (5) InfoSec advice, and (6) InfoSec troubleshooting support. The adoption of a longitudinal social network analysis (SNA), called stochastic actor-oriented modelling (SAOM), enabled us to analyse the changes in the socialising patterns and the InfoSec climate perceptions over time. Consequently, this analysis explains the forming mechanisms of the employees' InfoSec climate perceptions as well as their socialising process in greater detail. Our findings in relation to the forming mechanisms of InfoSec-related socialisation and InfoSec climate, provide practical recommendations to improve organisational InfoSec. This includes identifying influential employees to diffuse InfoSec knowledge within a workplace. Additionally, this research proposes a novel approach for InfoSec behavioural research through the adoption of SNA methods to study InfoSec-related phenomena.

**Keywords**: behavioural information security; information security climate; information security management; social network analysis; stochastic actor-oriented modelling

# 1 Introduction

As organisations are rapidly adopting innovative technology and strategic information systems to support data-intensive operations, maintaining organisational information security (InfoSec) has become a priority. Technical InfoSec measures such as anti-virus software and firewalls are no longer sufficient for organisational InfoSec because of the increased targeting of organisational employees. Therefore, management must find effective ways to equip their employees with adequate InfoSec knowledge and skills. These managerial efforts help develop a secure workplace where employees are aware of their InfoSec duties and voluntarily perform InfoSec behaviours enabling adequate organisational InfoSec to be achieved.

There has been an emerging research theme in the behavioural InfoSec research field that focuses on the relationship between the work environment and the employees' InfoSec perceptions and behaviours. Willison and Warkentin (2013) extended the Security Action Cycle by adding 'pre-kinetic events' that were explained to result in the employees' negative perceptions of the workplace subsequently leading to InfoSec abuses. Baskerville, Park and Kim (2014) analysed the workplace's InfoSec vulnerabilities exploitable by potential perpetrators to commit InfoSec violations. To prevent insider threats and raise InfoSec awareness, situational support and peer-learning are critical for educating the employees about the skills and knowledge to comply with InfoSec directives (Warkentin, Johnston, & Shropshire, 2011). The active sharing of InfoSec advice among employees also reduces the time spent on re-inventing InfoSec solutions and enables efficient allocation of organisational resources to other InfoSec tasks of higher importance (Safa, Solms, & Von Solms, 2016). Negative perceptions of the workplace, exploitable vulnerabilities, situational and peer-learning support, and the sharing of Infosec advice among employees are some of the topics discussed in the research literature.

We argue that there are two critical issues concerning intra-organisational provisions of InfoSec resources such as InfoSec advice and troubleshooting support. They focus on: (1) the ways to provide these InfoSec resources and (2) the effectiveness of such provisions measured by improvements in the employees' InfoSec perceptions and behaviours. Recent research has primarily addressed the first issue by identifying the factors which facilitate the employees' sharing of InfoSec knowledge in the organisational context (Rocha Flores, Antonsen, & Ekstedt, 2014; Safa et al., 2016).

Measuring the effectiveness of the provisions of InfoSec resources is challenging, since it ideally requires a longitudinal design to observe improvements in the employees' and organisational InfoSec before and after such provisions. There have been a few action research projects which monitored InfoSec-related interventions and evaluated their impacts throughout the research process (see e.g., Puhakainen and Siponen 2010; Tsohou et al. 2013). However, these studies focus on the changes in the employees' individual perceptions and behaviours and overlook the changes in the InfoSec environment. Acquiring a comprehensive understanding about the social dynamics that constantly take place within a work environment, which entail how the employees' InfoSec perceptions shape their provisions of InfoSec resources and vice versa, can reveal opportunities to enhance the organisational InfoSec through manipulating features of the work environment. On this background, the objective of this research is to acquire such comprehensive understanding about the simultaneous formation of the employees' InfoSec perceptions and of the InfoSec environment conceptualised as a network of InfoSec support provisions between the employees.

We employed a longitudinal social network analysis (SNA) method, called stochastic actor-oriented modelling (SAOM) (Steglich, Snijders, & Pearson, 2010), to investigate the relationship between the employees' InfoSec perceptions and their socialisation in a large organisation before and after an InfoSec awareness program was implemented. We selected the SNA approach and SAOM method because it allowed a simultaneous analysis of both the individual factors (i.e., the employees' InfoSec perceptions) and environmental factors (i.e., the employees' socialisation and its structural features). We explored the concept of InfoSec climate (Chan, Woon, & Kankanhalli, 2005; Schneider & Reichers, 1983) and its forming process which was facilitated by the employees' socialisation (Ashforth, 1985; Weick, 1995). Unlike current studies which conceptualised socialisation as part of the employees' perceptions (see e.g., Chan et al., 2005; Goo, Yim, & Kim, 2014; Jaafar & Ajis, 2013), we analysed socialisation in the form of networks with network ties representing the actual provisions of work advice, organisational updates, trust for expertise, InfoSec advice and troubleshooting support among employees. Longitudinal data between two separate points in time were collected and analysed to reveal the changes in network ties and in climate perceptions over time.

We applied and present an original approach to study InfoSec-related phenomena, which employed SNA method to examine the networks of InfoSec-related interactions in conjunction with the individual employee's InfoSec perceptions. Through the analysis, we explored the socialising mechanisms brought about by these networks, which facilitated the formation of InfoSec climate perceptions, as well as the impacts of the networks on each other. Acquiring knowledge of these socialising mechanisms enables the identification of those employees influential in the InfoSec domain, who can assist management in raising organisational InfoSec awareness through their influence.

# 2 Conceptual Framework

In the following sections, we discuss the concepts of InfoSec climate and workplace socialisation. Then, we explain the relationship between these two concepts by consulting social influence theories. Based on this we propose a conceptual framework that describes the key mechanisms contributing to the formation of InfoSec climate within a workplace. This conceptual framework and the described mechanisms will be evaluated by the SAOM method.

## 2.1 InfoSec Climate Perceptions

InfoSec climate refers to the common and recognised practices in the workplace, defining how InfoSec is treated by the organisation (Lowry & Moody, 2013). The concept of InfoSec climate has been adopted by InfoSec researchers from the work safety climate literature. Chan et al. (2005) defined it as the employees' perceptions of the observed InfoSec environment, consisting of their colleagues and supervisors' InfoSec behaviours. InfoSec climate fosters and maintains InfoSec compliance and InfoSec culture (Chan et al., 2005), as well as promotes the provisions of InfoSec advice and troubleshooting support (Dang-Pham, Pittayachawan, & Bruno, 2017). The perceptions of the InfoSec climate, in this research, are defined as comprising of the employees' perceptions of colleagues and supervisors' InfoSec behaviours (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013). These perceptions indicate how InfoSec matters are treated and prioritised in the workplace (Lowry & Moody, 2013).

Dourish and Anderson (2006) discuss that InfoSec-related perceptions and behaviours have both individualistic and collective characteristics. In daily work, the employees' decisions to perform InfoSec behaviours are influenced by factors in the work environment (Padayachee, 2012; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Subjective norms, which refer to the pressure exerted by the people who appear important to a person, are confirmed across studies as an important contributing factor of both desirable and malicious InfoSec behaviours (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cheng, Li, Li, Holm, & Zhai, 2013; Guo & Yuan, 2012; Herath & Rao, 2009; Ifinedo, 2014; Lee & Lee, 2002). Subjective norms describe the shared patterns of thoughts and behaviours that can be constructed via communication (Hogg & Reid, 2006). Recent behavioural InfoSec research has investigated the sharing of InfoSec advice as a means to raise employees' InfoSec awareness (Rocha Flores et al., 2014; Safa et al., 2016; Warkentin et al., 2011), and such sharing was also found to create normative InfoSec behaviours such as risky InfoSec workarounds (Kirlappos, Parkin, & Sasse, 2014). This has led the research to the following discussion of the socialisation's impact on the formation of InfoSec climate perceptions.

## 2.2 Socialisation and the Formation of InfoSec Climate Perceptions

Socialisation refers to an employee's inclusion in a workplace through communication and provisions of organisational resources, which facilitate organisational learning and development of organisational climates (Morrison, 1993); such socialisation plays a major role in the formation of InfoSec climate by facilitating the sense-making activities among employees (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013) to reach a consensus on meanings (Ashforth, 1985; Schneider & Reichers, 1983; Weick, 1995). Socialisation in the forms of provisions of work advice and trust helps to reduce uncertainty, i.e., lack of information, and clarifies ambiguity, i.e., too many overlapping information, respectively (Saint-Charles & Mongeau, 2009). In the InfoSec context, the socialisation among employees, their colleagues and direct supervisors has been conceptualised as involving discussions about InfoSec-related matters (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013). The increased InfoSec-related socialisation of employees with their colleagues and supervisors raises awareness of the InfoSec practices employed by their organisation, which contributes to the development of an InfoSec climate (Chan et al., 2005).

