Accepted Manuscript

Title: Investigation into the formation of information security influence: network analysis of an emerging organisation

Author: Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno

PII: S0167-4048(17)30117-7
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.05.010
Reference: COSE 1151

To appear in: Computers & Security

Received date: 27-8-2016
Revised date: 18-5-2017
Accepted date: 25-5-2017

Please cite this article as: Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno, Investigation into the formation of information security influence: network analysis of an emerging organisation, Computers & Security (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.05.010.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.
Investigation into the formation of information security influence: network analysis of an emerging organisation

Duy Dang-Pham¹, Siddhi Pittayachawan², and Vince Bruno³

School of Business IT and Logistics, RMIT University
Melbourne, Australia

[1] corresponding author; email address: duy.dang@rmit.edu.au
[2] Email address: siddhi.pittayachawan@rmit.edu.au
[3] Email address: vince.bruno@rmit.edu.au

Duy Dang-Pham is completing his Ph.D. (Business Information Systems) in the School of Business IT and Logistics, RMIT University, Australia. His research on information security management and behaviours, and especially the applications of social network analysis methods in the behavioural information security field, has appeared in journals such as Information & Management, Computers & Security, Computers in Human Behavior, and Business Horizons.

Dr. Siddhi Pittayachawan is a Senior Lecturer of Information Systems and Supply Chain Management in the School of Business IT and Logistics at RMIT University. He holds a Ph.D. in Business Information Systems. He is an OUA Program Coordinator, Bachelor of Business (Logistics and Supply Chain Management). His research interests include trust, information system adoption, information security behaviour, sustainable consumption, supply chain management, and business education.

Dr. Vince Bruno holds a Ph.D. in Business Information Systems from RMIT University, Australia. He is a Lecturer of Information Systems in the School of Business IT and Logistics, at RMIT University. His research interests focus on usability, application development, databases, and IS education.

Abstract

While prior research has been examining information security behaviours in mature environments with formal policies and practices, there is less attention paid to new or transforming environments that lack security controls. It is crucial to understand what factors affect the formation of an emerging information security environment, so that security managers can make use of the forming mechanisms to improve the security environment without relying too much on enforcement. This research adopts exponential random graph modeling to predict the occurrence of information security influence among 114 employees in a recently established construction organisation. Our empirical findings show that physically co-locating, as well as having specific senior levels and similar tenure can result in more security influence. Other contributing work relationships include the exchange of work-related advice, interpersonal trust, and seeing others as role model and long-term collaborators. The structural features of the information security influence network were also
examined, which offer strategies for security managers to diffuse security behaviours within
the workplace. Furthermore, specific directions for future network research were elaborated
in detail.

Keywords
information security influence; behavioural security; information security behaviour;
information security management; social network analysis

1 Background

The need to protect organisational information security has been growing rapidly over the
past decades due to heavy reliance of modern organisations on their information systems
(Bulgurcu et al. 2010). More importantly, it was realised that technological measures alone
cannot protect organisational information security, and organisations require a great amount
of the end-users’ efforts to perform information security behaviours (Crossler et al. 2013). As
a result, the end-users hold a critical role in reducing information systems’ risks, while at the
same time being the weakest link in the organisation’s information security chain (Bulgurcu
et al. 2010). Behavioural information security research thus emerged as an important field,
which has been contributing to theoretical knowledge and practices with regard to promoting
desirable information security behaviours and deterring malicious ones (Crossler et al. 2013).

Empirical evidence has pointed out that information security behaviours differ across
contexts and physical locations, even when the same behaviours are examined (D’Arcy and
Devaraj 2012; Dang-Pham and Pittayachawan 2015; Li and Siponen 2011). Such differences
can be explained by the environmental factors affecting the end-users’ cognitive processes
that determine how they will perform security behaviours, including the availability of
adequate security protection, supportive learning resources, or social pressure, just to name a
few (D’Arcy and Devaraj 2012; Ifinedo 2014; Li and Siponen 2011; Warkentin et al. 2011).
To analyse the contextual differences, prior behavioural security studies have examined
information security environments with contrasting features such as public space and home
(Dang-Pham and Pittayachawan 2015), workplace and home (Li and Siponen 2011), or
virtual teams and employees who are physically co-located (D’Arcy and Devaraj 2012).

Nevertheless, even a formal workplace that has implemented security protection can struggle
to maintain its information security workplace, especially during and after organisational
transformation processes such as mergers and acquisitions (M&A) (Dhillon et al. 2016;
Huang and Chuang 2007). In fact, organisations could encounter tremendous impacts on its
business processes and information systems during such transformation (Robbins and
Stylianou 1999), and organisational failure can be common (Creasy et al. 2009). The
transformed environmental factors such as re-written policies and processes, norms, and
technical infrastructure (Dhillon et al. 2016; Huang and Chuang 2007), or the employees’
different perceptions of organisational supports and fit (Creasy et al. 2009), can affect how
they perform information security behaviours.

1.1 Impacts of the workplace on information security behaviours

Various factors that contribute to the end-users’ information security behaviours have been
explored by empirical research (Siponen et al. 2014; Sommestad et al. 2014). Most recently,
behavioural information security studies focused on the impacts of the workplace’s features
on the employees’ information security behaviours (Dang-Pham et al. 2016). For instance,
Warkentin et al. (2011) found that the employees’ self-efficacy in performing secure
practices can be enhanced by having access to learning resources, such as situational support
and verbal persuasion. Furnell and Rajendran (2012) and Padayachee (2012) argued that the employees’ information security behaviours can be influenced by their socialisation with supervisors and colleagues. Ifinedo (2014) found evidence supporting that the employees’ social bonds in the workplace contribute to their intention to comply with information security policy.

It must be highlighted that while end-users greatly contribute to organisational information security, in other circumstances their information security behaviours can result in dreadful and undesirable consequences. Stanton et al. (2005) identified six types of end-users’ information security behaviours, which can be classified based on the end-users’ expertise (i.e. novice or expert) and intentions (i.e. malicious, neutral, or benevolent). Information security behaviours carried out with benevolent intention, such as personal compliance with policy (Bulgurcu et al. 2010; Siponen et al. 2014; Vance et al. 2012) or mentoring others on their information security practices (Safa et al. 2016; Warkentin et al. 2011), constitute a secure workplace.

With regards to malicious information security behaviours, Baskerville et al. (2014) postulated that information security abuses occurs when the perpetrators find the opportunities to do so by evaluating the security environment. Willison and Warkentin (2013) and Dang (2014) argued that malicious information security behaviours can be caused by work strains and prevented early by reducing the workplace stress. Kirlappos et al. (2014) found information security workarounds, or shadow security, are created and diffused at the department level by the employees’ supervisors via informal induction. Guo and Yuan (2012) discussed that the intention to perform misbehaviours is not discouraged directly by organisational punishment but rather indirectly via the group social sanction.

The reviewed studies explain how employees can be influenced to perform both desirable and malicious information security behaviours by their peers and supervisors (Furnell and Rajendran 2012; Ifinedo 2014; Kirlappos et al. 2014; Padayachee 2012). In fact, subjective norm, or a form of social influence that comes from the important people of a person, is one of the factors that affects information security behaviours across the studies (Sommestad et al. 2014). Given the impacts of interpersonal influence caused by environmental cues on individuals’ security behaviours and organisational security as a whole, further research is needed to explore in-depth for such an influence (Warkentin et al. 2011).

1.2 Research motivations

There are limitations in the current body of knowledge that motivated us to conduct this research. First, as the recent research of Dhillon et al. (2016) has pointed out in their literature review, there are few studies that have investigated into the turbulent information security environment that undergo workplace’s transformation process. Second, most studies have focused much on the individualistic cognition of the employees, thereby overlooking the dynamics that take place between these employees and in the information security environment.

For instance, behavioural theories such as Theory of Planned Behaviour (Ajzen 2011) and General Sanction Theory (Straub and Welke 1998) have been widely employed to understand the mechanisms of the end-users’ information security behaviours that are affected by factors of the work environment like subjective norms, perceived behavioural control, or perceived sanction (Padayachee 2012; Sommestad et al. 2014). However, end-users operate with bounded rationality and limited information (Ajzen 2011), while environmental factors such as effective sanctions require the end-users to be aware of the sanctions first before perceiving their effects (Straub and Welke 1998). With the traditional research approach, the
end-users’ different types of access to organisational resources with different levels of intensity are hard to be captured and analysed in detail (Dang-Pham et al. 2016; Otte and Rousseau 2002; Sykes et al. 2009). Social network analysis (SNA) techniques have been recently employed in information systems studies to overcome such limitations and to explore in-depth the characteristics of interpersonal influence (Sykes et al. 2009; Zheng et al. 2010). In the behavioural security research field, Dang-Pham et al. (2016) conducted an exploratory study that compared information security networks with other core organisational networks. Nevertheless, their study is exploratory in nature and thus lacks the theoretical perspective.

This research addresses the mentioned limitations in multiple ways. First, our research setting is an emerging information security environment of a sister company to a larger enterprise, which comprises newly recruited employees as well as employees who formerly worked in the enterprise. Consequently, this company has disruption and cultural conflict that normally take place in a transforming organisation (Creasy et al. 2009; Dhillon et al. 2016; Huang and Chuang 2007). We address the limitation regarding the overlooked workplace dynamics by employing exponential random graph modelling (ERGM), which is a network predictive analysis technique, to test hypotheses and statistically examine the structural features of the information security influence network.

The adoption of SNA methodology to study information security influence offers several benefits. Unlike the traditional research approach that treats individuals as main unit of analysis and focuses on the individual’s cognition related to influence (e.g. individual’s perceptions of norms, climate, or perceived support), SNA examines directly the influence as a type of interaction between people (Otte and Rousseau 2002). This approach also objectively measure an individual’s influence by the number of nominations sent from their peers who recognise their influence. Furthermore, various prominent effects from the sociology field that explain the social influence process such as proximity (i.e. social or physical distance) or homophily (i.e. sharing similar attributes) can be tested with SNA without violating the statistical assumptions of common regression analyses (Borgatti et al. 2013; Dang-Pham et al. 2016). The structural features of influence (e.g. transitivity and hierarchy) can also be examined visually by inspecting the network diagram or statistically by ERGM (Borgatti et al. 2013).

More important, ERGM as a research tool offers more flexible and sophisticated analytical capabilities than the descriptive approach, which were employed by the exploratory study of Dang-Pham et al. (2016). The theoretical perspective is highlighted in our research as we use ERGM method to test theoretically-based hypotheses about the workplace’s effects on the formation of information security influence. The analytical strengths of the SNA approach, as well as of the ERGM method in particular, justify its adoption in our study and highlight our contributions to the current body of knowledge, as we attempt to investigate information security influence in detail from the novel network perspective.

1.3 Research setting

This research analyses the formation of an emerging information security environment of VNC, a large construction company in Vietnam specialised in building large-scaled projects such as serviced apartments, hotels, and resorts. VNC is a sister company of one of the top four construction enterprises in Vietnam, which was established in 2013 to focus particularly on the segment of residential projects. The other sister companies and the enterprise itself build major infrastructure in Vietnam such as industrial parks, seaports, as well as roads and
highways. According to the director of VNC, the company is relatively new yet its annual revenue consistently ranks much higher the market’s average.

It is worth mentioning that VNC does not have a formal IT department at the moment but a small team of IT technicians. The managing director is directly involved in planning IT strategies and entrusts the procurement and implementation of IT infrastructure to those technicians. In fact, VNC follows the IT infrastructure of its parent enterprise. The top management from VNC shared with us during the meeting that the organisation structure was designed to fully support the agile and dynamic nature of their construction projects. Furthermore, VNC as a sister company often receives projects from its parent enterprise. Therefore, their attention to supportive functions such as business development and IT is minimal. Instead, the top management emphasised on developing strong construction and quality control departments over the past three years since VNC’s establishment to ensure their deliverables are of the highest quality.