The socialisation within a workplace can be conceptualised and studied in two different forms, either reflecting the individual's perceived level of socialisation or characterising the actual social interactions between pairs of employees. The former form has been the focus of previous InfoSec climate research (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013), whereas studies in the management and organisational behaviour disciplines have investigated workplace socialisation in the form of organisational networks (see e.g. Ibarra & Andrews, 1993; Saint-Charles & Mongeau, 2009).

Organisational networks can be categorised into instrumental and expressive interaction networks (Borgatti, Everett, & Johnson, 2013; Ibarra & Andrews, 1993; Saint-Charles & Mongeau, 2009). In line with our research context, we further add a third type of networks i.e., the InfoSec support network that comprises InfoSec-related interactions between the employees. We explain the three types of networks as follow.

*Instrumental networks* refer to the interactions and relationships that are related to work-role and work situations, and expressive networks are the links that concern emotional matters such as friendship and social support (Ibarra & Andrews, 1993; Saint-Charles & Mongeau, 2009). In line with these prior studies, we considered the employees' provision of work advice as part of the instrumental networks. Since performing InfoSec behaviours requires understanding relevant policies and directives, individuals who have first access to the latest organisational updates can be perceived as influential by other employees. The instrumental network in our study is thus defined as comprising the provisions of work advice and organisational updates.

Consistent with organisational network studies, the expressive networks in our research comprised the employees' provision of personal advice and trust. Interpersonal trust is multi-faceted, which involves trusting a person for their expertise and personal characteristics such as benevolence and integrity (McKnight, 2002; Mcknight & Chervany, 1996). While nominating a person capable of discussing personal matters indicates the nominator's trust in the person's perceived goodness, the 'trust for expertise' network consisting of nominated people who are trusted for expertise covers the other facet of trust. As a result, the expressive network in our study consists of the socialisation that facilitates the provision of personal advice and trust for expertise.

The *InfoSec support network* refers to the provisions of InfoSec advice and troubleshooting support among the employees. In the InfoSec context, the provision of InfoSec advice and troubleshooting support represent the socialisation which involves discussions about InfoSec matters that shape the employees' perceptions of InfoSec climate (Chan et al., 2005). The nomination as a person that is capable of providing InfoSec advice and troubleshooting support indicates that the nominee possesses expert power to influence other colleagues' InfoSec perceptions and behaviours (French & Raven, 1959).

In summary, our study is concerned with three types of organisational networks, namely the instrumental, expressive, and InfoSec support networks. These represent the different types of workplace socialisation that would form the employees' perceptions of InfoSec climate. In the next section, we discuss the two different mechanisms, i.e., selection and influence processes, to explain how employees would shape their InfoSec climate by socialising with their colleagues within the three aforementioned networks. These processes, together with the organisational networks, provide the conceptual framework that will be examined with the longitudinal SNA method.

## 2.3 Selection and Influence Processes

The formation of InfoSec climate is achieved when the employees reach a consensus on or institutionalise common perceptions of InfoSec climate through their socialisation. There are two possible explanations for that phenomenon. First, employees may deliberately select and socialise with those whom they see as possessing similar traits; this is also called the homophily effect (Borgatti et al., 2013; McPherson, Smith-Lovin, & Cook, 2001). On this basis, employees who have similar climate perceptions may already form ties and socialise with each other without changing perceptions, i.e., the influence process does not take place. Second, employees may institutionalise common InfoSec climate perceptions as a result of their socialisation, or in other words there is an influence process that makes the employees adjust their perceptions of InfoSec climate to match with those of their socialised partners. These two processes are referred to as selection and influence processes respectively (Steglich et al., 2010).

The relationship between selection and influence processes has been a recurring topic of debate and prominent explanation for social phenomena that involve collective behaviours and perceptions (Steglich et al., 2010). Understanding the impacts of selection and influence processes on a behaviour or perception offers some benefits. For instance, a confirmed effect of social influence on an InfoSec behaviour, e.g., InfoSec compliance or violation, would justify the implementation of interventions that aim to alter peers' behaviours to create contagious changes. In contrast, a confirmed selection effect would indicate that similar behaviours in the workplace are formed and maintained by the deliberate socialisation between employees of matching profiles. Therefore, to change those behaviours would require interventions that modify or remove the existing socialisation between people, rather than focusing on changing the behaviours per se (Dijkstra et al., 2010).

Prior studies on InfoSec climate (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013), which analysed the effect of socialisation on the employees' InfoSec climate perceptions, have overlooked the distinction between selection and influence processes. This is due to the traditional research approach that solely conceptualises the employees' socialisation as their perceptions and not in the form of networks. Consequently, it remains unclear how InfoSec climate perceptions can be influenced by the workplace socialisation, although the relationship between these two constructs has been confirmed by existing research.

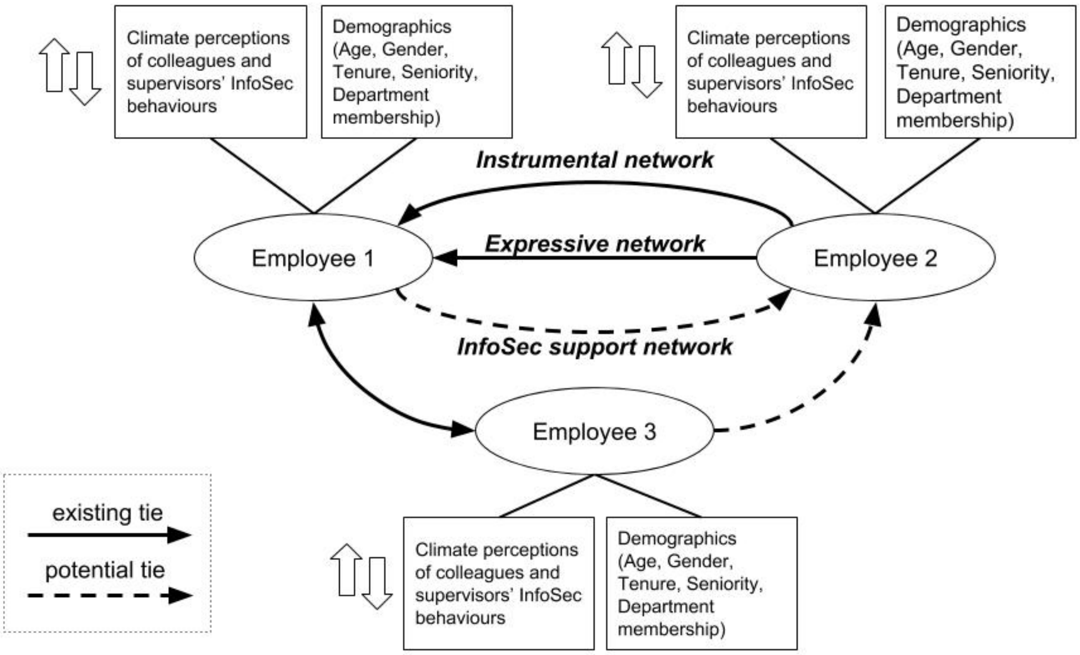

Climate perceptions of colleagues and supervisors' InfoSec behaviours
Demographics (Age, Gender, Tenure, Seniority, Department membership)
Climate perceptions of colleagues and supervisors' InfoSec behaviours
Demographics (Age, Gender, Tenure, Seniority, Department membership)
Instrumental network
Employee 1
Expressive network
Employee 2
InfoSec support network
Employee 3
existing tie
potential tie
Climate perceptions of colleagues and supervisors' InfoSec behaviours
Demographics (Age, Gender, Tenure, Seniority, Department membership)

*Figure 1. Conceptual framework*

Figure 1 presents the conceptual framework which summarises the key components in our research, i.e., the employees and their personal attributes, and the different network ties between them which represent their socialisation. The solid and dash lines represent existing and potential ties respectively, of which the latter is assumed to be the possible outcome of the former. Specifically, we assume that employees would socialise with their colleagues in a network, e.g., seeking InfoSec advice, if they are already socialising in another network, e.g., seeking work advice. It would be more likely for employees to prefer interacting with colleagues whom they trust and know their expertise well because of their previous interactions.