VNC has 114 office employees working in 10 locations. Moreover, VNC was established with 41 employees who came from the parent enterprise, and VNC has subsequently recruited 73 new employees to date. To this end, we were sourced by the company to conduct network analysis with two primary objectives. First, the research aims to identify the key influencers who can effectively diffuse information security awareness to all employees at VNC. Second, the company would like to understand the diffusing mechanisms so that they can continue the diffusion of information security awareness in the future.

We took this opportunity to analyse the formation of VNC’s information security environment. The information security environment is represented as a network of information security influence among the employees. More importantly, we employed exponential random graph modeling (ERGM) to predict the occurrence of information security influence among the employees, so to explain the forming mechanisms of the security environment. Ultimately, we aim to answer our research question:

“What are the factors that lead to information security influence among employees (i.e. formation of the information security environment)?”

2 Theoretical model

In this section, we elaborate our hypotheses based on the extant theoretical background, which constitutes our theoretical model that will be empirically tested with social network analysis method.

2.1 Main effects

Interpersonal influence takes place when one actor adapt another’s attitudes and behaviours as they exchange information via the direct ties between them (Leenders 2002). Network research has been investigating the impacts of two prominent relationships, namely instrumental and expressive ties (Ibarra and Andrews 1993; Saint-Charles and Mongeau 2009). These instrumental and expressive relationships play critical roles in a workplace as they allow employees to clarify uncertainty and ambiguity from constantly interpreting the workplace’s features (Saint-Charles and Mongeau 2009).

By seeking instrumental and work-related advice from a colleague, a person gains knowledge about the colleague’s expertise and recognises their expert power. This expert power enables the giver of work advice to influence the receiver’s behaviours (French and Raven 1959). Furthermore, information security procedures are embedded into daily operations when the operations involve interacting with confidential information and computer systems.
Therefore, the exchanged advice about one’s work also includes handling information security issues, and the receiver’s information security behaviours would be subsequently modified as per the work advice-giver’s recommendations. In fact, prior network research Dang-Pham et al. (2016) found the networks of information security influence and exchange of work advice correlated with each other. As a result, we hypothesise:

**H1:** Employees have their information security behaviours influenced by colleagues who often give them work-related advice

Employees in the same workplace can have different interpretations of information security risks that causes ambiguity (Dourish et al. 2004). These employees would then seek colleagues whom they regard as trustworthy friends to reduce the ambiguity about information security matters. The impact of friendship on interpersonal influence between people is quite established in network research, as facilitated by the normative and informative influence processes (de Klepper et al. 2010). Specifically, informative influence process involves an individual being convinced by their friends whose informational creditability is perceived as high by that individual, whereas normative influence is about an individual wanting to be like their friends (de Klepper et al., 2010; Leenders 2002). This process is similar to the referent power base discussed in the theory of social power bases (Raven 2008). Employees can emulate information security behaviours of the colleagues whom they select as frames of reference or role models, based on their own preferences and knowledge of these colleagues. Therefore, we hypothesise:

**H2:** Employees have their information security behaviours influenced by colleagues whom they trust

**H3:** Employees have their information security behaviours influenced by colleagues whom they see as a role model at work

Finally, it takes time for a person to evaluate the characteristics of other people before the person can see them as a role model worthy for emulating their behaviours. Moreover, employees who have spent most of the time together in collaborative projects could exchange of work advice more frequently and gain more trust, which are essential relationships for interpersonal influence (Ibarra and Andrews 1993). Furthermore, long-term work collaborators tend to form group identities that facilitate influence within the groups (Tajfel and Turner 1985). As a result, we propose the following hypothesis:

**H4:** Employees have their information security behaviours influenced by colleagues whom they have collaborated with for a long time

### 2.2 Control variables

In addition to the mechanisms of interpersonal influence discussed above, the occurrence of information security influence can be conditional on the perceived attributes of the influencers. These personal features make an individual more influential to others as posited by influence theories (French and Raven 1959; Leenders 2002; Tajfel and Turner 1985), which we will elaborate below. The inclusion of these control variables, as established forming mechanisms of influence, will help to reveal the hypothesised main effects more clearly in later analysis.

**Work tenure and seniority:** The theory of social power bases (French and Raven 1959; Raven 2008) posited six types or bases of power that can make a person more influential to others. These bases include (1) informational, (2) reward, (3) coercive, (4) legitimate, (5) expert, and (6) referent power (Raven 2008). In behavioural information security context, there have been empirical studies that have examined the effects of these power bases. For
instance, Dourish et al. (2004) discussed that employees tend to seek colleagues, whom they consider as information security expert, when encounter security issues. Kirlappos et al. (2014) also found that security workarounds can be propagated within the work units and legitimised by the employees' direct supervisors. These are examples of the effects of expert and legitimate power bases on information security influence. In an organisational context, legitimacy often associates with formal and hierarchical job roles (Ibarra and Andrews 1993; Raven 2008). Consequently, it is expected that employees holding senior positions would demonstrate their legitimate power have strong influence over others' behaviours, including information security practices.

**Sharing the same work location:** Social identity theory (Tajfel and Turner 1985) suggested that individuals tend to align their attitudes and behaviours with those of their identified groups. The effect of this group norm is especially highlighted in studies about M&A, which explains the “us versus them” belief that commonly takes place in post-merger organisations (Panchal and Cartwright 2001). Furthermore, prior research has also found that employees tend to interact more with colleagues who are physically located near them, which subsequently facilitates interpersonal influence (Borgatti and Cross 2003; Ibarra and Andrews 1993). Given the mixture of old and new employees at VNC, as well as their different work locations, it is anticipated the social identity and work proximity effects would also govern the employees’ security behaviours. Similarly, we include these effects as control variables in our theoretical model (figure 1).

### 3 Research method

#### 3.1 Data collection and measures

A questionnaire was designed to include questions (table 1) that capture the network of information security influence among the employees, as well as the four networks discussed in the proposed hypotheses. We followed the network questions used in Dang-Pham et al.’s (2016) study to produce comparable findings, especially when these researchers examined a more mature information security environment than ours (i.e. a construction enterprise established in 1992 with a dedicated information security team). The employees’ demographics were extracted from VNC’s human resource databases. We conducted both online and offline surveys for one month, and retrieved back 93 usable responses (i.e. 82 per cent of VNC’s total employees).

#### 3.2 Ensuring network research rigour

##### 3.2.1 Reliability

The design and administration of network questionnaire have impacts on the rigour of network research. For example, participants’ non-response due to fear of anonymity being violated and difficulty in recalling names is a primary risk to research rigour (Borgatti et al. 2013). The former risk is caused by the intrusive nature of network questionnaire, which demands the participants to provide real names of them as well as the actors that they interact with. To alleviate this risk, a confidentiality agreement was signed by VNC’s management and shown to all employees to ensure protection of the respondents’ anonymity, thus increasing their confidence in participating in the research.

The response rate of 82 per cent of VNC’s total employees might be considered as high, and there would be concerns about a possibility of bias due to the respondents’ work ethics that make them deeply respect the authority. The bias due to social desirability is inevitable for
sociometric questioning, which can lead to respondents nominate relationships with people that in fact they do not have (Zwijje-Koning and de Jong 2005). To alleviate such bias, Borgatti et al. (2013) recommended building rapport with the respondents and using online survey for data collection, which has the least sensitivity and can minimise the respondents’ self-consciousness. In addition to the use of online survey, we included the confidentiality agreement to the survey’s front page, which was signed by VNC’s management and stated that they would not have access to the collected data. The employees were clearly explained that they had the rights to voluntarily refuse to participate or withdraw the collected responses by contacting the researchers, without receiving any adverse consequences.

The problem of recalling names can be addressed by using a roster (Borgatti et al. 2013). For each of our network questions (online version), there is a dropdown list that contains all the names of the employees and their departments in VNC. The participants can browse through the names list and select the colleagues that they interact with. In fact, an electronic network questionnaire is the most desirable form of collecting network data since it is less prone to data handling errors, sensitivity issues, and interviewer response effects (Borgatti et al. 2013). Similarly, we attached a roster to the offline questionnaires so the participants can recall their colleagues more easily.

Another issue associated with names is the number of nominations that the participants are required to make for each network question (Borgatti et al. 2013). Our network questionnaires asked the participants to nominate maximum five colleagues per question as they feel appropriate. The maximum limit of five nominations was set according to Merluzzi and Burt’s (2013) recommendations about the number of names required for network research in Asian-Pacific organisations. Moreover, nominating maximum five colleagues per question requires a reasonable amount of effort from the respondents without causing much burden. Since the network data are nominations (e.g. influenced by who), we transposed the networks to assist interpretability (e.g. influence whom).

3.2.2 Validity

Validity in network research concerns designing precise questions that can accurately capture the intended interactions or relationships (Borgatti et al. 2013). In this regard, we adapted the questionnaire that was employed by an existing network research in the behavioural security context (Dang-Pham et al. 2016). Moreover, the general director was consulted during the design process to ensure the appropriateness of the questions. Furthermore, as seen in table 1, we provided detailed examples per network question to assist the participants’ interpretation and reduce ambiguity.

3.3 Exponential random graph modeling

Since interactions and relationships are the main unit of analysis in a network research, network inferential analysis techniques enable predicting a tie’s occurrence by using another tie as a variable. Other analysis methods such as structural equation modeling (SEM) are inappropriate and irrelevant in our case, for latent constructs are not of our concerns and the network data violates the statistical assumption of common regression methods (Borgatti et al. 2013). ERGM is a predictive method for network analysis, which produces coefficient estimates from Markov Chain Monte Carlo (MCMC) estimation process (Robins et al. 2007). Furthermore, ERGM allows network researchers to predict the occurrence of ties with more sophisticated formation mechanisms such as transitivity or reciprocity.

Network researchers determine the contributing factors towards the occurrence of ties by evaluating a statistical model, which comprises terms to describe various network formation
mechanisms, that can replicate the network observed from the collected data (Robins et al. 2007). The “ergm” package (Hunter et al. 2008) of the statistical programming language R offers a wide range of network terms that can be used to develop random graph models. For instance, the baseline “edges” term captures the occurrence of the focal ties, while terms such as “edgecov” and “nodecov” add ties and node’s attributes as covariates to the model (Morris et al. 2008).

We followed Robins et al.’s (2007) five-step procedure to specify our models, especially by progressively adding terms to capture the local formation processes, then the structural configurations such as triad effects. The MCMC estimation process was then conducted to estimate our random graph model with interval and burn-in set relatively high at 5,000 and 50,000 respectively. The model converged at the 2nd iteration out of 20, and Geweke statistics of all included network terms were greater than 0.05, which indicated the model is free from degeneracy. The MCMC estimation process also produced statistics about the estimated distributions of the four core network features (i.e. in- and out-degrees, shared edgewise partners, and geodesic distance) to assist evaluation of the model’s goodness-of-fit.

Figure 2 illustrates the goodness-of-fit statistics so that visual evaluation can be performed. The black line represents the observed network’s features that should be reproduced by the random graph model. The boxplots are the estimated values from our model about the core network terms, and the grey lines are the 95 per cent bounds of the distributions. Acceptable goodness-of-fit of the model requires the grey lines and boxplots to cover the black lines, which indicate that the random graph model can reproduce the observed network via simulations. As seen in figure 2, our model captures well the distributions of in-degree and out-degree (except an unexpected spike of in-degrees equal to 5). Likewise, there appears to be no problems in the pattern of edge-wise shared partners. The limitation of our model is that it fails to capture well the observed pattern of minimum geodesic distance. However, this limitation can be overlooked since it is not the primary research focus (Kim et al. 2015; Lusher et al. 2012).