In line with the selection process described above, the occurrence of ties is also assumed to be motivated by employees who have certain demographics such as age and gender. The assumed effect of demographics on the employees' socialisation is consistent with social influence and homophily theories (French & Raven, 1959; Ibarra & Andrews, 1993; McPherson et al., 2001), which posit that employees who have certain traits (e.g., seniority, tenure) are perceived more influential, and that people purposely choose to interact with similar others (e.g., having the same gender or working in the same department).

Consistent with InfoSec climate studies (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013), the emphasis of our conceptual framework is on the impact of the InfoSec support network on the employees' InfoSec climate perceptions, particularly the perceptions of the InfoSec behaviours performed by their colleagues and direct supervisors. The up-and-down arrows next to the climate perceptions component in Figure 1 highlight our research interest that focuses on the changing patterns of such perceptions as a consequence of the employees providing and receiving InfoSec support to/from each other. In line with the selection process and homophily effect discussed above, we also assume that the likelihood for the employees to establish ties is affected by having different levels of climate perceptions, i.e., high or low perceptions.

# 3 Research Method

We employed a longitudinal SNA method called SAOM which simultaneously analyses the employees' perceptions of InfoSec climate and the patterns of socialisation in the form of networks. The SAOM method was developed especially for the purpose of detecting the selection and influence processes by separating them during the analysis (Steglich et al., 2010). The following sections discuss the research context, the variables which we included in the questionnaire to collect data, the data collection process, and the preparation for the SAOM analysis.

## 3.1 Research Context

We were approached by a large construction and manufacturing enterprise in Vietnam (anonymised as 'ABC') to provide advice and help improve their employees' InfoSec awareness. The study reported here is part of the research project we subsequently performed together with the organisation. ABC is one of the largest enterprises in Vietnam, which employed a total of 311 office staff and more than 800 workers who worked at the manufacturing facility, at the time when our research was conducted. The company's main services include designing, manufacturing and exporting high quality furniture, as well as delivering fitting projects for local and international clients. Due to the increased InfoSec violations that had occurred, ABC was motivated to improve the InfoSec environment by stimulating InfoSec-related interactions i.e., the sharing of InfoSec advice and troubleshooting support among the office staff.

The collaboration with ABC in this project on the diffusion of InfoSec knowledge provided a research opportunity to study the changing dynamics in an InfoSec environment. In line with the emerging theme of behavioural InfoSec in the literature, we advised ABC to instigate, measure and analyse the changes in the employees' InfoSec climate perceptions, which indicated the priority of InfoSec in the workplace, and the provisions of InfoSec resources between them by using SNA methods.

The adoption of SNA techniques to design and implement organisational changes, which includes making use of opinion leaders to diffuse new ideas, has been applied in prior studies (Cross, Laseter, Parker, & Guillermo, 2006; Valente, Palinkas, Czaja, Chu, & Brown, 2015).

Since ABC's objective was to increase the provisions of InfoSec resources among their employees, SNA methods offer the analytical capabilities to quantitatively evaluate the improvements in the networks representing such provisions. We identified a number of InfoSec champions and conducted small InfoSec training sessions for these champions, who were then tasked to diffuse InfoSec knowledge to other colleagues in ABC.

## 3.2 Variables

We organised the six forms of socialisation, the provisions of work advice, organisational updates, personal advice, trust for expertise, InfoSec advice and troubleshooting support in our study, into three types of networks: instrumental, expressive and InfoSec support. These networks represent the socialisation that facilitates sense-making activities and forms InfoSec climate perceptions. The questions for establishing these networks and their categories are summarised in Table 5 Appendix A.

We used two sets of questions adapted from studies on InfoSec climate (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013) to measure the employees' perceptions of their colleagues and direct supervisors' InfoSec behaviours, which describe their perceptions of InfoSec climate. We employed a seven-point scale to ask 10 questions about the level of InfoSec behaviours performed by the employees' colleagues and direct supervisors (see Table 6 Appendix A). We also included background characteristics of the employees as variables in our SAO model. The employees' demographics, namely age, gender, tenure (in years), seniority (operational, manager, and executive), champion status, and department membership were collected by an additional set of relevant questions.

## 3.3 Data Collection and Preparation

We collected our data in two waves by launching the same questionnaire twice. Data collection of wave 1 was performed before the diffusion of InfoSec knowledge took place, and wave 2 took place three months after the diffusion. The questionnaire had two sections; the first section captured the six networks of interest by asking the employees to nominate a maximum of seven colleagues who engaged with them in a network (refer to Table 5 Appendix A). They could nominate multiple colleagues who socialised with them in the different networks. The second section asked the employees to answer the Likert scale questions that measure their climate perceptions of colleagues and supervisors' InfoSec behaviours (Table 6 Appendix A).

Questionnaires designed to collect data about whole networks require identifiable information such as the respondents' real names, which can be a source of common method bias and affect the response rate since employees may not want to be identified and evaluated for their responses (Borgatti et al., 2013; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). To alleviate this issue, the top management of ABC published a memorandum of understanding that they will not access the identifiable data. We also explained to the employees in the questionnaire that their real names and nominations are collected for the purpose of mapping out the networks only. To further minimise common method bias, we mixed the order of questions so that they did not appear to measure the same constructs, as well as provided detailed definitions and examples to clarify potentially vague questions (Podsakoff et al., 2003).

Missing data is problematic for longitudinal research and can result in biased findings without proper treatment (Ripley, Snijders, & Preciado, 2011). 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). Our questionnaire was sent to 311 office staff employees of ABC in wave 1, which returned 264 responses, a response rate of 85 per cent. In wave 2, we collected 230 responses from a total of 288 employees, a response rate of 80 per cent. We trimmed the dataset by selecting only the employees who casted their nominations in both waves. This meant the exclusion of respondents who were only nominated in one of the two waves and of those who did not make any nominations, or casted their nominations only once in either wave 1 or wave 2. This resulted in a dataset consisting of 151 employees.

Performing SAOM analysis requires individuals' perceptions and behaviours to be represented by a single-item, composite variable in integer format (Ripley et al., 2011). In our study, this requirement also applies to the theoretical constructs of perceptions of InfoSec climate. We performed confirmatory factor analysis (Brown, 2006) to fit measurement models for the InfoSec climate perceptions of colleagues ('COL' model) and supervisors' InfoSec behaviours ('SUP' model). 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 used the Bollen-Stine bootstrapping method (Bollen & Stine, 1992) to evaluate whether the model was specified correctly and achieved adequate goodness-of-fit. Both models exhibited acceptable goodness-of-fit with Bollen-Stine bootstrap p-values equal to 0.357 (COL model) and 0.669 (SUP model). Table 1 further shows that there were no issues with convergent validity, except the removal of one item, SUP5 due to its loadings at below the ±0.35 threshold (Lewis, Templeton, & Byrd, 2005). These results supported the theoretical structure of the two constructs describing the employees' perceptions of InfoSec climate.

| 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 1. Convergent validity (W1=wave 1; W2=wave 2)*

Factor score weights from the fitted models were used to calculate composite scores of the latent constructs by calculating the sum products of these weights and the employees' responses. Next, we rounded the calculated composite scores to integers to meet the data requirement of SAOM method.

## 3.4 Strategy of SAOM Analysis

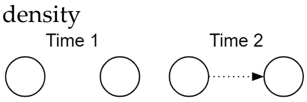
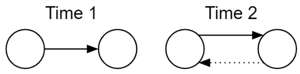
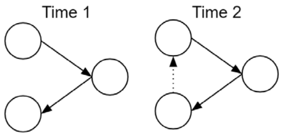
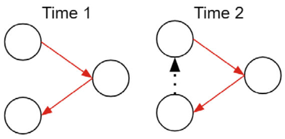
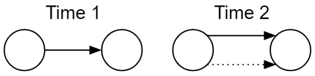
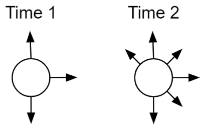
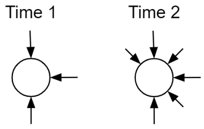
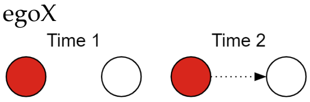
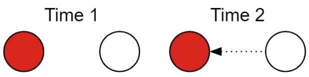
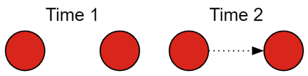
We specified and estimated a stochastic actor-oriented (SAO) model by using the R statistical package called 'RSiena' (Ripley et al., 2011) to examine the conceptual framework shown in Figure 1. Snijders et al. (2010) provide a comprehensive and detailed introduction featuring the SAOM method, which involves specifying a mathematical model (i.e., the SAO model) with parameters which describe the simultaneous changes in the employees' selection patterns, 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. The mechanisms of these changes are then evaluated by using the Markov chain Monte Carlo (MCMC) approach (Dijkstra et al., 2010; Ripley et al., 2011).