4 Analysis and findings

4.1 Descriptive analysis

We begin with visually analysing the “information security influence” network diagram that reflects the security environment of VNC (figure 2). The network’s density, which reflects how well-connected the nodes in the network are, is 0.02. Networks are considered connected in different contexts depending on their density level (Gesell et al. 2013), but a density level of 0.02 can be deemed as thin and sparse. In other words, information security influence is a rare network tie that not every actor in this network can possess. Such rarity is consistent with an average degree of 1.916, which means that each employee in the information security influence network possesses only two ties on average.

Transitivity and hierarchy are two important structural features of a network that require elaboration. Specifically, the former refers to how fast information security influence can travel in the network, while the latter refers to whether there are any central nodes that dominate the rest in terms of security influence. The ratio of transitive triads over total number of triads in our network is 0.152, or 15 per cent. Like density, different networks have their own acceptable threshold for this ratio, even though a transitivity ratio of 0.3 can be considered transitive (Gesell et al. 2013). Comparing our ratio of 0.152 to 0.3, the information security influence network appears quite transitive. Moreover, two random
employees in the information security influence network are linked with more than two hops on average (average distance=2.421).

Hierarchy can be evaluated by computing degree centralisation measures, which indicate the inequality in the nodes’ degrees (Hanneman and Riddle 2005). The degree centralisation measures of the information security influence network are 0.12 (overall), 0.12 (out-degree), and 0.03 (in-degree). Given these relatively small statistics, there is not much inequality or hierarchy in the network. However, it can also be observed that there is more hierarchy with respect to out-degree (i.e. one’s ability to influence another) than in-degree (i.e. being influenced by another).

When performing visual inspection on networks, researchers take note of patterns such as the clusters that are linked to each other via a few number of brokers or gatekeepers, or the number of distinctively prominent nodes, as well as isolated and peripheral nodes that usually locate at the network’s border. In overall, it is quite challenging to visually observe any meaningful or distinctive patterns in our information security influence network.

The colours of the nodes in figure 3 denote their work locations. VNC assigned their employees to nine different large construction projects, each of which lasts for at least five years. In other words, employees in VNC were located in the same location to collaborate with other project members for a long period, before they will be assigned to continue working with the same project group or change to a new one. The sizes of the nodes represent their out-degree centrality measure, or how many colleagues nominated them as capable of influencing information security behaviours. Nodes with large sizes are those who are influential in the network. Nodes that are very small have minimal influence over others’ information security behaviours, and thus can be ignored.

The colours of ties follow their sources’ colours. This format allows the readers to clearly see the influencing areas of the nodes. For example, we can see which employees are influenced by employee #85, who works in the safety department, by tracing to the receivers of the ties that have the same green colour. We can also see that orange ties appear the most in figure 3, which indicates that this work location has the most number of influential employees as compared to others. The head-quarter, where VNC’s director (#74) and the supportive departments (e.g. accounting, business development) locate, is coloured light green. It is interesting to observe that the head-quarter is not as influential as the orange location, given the fewer amount of green ties in the network, and some of the head-quarter’s employees have their information security behaviours influenced by those from other work locations.

At the node-level, the most influential employees in information security work in the safety (#85, #42, #35), construction (Cons) (12, 24, 2, 29), design (57), and administration (Admin) (6) departments, in addition to the director (74). It is understandable that the employees from administrative departments can influence others’ security behaviours since their primary functions are often concerned with policies and procedures. For those who work in the main departments such as construction and design, their influential statuses can result from the daily work collaboration, whose impacts on security influence will be elaborated in the next ERGM section.

4.2 Forming mechanisms of information security influence ties

The primary purpose of ERGM analysis is to determine the forming mechanisms that explain why “information security influence” ties occur between pairs of random employees, hence the formation of information security environment. The estimated coefficients of the
hypothesised mechanisms and control variables are reported in table 2 below. These coefficients are conditional log-odds that can be converted to percentage of probability for better interpretation. The baseline likelihood of security influence ties’ occurrence is informed by the “edges” effect, which is -4.03. The probability of a security influence tie to occur between a pair of employees, without any contributing effects, is 1.75 per cent. In other words, it is rare to observe a random employee influences another’s information security behaviours. However, this likelihood can be increased or decreased once the other effects are added to the baseline term “edges”.
4.2.1 Effects of other networks on information security influence

Our hypotheses investigate the occurrence of information security influence ties based on organisational activities such as exchange of work-related advice (H1), interpersonal trust (H2), observing and following role model’s behaviours (H3), and work collaboration (H4). Given the p-values of these coefficients are lower than the recommended threshold of 0.001, all four hypotheses (H1–4) achieved statistical significance and are supported.

Moreover, these activities were found to increase the likelihood of information security influence to occur between the employees at VNC. For example, the likelihood of employee A convincing B to perform information security behaviours becomes 5.47 per cent if A frequently gives B work-related advice, and 15.6 per cent if A is also trusted by B. We also observed that the effect sizes of “give work-related advice” and “trust” are similar (1.18 and 1.16), are both lower than “nominated role model” (1.33) and “nominated collaborator” (1.61) relationships. In fact, the highest contributing effect of “nominated collaborator” ties to “information security influence” ties hinted to important homophily effect in this recently established VNC.

4.2.2 Effects of personal attributes on information security influence

Homophily effect refers to the situation when people choose to connect with similar others, and it has been an important effect that results in network ties (Borgatti et al. 2013). In our model, employees’ attributes such as work location, tenure, and seniority were included as controls for our main effects (H1–4), as well as to offer additional explanations for the forming mechanisms of information security influence. The results indicate that “information security influence” ties tend to occur more between employees who work in the same location. Sharing the same workplace increases the likelihood of security influence’s occurrence from 1.75 to 2.71 per cent.

Next, two “absdiff” terms were added to the model to capture the absolute differences between the tenure (in years) between pairs of employees (Morris et al. 2008). Moreover, we extracted from VNC’s human resource database two types of tenure, including the work period that the employees have spent in CFC—the parent enterprise of VNC—and in VNC since 2013. This information allows us to identify the “veterans” that were sent from CFC to VNC at the time it was established, as well as the “newcomers” that were recruited in the past three years. A positive estimated coefficient of “absdiff” indicate heterogeneity in connections, whereas a negative coefficient means homogeneity (Morris et al. 2008). In other words, the smaller the difference in an attribute (homophily), the higher chance of network ties’ occurrence. In our case, only the homophily effect of having similar tenure in VNC is confirmed. This result suggests that there is a tendency of the newcomers in VNC to have information security behaviours influenced by each other rather than listening to the veterans from the parent enterprise CFC. Furthermore, this is consistent with the above finding about the positive impact of “nominated collaborator” on the occurrence of security influence ties, which explains that the employees tend to have their security behaviours influenced by the colleagues whom they nominated for having collaborated with them in most projects.

We also examined the influential status caused by the employees’ seniority, including six categories as identified in the human resource database. These categories include: (1) operational staff, (2) team leader, (3) deputy manager, (4) manager, (5) deputy director, and (6) managing director. The “nodefactor” term compares the occurrence of ties caused by different levels of an attribute with one level serving as a base (Morris et al. 2008). In our case, we used operational staff as the base (level 1) and compare the remaining levels with it. The results suggest that being a manager increases the likelihood of influencing others’
information security behaviours, while the managing director has a significantly higher chance to do so (log-odds=2.4). In fact, the director’s influential effect in information security is even higher than the organisational activities discussed above. Interestingly, a director may not necessarily give work-related advice or be trusted by others, yet still has 16.4 per cent chance of influencing their colleagues’ security behaviours.

4.2.3 Effects of network structure on information security influence

Lastly, we incorporated a number of structural terms to explain the formation of “information security influence” ties. First, “gwodegree” and “gwidegree” terms describe homophily in the network patterns of being information security influencers and influencees respectively. A negative coefficient of these terms suggests that employees in the security influence network possess similar amount of out- or in-degrees. In our study, there is a tendency that most employees nominated equal numbers of colleagues who can influence their information security behaviours (i.e. “gwidegree” coefficient is negative). Furthermore, these terms help to control the number of degrees in the network, similar to the other terms “isolates”, “idegree0”, and “odegree0”, which assist better model’s goodness-of-fit.

Second, there is the set of “dgwdsp” and “dgwesp” terms that capture the triad effect of outgoing two-path (OTP) shared partners, which have been introduced in the latest “ergm” R package in 2016 (Hunter et al. 2008). The “dgwdsp” term informs the tendency that employee A indirectly influences B’s security behaviours via multiple intermediaries, regardless of whether there is a direct security influence tie that comes from A to B. In contrast, the “dgwesp” term informs the same tendency but with the condition that A directly influences B’s security behaviours.

When the two terms are examined at the same time, “dgwdsp” informs the tendency of having shared partners between pairs that are not tied, while “dgwesp” informs the tendency of pairs that are tied. In security influence context, a positive and significant “dgwesp” and an insignificant “dgdsp” coefficients inform that when A influences B’s security behaviours, there is a high chance that A will influence multiple other colleagues who also influence B. Interpreting this result alone indicates that there is transitivity in the information security influence network. When discussing with the “edges” term, it suggests that the likelihood for A to influence B’s security behaviours can increase if A indirectly influences B via multiple intermediaries.

5 Discussion and implications

From the discussed findings, we learned more about the information security dynamics within an unstructured and informal information security workplace such as VNC. Specifically, information security influence was found to be governed by organisational interactions (e.g. exchange of work advice and trust), relationships (e.g. sharing department membership, differences in tenure and seniority), and by the influence network’s own structural features.

From the theoretical lens of sociology literature, our findings provide empirical evidence that supports the prominent homophily effects, or a phenomenon when people prefer to associate with similar others (Borgatti et al. 2013; McPherson et al. 2001), in the behavioural security context. The finding that employees tend to have their security behaviours influenced by colleagues in the same work location is also consistent with prior researches (Dang-Pham et al. 2016; Kirlappos et al. 2014), even in an unstructured security environment without formal IT support such as at VNC. We also found features of post-merger & acquisition organisations in VNC as an emerging organisation having a combination of old and new
employees. The finding about the tendency of “newcomers” to learn about information security from each other more than from the “veterans” suggests the “us versus them” characteristic (Panchal and Cartwright 2001).

Employees holding senior management positions were found to have a higher chance to influence others’ information security behaviours. This finding supports the proposition of Raven’s (2008) theory of power bases that staff with formal authorities are often seen as influential thanks to their legitimate power in the workplace. It was more interesting to observe that these effects were statistically significant only when the influencers are managers and directors but not in deputy roles. This could be due to the actual authority possessed by employees holding full managerial positions that the deputy managers lack in VNC’s context. Furthermore, it is revealed that senior employees are used as frames of reference by others to adjust their information security behaviours when formal IT presence is missing.

Practical implications concerning the appropriate staffing practices, particularly in a work setting such as VNC, to control for information security influence can be drawn from above findings. First, top management should be aware of the possibility of different information security behaviours emerge within the work locations (e.g. in department or team). Employees of senior positions, who would have high chance to influence others’ security behaviours, should be consistently trained and appointed as local champions to control for any potential discrepancy in security practices.