Since this research did not formulate hypotheses and proposed a conceptual framework instead of a theoretical model, its approach is exploratory in nature. The SAO model specified and subsequently evaluated a large body of 109 parameters which described the possible forming mechanisms of the networks and InfoSec climate perceptions in accordance to the conceptual framework in Figure 1. The 109 parameters are outlined as follows and elaborated on in Appendix B.

Each of the three networks had six parameters included in the SAO model. These 18 parameters describe the structural changes, such as the density of the network or the tendency of the nodes to reciprocate ties over time. In relation to the conceptual framework in Figure 1, we were interested in exploring the impacts of the networks on each other. We specified in our SAO model nine parameters to evaluate the mutual impacts between pairs of networks, i.e., between instrumental and expressive networks, instrumental and InfoSec support networks, and expressive and InfoSec support networks.

There are eight attributes of the employees, namely (1) age, (2) gender, (3) tenure, (4) seniority, (5) department membership, (6) champion status, and climate perceptions of (7) colleagues and (8) supervisors' InfoSec behaviours, each of which is assumed to impact on the formation of the networks in three different ways. Three different parameters can be used to model the tendency of nodes to send or receive ties, especially when the sender or receiver have a high score for an attribute, e.g., older age, higher tenure or seniority, or when the sender and receiver have similar attributes. In the latter case, having similar attributes can be an exact match, e.g., same gender or same department membership, or approximate match, e.g., small age gap or tenure gap, which are described by another two parameters. A total of 66 parameters were included in the SAO model to specify the individual attributes' effects on network formation.

To describe the impacts of the InfoSec network on the formation of two types of climate perceptions, two parameters were included in the SAO model. Four parameters were included in the model to describe the changing patterns of the two types of climate perceptions over time. The impacts of the five individual attributes, namely age, gender, tenure, seniority, and champion status, on the development of two types of climate perceptions were modelled with 10 parameters. Consequently, a total of 16 parameters were included to describe the formation process of the employees' climate perceptions. Table 2 summarises the parameters that were included in the SAO model to describe the changes in the networks and in the employees' climate perceptions.

| Parameter | Description | Number of parameters | Variables |
|---|---|---|---|
| rate | The number of model-based simulated opportunities for the nodes to add, remove or keep their ties between the two data collection waves | 3 networks | Instrumental network, Expressive network, InfoSec support network |
| density  | The node's tendency to establish ties | 3 networks | |
| reciprocity  | The node's tendency to reciprocate or return ties | 3 networks | |
| gwespFF  | The node's tendency to close a triad, by sending a direct tie to another indirectly connected node | 3 networks | |
| gwespFBMix  | The node's tendency to close a triad, by sending a direct tie to another node that is indirectly connected by a different type of tie | 3 networks | |
| crprod  | The tendency of different types of ties to co-occur | 6 (i.e., six pairs) | |
| outActSqrt  | The tendency of a node to keep sending ties to other nodes, when that node already has many outgoing ties | 3 networks | |
| inPopSqrt  | The tendency of a node to keep receiving ties from other nodes, when that node already has many incoming ties | 3 networks | |
| egoX  | The tendency of a node to send ties to other nodes, when that node has a high score for an attribute | 21 (7 attributes x 3 networks) | Age, Gender, Tenure, Seniority, Champion status, COL, SUP |
| altX  | The tendency of a node to receive ties from other nodes, when that node has a high score for an attribute | 21 (7 attributes x 3 networks) | |
| sameX  | The tendency of two nodes to establish a tie when they have the same attribute (categorical data) | 12 (4 attributes x 3 networks) | Gender, Seniority, Department membership, Champion status |

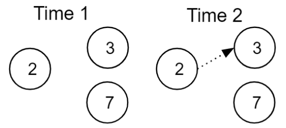
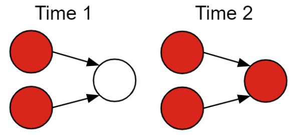
| Parameter | Description | Number of parameters | Variables |
|---|---|---|---|
| simX  | The tendency of two nodes to establish a tie when they have the same attribute (continuous data) | 12 (4 attributes x 3 networks) | Age, Tenure, COL, SUP |
| totSimW  | The tendency of nodes to change their individual attribute in accordance to their connected nodes who have attribute *W*.<br>In this research, this parameter evaluates the tendency of employees (as nodes) to change their climate perceptions, to match with those of the connected colleagues who have the same department membership (as attribute *W*) | 2 perceptions | InfoSec support network, Department membership, COL, SUP |
| linear shape | The tendency of climate perceptions to increase or decrease over time in a linear fashion | 2 perceptions | COL, SUP |
| quadratic shape | The tendency of climate perceptions to self-adjust to a higher/lower level when the current score is too low/high | 2 perceptions | |
| effFrom | The effect of an individual attribute on climate perceptions | 10 (5 attributes x 2 perceptions) | Age, Gender, Tenure, Seniority, Champion status, COL, SUP |
| **TOTAL** | | 109 | |
| **Key:** COL = Climate perception of colleagues' InfoSec behaviours; SUP = Climate perception of supervisors' InfoSec behaviours | | | |

*Table 2. Parameters included in the SAO model*

# 4 Analysis and Findings

The results of the SAOM analysis identified 36 parameters that achieved statistical significance, out of the 109 parameters included in the SAO model. We present these parameters' effects in the following sections; the statistical results concerning the effects which are captured by these parameters are reported in Appendix C.

## 4.1 Structural Changes in the Networks

The parameter *rate* presents the mode-based, simulated number of opportunities for changing ties per actor in a network between the two points in time (Ripley et al., 2011). The SAOM method simulates a series of mini-steps in such a period, based on characteristics of the empirical network, where the actors can add, remove, or maintain their ties in each mini-step. The InfoSec support network had the highest number of change opportunities, followed by the expressive and instrumental networks. This result shows that the diffusion of InfoSec knowledge had effectively stimulated the employees' sharing of InfoSec advice and troubleshooting support. The stability of the expressive and instrumental networks indicates that the normal work routines at ABC, as represented by the provisions of work and personal advice, remained unchanged.

The outdegree effect for the instrumental, expressive and InfoSec support networks achieved statistical significance with negative values, indicating that these networks were sparse. Network ties rarely occurred between employees, although more InfoSec support network ties were created over time. The *reciprocity* parameter, which describes the employees' tendency to reciprocate ties, only achieved statistical significance for the instrumental and expressive networks but not for the InfoSec support network. The odds ratios–which indicates the likelihood of a phenomenon appearing–of the *reciprocity* parameters for instrumental and expressive networks were 2.3 ($e^{0.84}$) and 4.7 ($e^{1.55}$) respectively. This means that work advice and organisational updates were reciprocated 2.3 times more than only being unidirectional, and 4.7 times more likely for the network of provisions for personal advice and trust for expertise.

Network transitivity is represented through transitive closure which describes the tendency of a network actor to close their triads formed with two other actors, by establishing a direct connection with an actor who is indirectly connected via multiple intermediaries. Our results, obtained through the positive estimate of the parameter *gwespFF* (see Appendix B for the details of the parameter's meaning) indicated that the instrumental and expressive networks were transitive, whereas the InfoSec support network was not. In the InfoSec support network, sharing the same providers of InfoSec support did not create new interactions, which was consistent with the sparse and thin nature of this network.

## 4.2 Forming Mechanisms of Socialisation

For each of the background characteristics such as gender, age, and tenure, we evaluated parameters that described the socialising tendency of the senders, receivers and matching partners. Evaluating the effects expressed by these parameters helps to determine the factors that influence the employees' socialising choices in the instrumental, expressive and InfoSec support networks. For instance, we evaluated the tendency for male and female employees to seek work advice from their colleagues, and the tendency for employees who worked in the same department to seek InfoSec support from each other.

Gender was found to influence the employees' decisions to seek work advice or organisational updates from their colleagues. We found that female employees tend to be sought more for instrumental resources compared to male employees; in addition, employees of the same gender tended to seek work advice and organisational updates from each other more. Gender also determined whom the employees would trust for expertise, with female employees attracting more trust nominations by other employees than male employees. Similarly, employees tended to trust colleagues of the same gender. In contrast, gender did not explain the patterns of seeking InfoSec support.

With regard to the employees' age, older employees tended to be sought for work advice and organisational support more, whereas younger employees were more likely to be sought for InfoSec support. Seniority also played a role for increasing the employees' received nominations in the instrumental network. We found that employees who held senior positions were nominated more to provide work advice and organisational updates. Likewise, the provision of these instrumental resources occurred more between those having the same seniority. Sharing the same department membership increased the employees' nominations in the three networks. Further, employees who served as InfoSec champions were 1.7 times more likely than non-champions to be sought for InfoSec support (with an odd ratio of $e^{0.55}$).

As our research objective was to detect the influence effect through separating selection and influence mechanisms, we included parameters that evaluated the employees' tendency to socialise with those who were perceived to hold similar InfoSec climate perceptions. The results of these parameters did not achieve statistical significance. The insignificant results of these parameters indicated that the employees' decision to socialise with other colleagues in the instrumental, expressive, and InfoSec support networks was not affected by having similar InfoSec climate perceptions.

We detected that the three types of socialisation co-occurred with each other. The employees' selection of colleagues to socialise with in one network influenced their socialising choice in other networks. The instrumental and expressive networks tended to co-occur with each other, indicating that employees were more likely to seek work advice and organisational updates from those whom they trusted and sought personal advice from, and vice versa. Similarly, InfoSec support ties co-occurred with instrumental and expressive ties, in which the co-occurrence between InfoSec support and instrumental networks had a higher likelihood. This means that employees sought InfoSec support from colleagues who also provided instrumental and expressive resources to them.

The instrumental and expressive networks exhibited different patterns of co-occurrence with the InfoSec support network which are shown in the results of their parameter *gwespFBMix* (see Appendices B and C for the details of the meaning and results of this parameter). The found negative estimate of –0.62 implies that employees were less inclined to seek InfoSec support from those colleagues with whom they shared the same trusted people. An explanation for this intriguing phenomenon was that employees who shared personal matters with the same trusted people might prefer to avoid interacting with each other. Consistent with the belief that knowledge represents power, resource seekers might minimise the possibility that their trusted contacts would know about their ignorance or dependence on others, by avoiding seeking resources from people who are close to their trusted contacts. In contrast, the positive effect of the same *gwespFBMix* parameter for the instrumental network suggested that employees who shared common providers of work advice were more likely to seek InfoSec support from each other. Since employees who sought work advice from the same people had a high chance of working in similar job roles, this result might reflect the employees' need to discuss relevant InfoSec-related matters with those who shared the same work duties. Table 3 summarises the SAOM findings about the selection process, i.e., formation of the instrumental, expressive, and InfoSec support networks.

| | **Formation mechanisms** |
|---|---|
| **Formation of instrumental network** | Employees tended to seek work advice and organisational updates from:<br>• Female employees or those of the same gender<br>• Older employees<br>• Employees who held more senior positions or those having the same seniority<br>• Employees who worked in the same department<br>• Employees who gave personal advice to or trusted them for expertise |
| **Formation of expressive network** | Employees tended to seek personal advice from or trust the expertise of:<br>• Female employees or those of the same gender<br>• Employees who worked in the same department<br>• Employees who gave work advice or organisational updates to them |
| **Formation of InfoSec support network** | Employees tended to seek InfoSec advice and troubleshooting support from:<br>• Younger employees<br>• Employees who worked in the same department<br>• InfoSec champions<br>• Employees who gave work advice or organisational updates to them<br>• Employees who gave personal advice to or trusted them for expertise<br>• Employees who received work advice and organisational updates from the same people<br>Employees tended to not seek InfoSec advice and troubleshooting support from:<br>• Employees who shared the same trusted people |

*Table 3. SAOM findings about selection process, i.e., formation of networks*

## 4.3 Forming Mechanisms of Infosec Climate

To understand the forming mechanisms of InfoSec climate which were caused by the influence process, we investigated how the employees' InfoSec climate perceptions had changed over time under other factors' effects. The SAOM results show that none of the background characteristics had an effect on the formation of the employees' perceptions of InfoSec climate.

Since we calculated the scores for InfoSec climate perceptions of each employee, which ranged from 1 (non-visible climate) to 5 (highly visible climate), we were interested in examining the variation of those scores. The SAOM result showed a positive and statistically significant effect of the *linear shape* parameter (see Appendix B for details of this parameter) for the climate perception of direct supervisors' InfoSec behaviours, which indicated that the scores of these perceptions tended to increase over time. It means that the general perceptions of direct supervisors' InfoSec behaviours became more favourable after the diffusion of InfoSec knowledge by the champions.

The negative effects of the *quadratic shape* parameter (see Appendix B for details of this parameter) for both types of climate perceptions suggested that the scores of these perceptions would be more likely to become low when they are high and vice versa. Moreover, these scores tended to deviate around the average point rather than around the polarising ends which reflect a climate that is too non-visible or too visible. These results suggested that the employees in ABC tended to adjust the level of their climate perceptions according to the majority of employees in the workplace.

It is worth mentioning that the effects of social influence were tested differently compared to the other effects by using the score-type test. This test is recommended when there is a parameter producing an estimated value with an unusually large standard error, which suggests the result is unstable and the default estimation procedure is unsuitable for the parameter (Ripley et al., 2011). By performing the score-type test, we observed a positive and significant one-sided test statistic of 3.0477 (with a Chi-square value of 9.2887 and a $p$-value of 0.0023) for the influence effect on the climate perceptions of colleagues' InfoSec behaviours. This result suggested that employees were inclined to adjust climate perceptions of colleagues' InfoSec behaviours to match with those of their colleagues in the same department, whom they had nominated as capable of providing them with InfoSec support. The result also indicated that there were no clear patterns about the change in the employees' climate perception of their direct supervisors' InfoSec behaviours, caused by the influence exerted by their colleagues who provided InfoSec support to them. Table 4 summarises the influence process, i.e., formation of the employees' climate perceptions.

| | **Formation mechanisms** |
|---|---|
| **Climate perceptions of colleagues' InfoSec behaviours** | • Self-adjusted to become more/less favourable when being too little/too much favourable<br>• Self-adjusted to match with the perceptions of the employees who gave InfoSec advice and troubleshooting support |
| **Climate perceptions of direct supervisors' InfoSec behaviours** | • Became more favourable over time<br>• Self-adjusted to become more/less favourable when being too little/too much favourable |

*Table 4. SAOM findings about influence process, i.e., formation of climate perceptions*

# 5 Discussion

The primary objective of this research was to seek a comprehensive understanding of the simultaneous formation of the employees' InfoSec perceptions and the InfoSec support provisions, which represents the InfoSec-related socialisation. Prior behavioural InfoSec research has explained the formation of InfoSec climate as an outcome of the employees' socialisation, with socialisation facilitating discussions on InfoSec-related matters which as a consequence raises the employees' awareness of the shared InfoSec practices in their workplace (Ashforth, 1985; Chan et al., 2005; Schneider & Reichers, 1983; Weick, 1995). Our findings indicate that employees tended to match their perceptions of colleagues' InfoSec behaviours with those of their colleagues, who provided them with InfoSec support, and supported the findings of those prior studies. By analysing not only the changes in the employees' InfoSec climate perceptions but also their socialisation in the form of networks, we further propose practical ways for organisations to facilitate positive improvements in their InfoSec climates through manipulating and exploiting the employees' socialisation.

## 5.1 Forming Mechanisms of InfoSec Perceptions and InfoSec Support Provisions

Our results established that the employees' provisions of InfoSec support, which facilitated the social influence that shaped InfoSec climate, were affected by the employees' sharing of department membership, similar ages and provisions of work-related resources and personal support. Consistent with these results, we advise to stimulate the employees' provisions of InfoSec support to develop a positive InfoSec climate, by devising strategies to exploit the employees' background characteristics and interactions.

One recommended strategy is to identify employees who are influential in the InfoSec domain in their department, based on their activeness in providing work advice, organisational updates and personal support to other employees. Managers can ask employees to nominate their local champions, and SNA tools can help identify these champions through network visualisations which depict the employees' provisions of resources. The identified forming mechanisms of the instrumental and expressive networks provide additional cues to facilitate the provisions of these resources, which indirectly contribute to a positive InfoSec climate via stimulating the provisions of InfoSec support.

In determining the employees' personal attributes, e.g., gender, age, seniority, and socialisation, e.g., providing work and personal advice, that impacted on their provisions of InfoSec support, we contribute to the research area of selecting InfoSec champions for organisational InfoSec programs where empirical studies are scarce. InfoSec managers can use the findings of this study as cues to identify the employees who actively provide their colleagues with InfoSec support, and consider training these employees or appointing them to be InfoSec champions. In addition, the rotating of InfoSec champions across different departments may be an effective way to provide employees with new perspectives and knowledge about InfoSec.

## 5.2 Methodological Contributions to InfoSec Research

We demonstrate through this study the use of the SAOM method for simultaneously analysing perceptions of InfoSec climate, as a personal attribute of individuals, and the interactions that take place between these individuals. This SAOM method and the SNA approach greatly complement the traditional approach employed by many behavioural InfoSec research studies, which solely focus on the individuals' personal and cognitive attributes. This limitation is evident in the research area of InfoSec climate, where prior studies only detected employees to develop positive climate perceptions by perceiving the ongoing socialisation but not considering the actual InfoSec support communicated via such socialisation (see e.g., Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013). This same argument also applies to other behavioural InfoSec studies which have examined the provisions of InfoSec support as products of the employees' cognition such as perceptions and attitudes, but not within the network that are formed through the acts of sending and receiving InfoSec support (see e.g., Safa et al., 2016; Warkentin et al., 2011). The adoption of SNA methods enables researchers to explore both the factors which trigger the individuals' decisions to initiate or accept InfoSec-related interactions, as well as the attributes of these interactions such as their intensity and type of content. We suggest further some applications of SNA methods in the behavioural InfoSec field.

Behavioural InfoSec researchers may apply SNA methods to investigate the impacts of networks on various InfoSec perceptions and behaviours provided by theories in the field. The literature reviews conducted by Padayachee (2012), Sommestad et al. (2014) and Warkentin and Mutchler (2014) have identified theoretical variables of prominent theories such as protection motivation theory (Rogers, 1975), theory of planned behaviour (Ajzen, 2011) and general deterrence theory (Straub & Welke, 1998); some of these variables have been consistently found to motivate InfoSec compliance and deter potential InfoSec violations. Researchers can perform SNA to evaluate the impacts of employees' interactions on the important drivers of InfoSec compliance, such as attitude toward InfoSec, subjective norms, perceptions of cyber-threats and severity of InfoSec sanctions. We anticipate that the outcomes of such SNA will help organisations to develop desirable InfoSec-related perceptions that lead to InfoSec compliance, while research findings about InfoSec-related networks can extend theories by providing knowledge of InfoSec processes. Similarly, organisations can benefit from research which analyses organisational networks to deter InfoSec violations and mitigate negative perceptions such as disgruntlement or perceived organisational injustice (Willison & Warkentin, 2013).

## 5.3 Directions for Future Research

This research was conducted in Vietnam, thus it is likely that the formation of the examined networks and the social influences facilitated by the employees' interactions were influenced by the Vietnamese culture. For instance, Vietnam is considered as a collectivistic society that has large power distance and prefers flexibility and relaxing work environment (Hofstede, 2001). Such environment is conducive to social influence, since it fosters the formation of privileged groups and emphasises the development of strong relationships and consensus between people (Hofstede, 2001). Consequently, the employees at ABC might have sought InfoSec support from or changed their InfoSec climate perceptions by accepting the social influence of the colleagues whom they wanted to establish effective work relationships with. In fact, our SAOM findings in relation to the self-adjustment tendency of the employees' climate perceptions of the direct supervisors' InfoSec behaviours is consistent with the collectivistic nature of the Vietnamese culture. People who embrace cultures that have large power distance tend to accept a hierarchical order (Hofstede, 2001). Interestingly, our SAOM findings indicate that the employees tended to seek their senior colleagues for work advice and organisational updates, but not for InfoSec support. The analysis also confirmed the positive impact of seniority on the formation of InfoSec support network. However, these effects were overshadowed by the effects of other factors such as the employees' department membership, age, and champion status. It is also worth noting that there are various cultural frameworks describing the dimensions of national cultures (see e.g., Trompenaars' (Trompenaars & Hampden-Turner, 2012) model of national culture), and that the unique organisational culture of each workplace may have an impact on the employees' InfoSec perceptions and behaviours (see e.g., Padayachee, 2012; Ruighaver, Maynard, & Chang, 2007). In relation to the cultural dimensions, we invite future researches to further investigate the impacts of national and organisational cultures on the formation of InfoSec support network and of InfoSec climate perceptions.

SNA methods can also support action research projects by providing the means to design interventions and quantitatively evaluate their outcome with network metrics. Action research studies hold important implications in the behavioural InfoSec field since their findings can determine the solutions that work and explain why they work, through evaluating theoretically-based interventions in a real context (Puhakainen & Siponen, 2010). Researchers outside of the behavioural InfoSec field have designed and implemented network-based interventions that induced practical organisational changes, including the use of opinion leaders to diffuse novel ideas, segmenting individuals into groups and delivering tailored training programs (see e.g., Borgatti & Cross, 2003; Hatala & Fleming, 2007; Valente, 2012). Provided the available tools and strategies to formulate network-based interventions, behavioural InfoSec researchers are encouraged to not only stop at analysing the impacts of networks on the employees' InfoSec perceptions and behaviours, but also evaluate the potential of network-based interventions for creating transformational changes in organisational InfoSec. For example, practical measures that reflect adequate organisational

InfoSec, which result from effective network-based interventions, may include the number of detected InfoSec violations or the employees' scores for InfoSec awareness tests. Since an improved InfoSec-related network implies an elevated level of sharing InfoSec resources among employees, it is reasonable to expect that the organisation having such a network will realise those positive outcomes.

# 6 Conclusions

Current behavioural InfoSec studies have emphasised the importance of investigating the impacts of human factors on organisational InfoSec, since acquiring the knowledge of these impacts is critical for formulating effective strategies and measures for achieving InfoSec success. Nevertheless, current research has predominantly focused on the employees' cognition and psychological attributes which influence their InfoSec perceptions and behaviours, while overlooking their interactions and relationships. Consequently, important insights for designing and implementing InfoSec improvements such as why employees seek or provide InfoSec support, as well as the unique structures of the networks reflecting different InfoSec workplaces, are unavailable to make informed decisions. The adoption of SNA methods enables researchers to comprehensively analyse InfoSec environments, comprising both the employees' personal attributes and their InfoSec-relevant interactions conceptualised in the form of networks.

Our research employed a longitudinal SNA method called SAOM to examine the formation mechanisms of a network characterising the employees' provisions of InfoSec support. The SAOM analysis also explained the formation of their InfoSec climate perceptions. The SAOM analysis identified the employees' sharing of department membership and gender, small age gap, and seniority as indicators for the longitudinal changes in their provisions of instrumental and expressive resources and InfoSec support. The provisions of work advice and organisational updates, personal support and trust for expertise were found to increase the sharing of InfoSec advice and troubleshooting support that developed a shared InfoSec climate. Specifically, the employees tended to match their climate perceptions of colleagues' InfoSec behaviours with those of their colleagues who provided them with InfoSec support, whereas climate perceptions of direct supervisors' InfoSec behaviours were unaffected. We offer practical recommendations to organisations to develop a positive InfoSec climate based on our research findings, while looking forward to future adoption of SNA methods to extend theoretical knowledge of the behavioural InfoSec field.

# References

Ajzen, I. (2011). Theory of planned behavior. In *Handbook of Theories of Social Psychology: Volume One* (p. 438).

Ashforth, B. (1985). Climate formation: Issues and extensions. *Academy of Management Review, 10*(4), 837–847.

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

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

Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science*, *49*(4), 432–445. https://doi.org/10.1287/mnsc.49.4.432.14428

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

Brondino, M., Pasini, M., & Costa, S. (2013). Development and validation of an Integrated Organizational Safety Climate Questionnaire with multilevel confirmatory factor analysis. *Quality & Quantity*, *47*, 2191–2223. https://doi.org/10.1007/s11135-011-9651-6

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study on rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

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* (Vol. 1, pp. 18–41).

Cheng, L., Li, Y., Li, W., Holm, E., & 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*, 447–459. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S0167404813001387

Cross, R., Laseter, T., Parker, A., & Guillermo, V. (2006). Using Social Network Analysis to Improve Communities of Practice. *California Management Review*, *49*(1), 32–62.

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

DeLay, D., Zhang, L., Hanish, L. D., Miller, C. F., Fabes, R. A., Martin, C. L., … Updegraff, K. A. (2016). Peer Influence on Academic Performance: A Social Network Analysis of Social-Emotional Intervention Effects. *Prevention Science*, 1–11. https://doi.org/10.1007/s11121-016-0678-8

Dijkstra, J. K., Lindenberg, S., Veenstra, R., Steglich, C., Isaacs, J., Card, N. A., & Hodges, E. V. E. (2010). Influence and selection processes in weapon carrying during adolescence: The roles of status, aggression, and vulnerability. *Criminology*, *48*(1), 187–220. https://doi.org/10.1111/j.1745-9125.2010.00183.x

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

French, J. R. P., & Raven, B. (1959). The bases of social power. In *Studies in Social Power* (pp. 150–167).

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.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, *49*(6), 320–326. https://doi.org/http://dx.doi.org/10.1016/j.im.2012.08.001

Hatala, J.-P., & Fleming, P. R. (2007). Making Transfer Climate Visible: Utilizing Social Network Analysis to Facilitate the Transfer of Training. *Human Resource Development Review*, *6*(1), 33–63. https://doi.org/10.1177/1534484306297116

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.

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations* (Second). Thousand Oaks CA: Sage Publications.

Hogg, M. a., & Reid, S. a. (2006). Social Identity, Self-Categorization, and the Communication of Group Norms. *Communication Theory*, *16*(1), 7–30. https://doi.org/10.1111/j.1468-2885.2006.00003.x

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. https://doi.org/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), 69–79. https://doi.org/10.1016/j.im.2013.10.001

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.

Kines, P., Lappalainen, J., Lyngby, K., Olsen, E., Pousette, A., Tharaldsen, J., … Törner, M. (2011). Nordic Safety Climate Questionnaire (NOSACQ-50): A new tool for diagnosing occupational safety climate. *International Journal of Industrial Ergonomics*, *41*(6), 634–646. https://doi.org/10.1016/j.ergon.2011.08.004

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security. In *USEC'14 Workshop on Usable Security*.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63. https://doi.org/10.1108/09685220210424104

Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems*, *14*(4), 388–400.

Lingard, H. C., Cooke, T., & Blismas, N. (2009). Group-level safety climate in the Australian construction industry: within-group homogeneity and between-group differences in road construction and maintenance. *Construction Management and Economics ISSN:*, *27*(4), 419–432. https://doi.org/10.1080/01446190902822971

Lowry, P. B., & Moody, G. D. (2013). Explaining Opposing Compliance Motivations towards Organizational Information Security Policies. *2013 46th Hawaii International Conference on System Sciences*, 2998–3007. https://doi.org/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), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Mcknight, D. H., & Chervany, N. L. (1996). The meanings of trust. *Measurement*, *55455*(612), 86. https://doi.org/10.1117/12.304574

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

Morrison, E. W. (1993). Newcomer Information Seeking: Exploring Types, Modes, Sources, and Outcomes. *Academy of Management Journal*, *36*(3), 557–589.

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

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & 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), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

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

Ripley, R. M., Snijders, T. A. B., & Preciado, P. (2011). Manual for RSIENA. *University of Oxford, Department of Statistics, Nuffield College*, *1*.

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

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

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

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

Schneider, B., & Reichers, A. (1983). On the etiology of climates. *Personnel Psychology*, (1934), 19–40.

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

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

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

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. https://doi.org/10.2307/249551

Trompenaars, F., & Charles Hampden-Turner, C. (2012). *Riding the Waves of Culture: Understanding Diversity in Global Business* (3.ed). New York: McGraw-Hill.

Tsohou, A., Karyda, M., Kokalakis, S., & Kiontouzis, E. (2013). Managing the Introduction of Information Security Awareness Programmes in Organisations. *European Journal of Information Systems*, *24*(1), 1–21. https://doi.org/10.1057/ejis.2013.27

Valente, T. W. (2012). Network Interventions. *Science*, *337*(6090), 49–53. https://doi.org/10.1126/science.1217330

Valente, T. W., Palinkas, L. A., Czaja, S., Chu, K.-H., & Brown, C. H. (2015). Social Network Analysis for Program Implementation. *Plos One*, *10*(6), e0131712. https://doi.org/10.1371/journal.pone.0131712

Warkentin, M., Johnston, A. C., & 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), 267–284. https://doi.org/10.1057/ejis.2010.72

Warkentin, M., & Mutchler, L. (2014). Behavioral Information Security Management. In G. Tucker & D.-H. Topi (Eds.), *Computing Handbook* (3rd ed., pp. 1–14). Taylor & Francis Group.

Weick, K. E. (1995). *Sensemaking in Organizations*. Thousand Oaks, CA: Sage Publications.

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

Zohar, D., & Luria, G. (2005). A Multilevel Model of Safety Climate: Cross-Level Relationships Between Organization and Group-Level Climates. *Journal of Applied Psychology*, *90*(4), 616–628. https://doi.org/10.1037/0021-9010.90.4.616

# Appendices

## APPENDIX A: SURVEY QUESTIONS

| Category | Network | Question |
|---|---|---|
| Instrumental | 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 that are happening or coming in ABC? |
| Expressive | Seek personal advice | When you want to discuss or ask for advice about personal life issues, whom would you talk to? |
| | Trust for 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? |
| InfoSec support | Seek InfoSec advice | Who would explain the importance of InfoSec to you, and/or teach you how to perform security behaviours, and/or use security technologies? |
| | Seek InfoSec troubleshooting support | When you encountered a security problem e.g. lost or damaged data, computer virus infection etc., whom would you seek help from? |
| **Note:** employees may nominate a maximum of seven colleagues per question. | | |

**Table 1. Network questions**

| Construct | Question (Item) | Scale | Adapted sources |
|---|---|---|---|
| Perception of direct supervisor's InfoSec behaviours (SUP) | How frequently do your direct supervisor(s) mention InfoSec matters to you and your co-workers? (SUP1) | Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always | Chan et al. (2005); Goo et al. (2014); Jaafar and Ajis (2013) |
| | How much do your direct supervisor(s) ask that you and your co-workers in the work unit must perform InfoSec behaviours? (SUP2) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Kines et al. (2011); Zohar and Luria (2005) |
| | How frequently do your direct supervisor(s) discuss InfoSec threats with you and your co-workers? (SUP3) | Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always | |
| | How serious, strict, or careful are your direct supervisor(s) when it comes to protecting InfoSec? (SUP4) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Zohar and Luria (2005) |
| | How frequently do your direct supervisor(s) allow you and your co-workers to overlook InfoSec when rushing deadlines? (SUP5) (reversed) | Never; Very rarely; Rarely; Sometimes; Occasionally; Very frequently; Always | Brondino, Pasini and Costa (2013); Kines et al. (2011); Zohar and Luria (2005) |

| Construct | Question (Item) | Scale | Adapted sources |
|---|---|---|---|
| Perception of colleagues' InfoSec behaviours (COL) | How much do your co-workers perform InfoSec behaviours in their daily work? (COL1) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Kines et al. (2011) |
| | How much do your co-workers care about InfoSec? (COL2) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Jaafar and Ajis (2013) |
| | How much training and updates about InfoSec do your co-workers receive? (COL3) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Goo et al. (2014) |
| | How much do your co-workers prioritise InfoSec when they are rushing deadlines? (COL4) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Chan et al. (2005); Jaafar and Ajis (2013); Lingard, Cooke and Blismas (2009) |
| | How much do your co-workers pay attention to and perform InfoSec behaviours, even when they are not supervised? (COL5) | Never; Very Little; Little; Somewhat; Much; Very much; A great deal | Brondino et al. (2013); Chan et al. (2005); Lingard et al. (2009) |

**Table 2. Questions about InfoSec climate perceptions**

# APPENDIX B: PARAMETERS INCLUDED IN SAOM ANALYSIS

The parameters that we evaluated in our SAO model, which represented the mechanisms in the conceptual framework, to explain the simultaneous changes in the network structures and the employees' perceptions of InfoSec climate were grouped into two categories, comprising those that explain: (1) the forming mechanisms of the networks, and (2) the forming mechanisms of InfoSec climate perceptions.

## Parameters for Modelling the Formation Mechanisms of Networks

The parameter *density* is included in almost every SAO model to explain the likelihood of occurrence of network ties between random actors and to characterise the shape of a network (Snijders et al., 2010). The estimate of this parameter is often negative, which describes the commonly sparse and thin structure of networks. Another parameter frequently included in network models is *reciprocity*, which describes the tendency for actors to reciprocate ties (DeLay et al., 2016; Snijders et al., 2010).

We modelled the triadic effects of transitive closure and structural equivalence concerning the actors' outgoing choices by including the parameters *gwespFF* and *gwespFBMix*. GWESP stands for 'geometrically weighted edgewise shared partners', referring to the evaluation of these triadic effects by focusing on the intermediate actors' contributions to a direct tie between two indirectly connected actors, where such contribution of having many intermediaries is downweighed, i.e., intermediaries that are geometrically far away from the indirectly connected pairs have less impact on their direct ties (Ripley et al., 2011). The GWESP parameters can be distinguished by the two letters next to the abbreviation, which can be 'F' ('forward') or 'B' ('backward'). These letters, in their order of appearance, refer to the directions of the ties which are sent from an actor to an intermediary, and from this intermediary to other actors who are indirectly connected to the former one. For example, the parameter *gwespFF* describes the transitive closure effect which counts the number of triads comprising three actors I, J and multiple intermediaries K, where the tie between I and J is facilitated by the forward tie sent from I to K and by the forward tie from K to J.

In the context of providing InfoSec support, the parameter *gwespFF* evaluates the likelihood of employee I to directly seek InfoSec support from J, which increases when I indirectly seeks support from J via numerous intermediate employees K. The parameter *gwespFBMix* examines the phenomenon where the likelihood for I to have a tie with J increases, when I and J both have ties to multiple K in between. The term 'Mix' in the parameter's name indicates that the configuration of interest involves more than one type of network ties, which in our study are the combinations of 'instrumental–InfoSec support' and 'expressive–InfoSec support' ties. With this parameter we examined the likelihood for employee I to directly seek InfoSec support from employee J, when I and J both seek work or personal advice from multiple employees K between them.

Degree-related parameters were included in our SAO model to improve goodness-of-fit (DeLay et al., 2016). We used these parameters to model the number of actors that received or sent many ties compared to the average number of ties, i.e., by using the parameters *inPopSqrt* and *outActSqrt*, or those that are not connected to any actors, i.e., are isolates (Snijders et al., 2010). Minimum in- and out-degrees or the specific number of outgoing and incoming ties can also be modelled (Ripley et al., 2011), which are useful when there are outliers in the network.

Parameters for modelling the changes in the employees' selection of socialised colleagues explain why network ties are created or maintained between pairs of employees over time. Background characteristics such as gender, department membership, age, tenure and seniority were modelled to evaluate the relationship between the actors' characteristics, e.g., long tenure or high seniority and their tendency to socialise. Homophily effects such as the tendency to socialise with actors having similar characteristics, e.g., same gender or same department, were modelled by the parameter *simX* for numeric variables (such as age and tenure) and *sameX* for categorical variables (such as department membership and gender). Since we calculated the scores measuring the employees' InfoSec climate perceptions, we used these scores in modelling the homophily effect. Since there are three different networks (instrumental, expressive and InfoSec support) in our model, we included the parameter *crprod* to study the co-changes in the employees' selection patterns in multiple networks over time. For example, the tendency for two employees to provide InfoSec support while trusting each other's expertise at the same time was modelled in that way.

## Parameters Modelling the Formation Mechanisms of Infosec Climate Perceptions

When performing SAOM analysis, the used RSiena tool includes the *linear shape* and *quadratic shape* parameters by default, where the former parameter describes the behaviour's tendency to increase or decrease over time in a linear fashion, and the latter describes the tendency for the actor to self-adjust the behaviour when its score becomes too high or too low (Ripley et al., 2011). In our study, these parameters examined the changes in the employees' climate perceptions of colleagues and direct supervisors' InfoSec behaviours that were independent of the external influence caused by interacting with other employees.

We included the parameter *totSimW* to model the employees' tendency to adjust InfoSec climate perceptions to match with those of the colleagues who provided InfoSec support to them, i.e., the assimilation effect. We also included the parameters *effFrom* which accounted for the effects of the employees' background characteristics on their InfoSec climate perceptions (e.g., higher seniority leads to higher InfoSec climate perceptions). Since we examined two types of climate perceptions i.e., of colleagues' and direct supervisors' InfoSec behaviours, each type of climate perceptions was modelled to have the same set of parameters explaining the mentioned effects.

## APPENDIX C: SAOM RESULTS

Table 7 summarises the effects in the SAOM analysis that achieved statistical significance, as well as the parameters describing them and the estimated results. Absolute t-statistics are calculated by dividing the estimate and the standard error to determine the parameters' statistical significance, i.e., the estimate is twice as large as the standard error. Although the parameters *inPopSqrt*, *outActSqrt*, *simX* and *effFrom*–as explained in Appendix B–were initially included in the SAO model, their results were neither reported in Table 7 nor discussed in section 5 since they did not achieve statistical significance.

| Effects for instrumental network | Parameter | Estimate | Std. Error |
|---|---:|---:|---:|
| rate | rate | 7.09 | –0.67 |
| outdegree | density | –5.15 | –0.74 |
| reciprocity | reciprocity | 0.84 | –0.24 |
| transitivity | gwespFF | 1.19 | –0.23 |
| gender of ties receiver | altX | 0.44 | –0.13 |
| gender of ties sender | egoX | –0.44 | –0.15 |
| same gender | sameX | 0.34 | –0.12 |
| same department | sameX | 0.94 | –0.12 |
| age of ties receiver | altX | 0.03 | –0.01 |
| seniority of ties receiver | altX | 0.50 | –0.17 |
| same seniority | sameX | 0.50 | –0.18 |
| expressive network | crprod | 1.90 | –0.23 |
| **Effects for expressive network** | **Parameter** | **Estimate** | **Std. Error** |
| rate | rate | 5.46 | –0.55 |
| outdegree | density | –4.20 | –1.01 |
| reciprocity | reciprocity | 1.55 | –0.19 |
| transitivity | gwespFF | 1.04 | –0.19 |
| gender of ties receiver | altX | 0.56 | –0.15 |
| same gender | sameX | 0.66 | –0.14 |
| same department | sameX | 1.05 | –0.14 |
| instrumental network | crprod | 1.75 | –0.33 |
| **Effects for InfoSec support network** | **Parameter** | **Estimate** | **Std. Error** |
| rate | rate | 8.29 | –1.05 |
| outdegree (density) | density | –2.60 | –1.05 |
| same department | sameX | 1.22 | –0.15 |
| age of ties receiver | altX | –0.03 | –0.01 |
| champion of ties receiver | altX | 0.55 | –0.16 |
| expressive network | crprod | 1.56 | –0.4 |
| gwespFBMix via expressive network | gwespFBMix | –0.62 | –0.3 |

| | | | |
|---|---|---|---|
| instrumental network | crprod | 1.25 | –0.37 |
| gwespFBMix via instrumental network | gwespFBMix | 0.56 | –0.27 |
| **Effects for perceptions of colleagues' InfoSec behaviours** | **Parameter** | **Estimate** | **Std. Error** |
| rate | rate | 2.07 | –0.41 |
| tendency for perceptions to increase/decrease over time | linear shape | 1.79 | –1.26 |
| tendency for perceptions to self-adjust | quadratic shape | –0.62 | –0.19 |
| assimilation of InfoSec climate perceptions caused by receiving InfoSec support from colleagues in the same department | totSimW | 8.40 | NA+++ |
| **Effects for perceptions of supervisors' InfoSec behaviours** | **Parameter** | **Estimate** | **Std. Error** |
| rate | rate | 2.74 | –0.59 |
| tendency for perceptions to increase/decrease over time | linear shape | 2.57 | –1.16 |
| tendency for perceptions to self-adjust | quadratic shape | –0.37 | –0.11 |

**Notes:**

1. +++ Score-type test was employed to examine this effect and the estimate was found statistically significant (Chi-square=9.2887; *p*-value=0.0023; one-sided statistic=3.0477).
2. Statistically significant effects have *estimate > 2*standard error* i.e., t-statistic > 1.96
3. Refer to Appendix B for the meanings of the included parameters

**Table 3. SAOM results (statistically significant effects only)**