Particularly in organisations that are similar to VNC, where there exists a combination of old and new employees who work together, top management is advised to pay attention to the divide between these two groups. The divide suggests additional considerations to the selection of security champions, who will be entrusted the tasks of disseminating and maintaining appropriate security practices. For instance, top management may select a capable newcomer to be the champion for a group of employees who also recently join the company. However, further interventions should be made in the later stages to remove such divide, so that information security practices can remain consistent in the workplace.

Our findings confirmed that all four organisational interactions, including (1) give work advice, (2) trust, (3) seeing as role model, and (4) collaborate in daily work, can result in information security influence. From these findings, top management can select security champions who actively engage in those four networks, as well as determine strategies for the champions to effectively disseminate information security practices. Common interventions to achieve such goal may include creating collaborative projects across different workgroups and mentoring or job shadowing system to facilitate exchange of work advice and build trust among employees (Hatala 2006). Through participation in the collaborative activities, the employees will have time to evaluate the security champions’ expertise and develop trust, which subsequently allow the champions to influence their security behaviours more effectively. These interventions are especially crucial for organisations that adopt a project-based structure such as VNC to increase the engagement and bonding among employees across different teams.

Finally, our findings suggest that information security influence is transitive, thus spreading within the workplace easily. More specifically, if a security champion can influence an employee indirectly via a number of in-between colleagues, then the chance for the champion to influence that employee directly becomes high. While transitivity assists the security champions in diffusing appropriate security knowledge and practices, there is a risk of undesirable security practices being conveniently disseminated via this structural feature as
well. Interestingly, the prior security network research by Dang-Pham et al. (2016) in another business context also found information security influence network to have transitive nature. While there is insufficient evidence to make claims about the general structure of information security influence network, the consistent findings about the transitive nature suggest this feature might be of importance.

The limitation of our study is the setting that focuses on an information security environment of a single company, which suggests that our empirical findings are best generalised to other contexts similar to ours. This limitation was primarily due to the sensitive and burdensome nature of whole-network survey that asks for real identities of the employees, thereby making it difficult to persuade companies to participate in the research. In fact, many empirical whole-network studies in other domains chose to focus on single work context, such as information security (Dang-Pham et al. 2016) or information systems adoption (Sykes et al. 2009; Zheng et al. 2010).

To extend our findings, we encourage future network studies in the behavioural security field to test the effects of other network ties on the occurrence of information security influence. For instance, this research has only examined the positive influence that encourages the employees to handle information security matter more carefully and be aware of the security threats. The spectrum of information security behaviours actually ranges from undesirable (e.g. sabotages or violations of policy) to desirable behaviours such as compliance (Crossler et al. 2013). Among the undesirable behaviours, network researchers can potentially evaluate information security accountability of a workplace by analysing the network ties of security delegation or transfers of security responsibilities among the employees (Dourish et al. 2004). Group sanction is another important factor in behavioural security research (Guo and Yuan 2012; Sommestad et al. 2014) which is worth exploring further. Network analysis methods can be applied to determine characteristics of the employees who can sanction others for not performing information security behaviours. Analysing the mentioned behavioural security networks expands our knowledge of the security interactions that matter and helps to devise practical intervention to improve the security environment. Recent development of SNA methodology also allows longitudinal analysis of the changes in network ties and actor’s attributes (Snijders et al. 2010). Such research would be important to identify the factors that can minimise or eliminate the “us versus them” effect.

6 Conclusion

Throughout this research, we have answered the research question pertaining to the formation of a recently established information security environment. Specifically, we conceptualised the information security environment of VNC as a network of ties denoting the information security influence that travels between employees. To understand the formation of such network or environment, we employed ERGM method to identify the mechanisms that establish information security influence ties between the employees.

We found information security influence ties were established by employees that have high seniority, and those ties also occurred between employee who have similar tenure. Moreover, physically co-locating was found to result in more information security influence, as well as potentially facilitates the work relationships that create such influence. The work relationships that facilitated information security influence include the exchange of work-related advice, interpersonal trust, and seeing others as role models and long-term collaborators. The positive effects of having similar tenure and long-term collaborators’ relationship on the occurrence of information security influence ties also suggested the “us versus them” effect on security influence within a new workplace such as VNC. Our findings
inform that VNC’s information security environment has a transitive structure and a few influential employees, while the remaining employees possess on average an even amount of four security influence ties. The transitivity nature highlighted that information security influence tended to occur between employees who shared common partners, which reflect the “word-of-mouth” effect. Formal authority, tenure homophily, physical proximity, work socialisation, and network transitivity were identified as key mechanisms of the formation of information security influence network, or the information security environment at VNC.

In addition to the scholarly objective to explore the formation of VNC’s recently established information security environment, the research outcomes also contributed to the business goals of VNC. Specifically, the investigation into the network about information security influence helped VNC’s top management identify the key influential employees in their workplace. The top management also detected the clusters of connected employees in the visualisation of the information security influence network. Combined with the identified mechanisms that create information security influence ties, VNC’s top management could devise strategies to develop a cohesive information security workplace.

We have also demonstrated the adoption of ERGM method to empirically test theoretically-based network hypotheses. As we focus on a company, one may argue that our findings can be generalised to other companies with similar profiles. In fact, behavioural security network research remains scant, and future studies are thus encouraged to replicate or extend our research in other contexts to validate findings. To this end, we have proposed some important research directions in the previous section, and we look forward to seeing more empirical network studies in the behavioural security field.

7 References


Dang-Pham, D., and Pittayachawan, S. 2015. “Comparing intention to avoid malware across


Figure 1: Theoretical model
Figure 2: Goodness-of-fit diagnostics
Figure 3: Information security influence network (93 nodes, 174 ties)
Note: Node’s label shows the employee’s unique ID and department; node’s colour depicts the employee’s work location; tie’s colour follows the source of influence’s colour
Table 1: Network questions

<table>
<thead>
<tr>
<th>Network questions</th>
<th>Networks (transposed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To improve how you perform daily work or overcome a challenge, who do you usually ask for advice? Examples of work-related advice can be direct answers, tips to improve how you perform daily work, or referrals to someone who can better help you</td>
<td>Give work-related advice</td>
</tr>
<tr>
<td>Which of the following colleagues would you consider as trusted friends, whom you could openly discuss opinions or seek advice about personal issues (e.g. about family, friendship, or how to fit in the work culture of VNC)</td>
<td>Trust</td>
</tr>
<tr>
<td>Which of the following colleagues whom you see as your role models at work, or you think that it would be very beneficial for you to learn from them or follow their ways of doing work?</td>
<td>Nominated role model</td>
</tr>
<tr>
<td>Which of the following colleagues have most often collaborated with you in projects since you started working in VNC?</td>
<td>Nominated collaborator</td>
</tr>
<tr>
<td>Overall, which of the following colleagues influence how you carefully handle and remain vigilant about information security and privacy issues in daily work (such as in the above mentioned situations)? *</td>
<td>Information security influence</td>
</tr>
</tbody>
</table>

*Note: a list of common information security situations was provided, such as verifying suspicious e-mail attachments, checking for updated anti-virus software, or setting strong passwords.
### Table 2: ERGM results

**Monte Carlo MLE Results:**

Iterations: 2 out of 20 (MCMC.interval = 5,000; MCMC.burn-in = 50,000)

<table>
<thead>
<tr>
<th>Network terms</th>
<th>Meanings</th>
<th>Estimates</th>
<th>S.E.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Likelihood of tie’s occurrence</strong> edges</td>
<td>Occurrence of “information security influence” tie between pairs of employees</td>
<td>-4.03***</td>
<td>0.41</td>
</tr>
<tr>
<td><strong>Controls for node attributes’ effects</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nodematch(“Work location”)</td>
<td>Employees working at the same location have higher chance to influence each other’s information security behaviours</td>
<td>0.45*</td>
<td>0.21</td>
</tr>
<tr>
<td>absdiff(“TenureAtCFC”)</td>
<td>“Information security influence” tie occurs between old employees who worked in the parent enterprise (named CFC)</td>
<td>-0.05</td>
<td>0.04</td>
</tr>
<tr>
<td>absdiff(“TenureAtVNC”)</td>
<td>“Information security influence” tie occurs between recently recruited employees at VNC</td>
<td>-0.17*</td>
<td>0.07</td>
</tr>
<tr>
<td>nodeofactor(“Seniority.2”)</td>
<td>Tendency of team leaders send out “information security influence” ties as compared to operational staff</td>
<td>0.34</td>
<td>0.30</td>
</tr>
<tr>
<td>nodeofactor(“Seniority.3”)</td>
<td>Tendency of deputy managers send out “information security influence” ties as compared to operational staff</td>
<td>0.55</td>
<td>0.36</td>
</tr>
<tr>
<td>nodeofactor(“Seniority.4”)</td>
<td>Tendency of managers send out “information security influence” ties as compared to operational staff</td>
<td>0.79*</td>
<td>0.34</td>
</tr>
<tr>
<td>nodeofactor(“Seniority.5”)</td>
<td>Tendency of deputy directors send out “information security influence” ties as compared to operational staff</td>
<td>0.15</td>
<td>0.47</td>
</tr>
<tr>
<td>nodeofactor(“Seniority.6”)</td>
<td>Tendency of directors send out “information security influence” ties as compared to operational staff</td>
<td>2.40**</td>
<td>0.89</td>
</tr>
<tr>
<td><strong>Network ties’ effects (edgecov)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Give work advice</td>
<td>Occurrence of “information security influence” tie is conditional on “give work advice” tie (H1)</td>
<td>1.18***</td>
<td>0.28</td>
</tr>
<tr>
<td>Trust</td>
<td>Occurrence of “information security influence” tie is conditional on “trust” tie (H2)</td>
<td>1.16***</td>
<td>0.25</td>
</tr>
<tr>
<td>Nominated role model</td>
<td>Occurrence of “information security influence” tie is conditional on “nominated role model” tie (H3)</td>
<td>1.33***</td>
<td>0.26</td>
</tr>
<tr>
<td>Nominated collaborator</td>
<td>Occurrence of “information security influence” is conditional on “nominated collaborator” tie (H4)</td>
<td>1.61***</td>
<td>0.24</td>
</tr>
<tr>
<td><strong>Structural terms</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dgwdsp(OTP)</td>
<td>Likelihood of employee A influences B’s information security behaviours indirectly via multiple employees</td>
<td>-0.03</td>
<td>0.03</td>
</tr>
<tr>
<td>dgwesp(OTP)</td>
<td>Likelihood of employee A influences B’s information security behaviours indirectly via multiple employees when there is a direct “information security influence” tie from A to B</td>
<td>0.40*</td>
<td>0.19</td>
</tr>
<tr>
<td>gwdegree</td>
<td>Homophily in the pattern of influencing others’ information security behaviours</td>
<td>-1.55</td>
<td>1.01</td>
</tr>
<tr>
<td>gwdegree</td>
<td>Homophily in the pattern of having information security behaviours influenced by others</td>
<td>-2.92**</td>
<td>0.92</td>
</tr>
<tr>
<td>isolates</td>
<td>Number of employees who neither receive nor send information security influence to others</td>
<td>-1.25*</td>
<td>0.61</td>
</tr>
<tr>
<td>idegree(0)</td>
<td>Number of employees who send but not receive information security influence ties</td>
<td>-1.53</td>
<td>0.94</td>
</tr>
<tr>
<td>odegree(0)</td>
<td>Number of employees who receive but not send information security influence ties</td>
<td>-0.52</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Akaike Information Criterion (AIC): 1119
Bayesian Information Criterion (BIC): 1260

**Note:** ***p<0.001; **p<0.01; *p<0.05**
Figures

Figure 1:
Figure 2:
Figure 3: