Title: Applications of social network analysis in behavioural information security research: concepts and empirical analysis

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

PII: S0167-4048(17)30063-9
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.03.010
Reference: COSE 1125

To appear in: Computers & Security

Received date: 16-1-2016
Revised date: 1-12-2016
Accepted date: 21-3-2017

Please cite this article as: Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno. Applications of social network analysis in behavioural information security research: concepts and empirical analysis, Computers & Security (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.03.010.

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.
Applications of social network analysis in behavioural information security research: concepts and empirical analysis

Duy Dang-Pham*, Siddhi Pittayachawan, Vince Bruno

School of Business IT and Logistics, RMIT University, Australia

Corresponding author’s email address: duy.dang@rmit.edu.au

Biographical Sketch

**Duy Dang-Pham** is completing his Ph.D. (Business Information Systems) in the School of Business IT and Logistics, RMIT University, Australia. He has been actively publishing in conference proceedings and journals since his undergraduate study. His primary research interests include information security/privacy behaviour and management, social media risks and supply chain management.

**Dr. Siddhi Pittayachawan** holds a Ph.D. in Business Information Systems from RMIT University, Australia. He is a Senior Lecturer of Information Systems and Supply Chain Management and a Program Director, Bachelor of Business (Honours), in the School of Business IT and Logistics, at RMIT University. His research interests focus on information system adoption, information security behaviour, green business, business education, measurement, and latent variable modelling.

**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:** The rapid digital transformation and technological disruption in modern organisations demand the development of people-centric security workplaces, whereby the employees can build up their security awareness and accountability for their actions via participation in the organisation’s social networks. The social network analysis approach offers a wide array of analytical capabilities to examine in-depth the interactions and relations within an organisation, which assists the development of such security workplaces. This paper proposes the novel and practical adoption of social network analysis methods in behavioural information security field. To this end, we discuss the core features of the social network analysis approach and describe their empirical applications in a real case study of a large organisation in Vietnam, which utilised these methods to improve employees’ information security awareness. Towards the end of the paper, a framework detailing the strategies for conducting social network analysis in the behavioural information security field is developed and presented.

**Keywords:** information security behaviour; information security compliance; information security management; information security governance; social network analysis
1 Introduction

The task of developing an information security workplace is growing in importance since modern companies are continuously digitalising their businesses and handling intensive volume of data. As employees bring innovative technologies along with potential security threats to the workplace (Harris, Ives, & Junglas, 2011; Weeger et al., 2015), organisations need to accommodate these disruptions, so to encourage flexibility and innovativeness while not compromising their information security. This sets the emphasis on analysing and exploiting the organisation’s social networks with appropriate methods to develop an effective people-centric security workplace, whereby the employees can build up their security awareness and accountability for their actions through social interactions and relations.

Unlike the traditional approach that focuses on perceptions and behaviours, social network analysis research directly examines the individuals’ environment consisting of interactions and relationships between individuals (Borgatti, Everett, & Johnson, 2013; Otte & Rousseau, 2002). By using network analysis methods, researchers can evaluate the structural features of the social environments such as connectedness, reciprocity, transitivity, or hierarchy, as well as the measures that inform the prominence of each actor in their networks (Borgatti et al., 2013; Hanneman & Riddle, 2005). In fact, social network analysis methods are most suitable for designing change programs and interventions for organisational development purposes (Gesell, Barkin, & Valente, 2013; Hatala, 2006). Since the management of information security concerns many socio-organisational factors such as interpersonal influence and sharing of knowledge that impact employees’ information security behaviours (Crossler et al., 2013; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014; Warkentin, Johnston, & Shropshire, 2011), the adoption of social network analysis becomes crucial.

Nevertheless, the empirical use of social network analysis techniques in behavioural information security field is limited despite its potentials. This research reviews the core concepts of this research approach and examines two organisational networks closely related to the management of information security behaviours: “information security influence” and “consumer IT adoption influence”. Throughout the paper, we present an empirical case study of a large interior contractor in Vietnam, which was collaborating with us in a project that utilised social network analysis methods to improve employees’ information security awareness. The aims of this paper are to introduce the potential applications of social network analysis in behavioural security research and demonstrate their uses in practicality. Towards the end of our paper, we propose a framework that summarises the strategies for conducting social network analysis in the behavioural information security field.

We organised the paper as followed. First, a literature review on the trends in behavioural information security field is present and explains our research motivations. Secondly, we review the core network measures and their potential applications in behavioural security context. To demonstrate the practical applications of SNA methods, we present an empirical case study of a large interior contractor in Vietnam. This contractor was collaborating with us to improve their employees’ information security awareness with SNA methods. Section 4 provides information about this contractor, followed by Section 5 that thoroughly diagnoses the organisation’s current security issues. Section 6 discusses in-depth analyses at the individual-level to select security champions for awareness diffusion. Section 7 reflects on the lessons learnt and devises a strategies framework to guide SNA research in behavioural security context. The paper concludes with Section 8, which outlines the limitations and future directions.
2 Literature review

2.1 Trends in behavioural information security field

People-centric security workplace refers to a work environment where the number of security controls is minimal while a security culture that emphasises personal accountability and responsibility is cultivated (Dang-Pham, Pittayachawan, & Bruno, 2015; Kirlappos, Beutament, & Sasse, 2013). Moreover, managers can foster such culture by focusing on the collective activities of the employees. The concept of this workplace is relevant to the data-intensive work in many modern organisations as well as their employees’ increasing adoption of technologies (e.g. mobile devices and software), which eventually make strict enforcement of complying with complex security procedures less feasible.

Likewise, recent trends in the behavioural information security field also focus on the effects of the work environment on employees’ security perceptions and behaviours. For instance, Willison and Warkentin (2013) extended the well-known Security Action Cycle and argued for the importance of the pre-kinetic events that explain how the interactions between the employees and their workplace would lead to the formation of misbehaviours. Similarly, the Emote Opportunity Model by Baskerville et al. (2014) aims to explain how the potential perpetrator’s observations of the workplace’s security features would result in actual abuses. Dang (2014) hypothesised that the employees would perform misbehaviours due to the stress that they experienced at their workplace. Kirlappos et al. (2014) conducted 118 interviews with employees from a large organisation, and they found that “shadow security” (i.e. security practices unknown to the organisation) stems from the unofficial security activities that take place within the departments such as informal induction and instructions.

In terms of security compliance, Warkentin et al. (2011) found the informal learning environment provides cues via supports and persuasion that enhance the employees’ confidence to perform security behaviours. All of these recent research (since 2011) show the emerging need to better understand how security workplace’s features can contribute to the employees’ security behaviours, as well as how to develop a people-centric security workplace. In fact, Kirlappos et al. (2013) argued that the traditional “command and control” security management approach often overlooks the employees’ needs and business processes, thus becomes unfit for modern organisations which encourage flexibility and innovativeness. These shortcomings call for support of having a more flexible approach to manage organisation’s security while prioritising alignment with the employees.

2.2 Research motivations

Developing people-centric security workplaces requires knowledge of the employees’ perceptions and behaviours, which are the core objectives of the behavioural security research field. One of the three important categories of behavioural security research consists of empirical studies that are grounded on theories (Siponen, Adam Mahmood, & Pahnila, 2014). These studies are important as they provide evidences derived from the reality, which validate the theoretical explanations of why and how the employees perform security behaviours. The nature of these studies satisfies the crucial requirement for achieving a balance between practicality and theories in information security research (Puhakainen & Siponen, 2010).

Sommestad et al. (2014) conducted a systematic literature review on the theories employed by contemporary studies to examine the contributing factors of security compliance. The result lists out the behavioural theories that have been predominantly tested such as Protection Motivation Theory, Social Control Theory, General Deterrence Theory, and Theory of Planned Behaviour (Sommestad et al., 2014). From this list, these researchers
extracted the good predictors of compliant and non-compliant behaviours, some of which characterised the interactions between the employees and their workplace such as perceived behavioural control, threat appraisal, descriptive and subjective norms, policy’s quality, and sanctions.

While prior studies have consistently found the mentioned factors able to explain security behaviours well, they focus solely on the individualistic cognition of the employees and thus provide limited contextual details of the work environment. Furthermore, the findings are also subject to the theoretical assumptions of the employed theories (Dang-Pham, Pittayachawan, & Bruno, 2014). For instance, in order to evaluate accurately the quality of security policies or the severity and certainty of formal sanctions, it is expected that the employees need to interact frequently with the information sources of the policy or sanctions. However, not all employees would have access to and read security policies (Wood, 2000) and this factor was mainly overlooked. Similar to reading security policies, there are also isolated employees in the workplace or those in virtual teams who have less access to the social activities, and thus may not perceive the effects of norms as much as the more exposed ones do. The study by D’Arcy and Hovav (2008) supported this argument as they found virtual employees perceive less deterrent effect from monitoring than non-virtual employees. As a result, Dang-Pham et al. (2014) suggested the use of social network analysis to shift the focus from the individualistic cognition to the interactions and relations between organisational objects (i.e. human and non-human) that characterise the structural features of the workplace. To validate their proposal, we collected empirical network data from a large interior contractor in a South East Asian country and demonstrate in this paper the analytical capability of social network analysis techniques in behavioural information security research.

2.3 An overview of social network analysis

As the name suggests, social network analysis (SNA) as a research approach sets emphasis on the networks, which could be interactions or relations, and studies their structural features. Researchers adopting SNA approach commonly prioritise the relationships (termed ties or edges) between the network’s actors (termed nodes or vertices) over the properties of the individual actors (Otte & Rousseau, 2002). This allows the social context of the actors, which is ignored in the traditional individualistic research approach, can be analysed more in-depth with SNA tools and techniques (Otte & Rousseau, 2002). As a result, the SNA approach aligns well with the aforementioned perspective and research intention, which treat information security as collective practices and focus on the socio-organisational interactions rather than the individualistic cognitive processes.

The use of SNA tools and techniques in the social sciences is not new. In fact, Borgatti and Foster (2003) shown the number of organisational studies that employed SNA approach has increased exponentially since the 1990s. Most recently, articles in prestigious journals started to discuss research directions and apply SNA techniques in areas such as information systems (Sykes, Venkatesh, & Gosain, 2009; Zheng, Padman, Krackhardt, Johnson, & Diamond, 2010). In contrast, only Dang-Pham et al. (2014) and Yoo and Lawrence Sanders (2013) have proposed the conceptual models and use of SNA in behavioural information security research so far. Amongst these works, Dang-Pham et al. (2014) outlined an agenda for using SNA to study malicious information security behaviours.

3 Core network measures and their applications

When performing SNA, researchers often examine the complete whole-network (which is characterised by its nodes and their ties), the nodes within that network, or the personal networks of the individual nodes (i.e. ego networks) (Borgatti & Foster, 2003; Otte &
Rousseau, 2002). At each level of analysis, researchers can use specialised software packages (e.g. UCINET, Pajek, SNA packages in R) to compute a wide range of network measures that can be analysed further. While we encourage readers to refer to the articles that explain in detail the network measures (often in a mathematical formula), our paper aims to provide a brief overview of these network measures such as their meaning and applications in the behavioural security research context. As a result, we remain consistent with our original objective, which is more about promoting the use of SNA techniques in behavioural information security research with empirical demonstrations. An overview of the network measures is provided in Table 1 below. The list of the network measures is not exhaustive, and we attempted to present the core measures that have potential applications in security research.
4 Demonstrating SNA applications in a real case study

To demonstrate empirically SNA’s analytical capability and the introduced concepts, we applied SNA to examine the information security environment of a company in Vietnam. Vietnam is a developing country and emerging IT sourcing hub in South East Asia. Due to the globalisation process, companies in Vietnam have been continuously improving their services and infrastructure to satisfy the international requirements. Many companies in Vietnam are starting to adopt globally acknowledged information security management standards and frameworks such as ISO 27001, COBIT, or ITIL. For example, ISO (2015) reported that there were 39 organisations in Vietnam certified for the ISO 27001 standard of security management in 2013. This paper discusses the practicality of SNA approach and its various tools by using the findings of a case study that we were collaborating with ABC, a large interior contractor in Vietnam of 374 office workers and more than 1,000 skilled workers in their factories. ABC is in the process of implementing their ISMS by following the guideline of ISO 27001, and they enlisted us to contribute academic advice to their implementation.

4.1 Diagnosis of case study’s security problems

Our meetings with ABC’s top management to diagnose the security problems concluded that their major and root issue is about the employees’ non-existing security awareness. Over the past two years, the network administrators in ABC have continuously found computer viruses infested their intranet due to the employees’ trivial and careless mistakes when using the Internet. These mistakes include downloading unapproved tools and applications (e.g. PDF converter), clicking on phishing e-mails or malicious Facebook messages, all of which had viruses implanted. In fact, IT staff at ABC has just recently stopped a “Locky” ransomware outbreak in their network. This ransomware locks the files on the computer after the end-user executes the malicious application, and the end-user must pay the “ransom” to regain controls over the locked files. Further investigation by tracing back to the ransomware’s source found that it originated from the computer of the human resource’s director, who downloaded an e-mail attachment that sent from his subordinate.

Due to these serious security issues frequently caused by careless actions, ABC sees conducting security awareness training as their top priority but also has several challenges in doing so. First, their previous experiences from conducting other types of work training and knowledge of the organisation’s culture suggest that launching a massive training workshop to all 373 employees would be inefficient. This is due to the large number of employees in a single workshop reduces the learners’ attention to the training contents. Moreover, the top management also rejected alternatives such as making training video and booklets and asking the employees to review them, since this approach lacks interactions.

The most feasible solution is to select security champions and have them diffuse security awareness in small groups, which can ensure both interactive engagement and the learners’ attention. Nevertheless, as most of ABC’s employees have never been interested in security topics before, even the top management found it very challenging to select the suitable candidates other than relying on a person’s formal seniority. Consequently, this provided an excellent opportunity to propose the use of SNA techniques to assist ABC in selecting the security champions and study their security implementation process.

4.2 SNA research design and action plan

Following the guideline of ISO 27001, we joined ABC’s security implementation project at the “Plan” stage which aims to outline the implementation methods and designing
appropriate security controls (ISO, 2015). Since one of the core strengths of SNA strategy is making interventions and analysing changes in the social networks (Cross, Laseter, Parker, & Guillermo, 2006; Dang-Pham et al., 2014), we decided to collect network measures before and after the implementation. More importantly, capturing the social networks before the implementation would provide a clear understanding of the current information security environment in ABC. At this moment, our project with ABC is still ongoing and this paper reports the findings of the initial stage. The subsequent phases involve having the security champions (selected from our social network analysis) execute the implementation plan and measure their effectiveness in improving their colleagues’ information security awareness.

From the diagnosis reported in the previous section, it is clear that the intervention is about using SNA methods to analyse network data and identify the suitable security champions for security awareness diffusion in the later stages. Furthermore, the initial diagnosis revealed that the root causes of the past security incidents include the employees’ careless uses of applications and attachments acquired from the Internet or social media. These IT uses have been recently investigated by studies as “shadow IT” (Silic & Back, 2014) and adoption of consumer IT (Harris et al., 2011), and these practices were argued to directly link with information security risks in organisations. Consequently, ABC’s top management is also interested in capturing the interpersonal influence regarding the employees’ adoption of the unofficial applications and software.

To capture information about the influences among employees pertaining to their adoption of information security practices and consumer IT, the following questions were included in the questionnaire:

- Please nominate maximum 07 colleagues who can influence your decision to use information security technologies and/or perform information security behaviours
- Please nominate maximum 07 colleagues who can influence your decision to use the technologies and devices that are not prescribed by ABC, but they can improve your work performance and/or solve your work issues

By asking these questions, we captured two social networks termed “influence security influence” and “consumer IT adoption influence”. We sent an online questionnaire to 374 ABC’s employees at all levels. After one month, we retrieved 264 valid responses (71% of ABC). Besides network data, we also extracted from their human resource’s databases the employees’ demographics such as gender, age, department, seniority (staff; manager; director), and tenure years at ABC. The analysis objectives and the detailed action plan to acquire the information desired by ABC can be summarised in Figure 1 below.

5 Diagnose the environment’s conduciveness for security awareness diffusion

Performing SNA at the network level allows the researchers to understand the structural features of the networks and identify quickly interesting actors or groups of actors. To begin, we visualise “influence security” network and perform some visual inspection on the visualised sociogram (Figure 2).

At first glance, the network looks thin since there are not many ties between departments, except the ties that connect all the departments with the three red nodes at the top of the figure. The size of the nodes in Figure 2 is proportional to their out-degree centrality, or the
sum of their outgoing ties that represent their security influence on other nodes. The direction of security influence is also visible by observing the black arrows, which point towards the nodes receiving influence from others. As seen, the three red nodes at the top are the IT department’s employees who hold tremendous controlling power as compared to other nodes. We also observed that while the architect division and construction department receive much influence from the IT employees, the project management department and factory division do not. Furthermore, there is active exchange of security influence between the construction and project management departments, which is understandable since these two departments constantly engage with each other in daily work.

According to our observation, the employees in ABC seem to perceive information security as something technical; thus, they would listen more to the IT employees who appear as having knowledge in this domain. After performing our independent visual diagnosis, we proceeded with reviewing the sociogram in Figure 2 with ABC’s top management. ABC’s top management agreed that the sociogram reflects accurately their company’s situation, which has been maintaining a “command-and-control” security management model. With this security management model, IT/security supports and authority are centralised to the technical departments such as IT and Business Solutions Provider (BSP). The top management also displayed great interests in the sociogram, especially when they observed the influence ties between pairs of employees that were unexpected to them despite their in-depth knowledge of the organisation’s internal relationships. It appears that we have achieved one of SNA’s goals, which is illustrating the invisible links in the organisation to its management.

The visual inspection further reinforces the top management’s resolve in decentralising the “command-and-control” security management model due to its disadvantages. On the one hand, the general director discussed his concerns in the meeting about the risk of the employees delegate their security responsibilities and duties to the technical staff, as well as the risk of collapsing the influence security network if one or more of the IT staff exit the company. The latter risk is particularly concerning to employees in the departments that lack within-ties and only accept influence that comes from the IT staff (e.g. after sale services, accounting, or project management). On the other hand, the vice director argued the main reason that resulted in the high out-degree of the IT staff could be caused by their formal job duties, which include offering security supports to everyone. Consequently, she reasoned that such risk is not too alarming since they can simply assign the job to the next suitable person. Nonetheless, they both acknowledged the risk of cascading failure in the situation that the few influential IT staff make a wrong security decision and have everyone follows it.

With the top management’s commitment to intervene and change the influence security network, we continued to identify the non-IT employees who can influence others’ security behaviours. To answer this query, we firstly performed descriptive analysis at the network level, and then we focused on the individual nodes. One way to understand the influencing relationships at network level is counting the ties within and between the departments. Due to the space limit, Table 2 displays only a portion of the calculated interrelationships amongst 20 business units in ABC.
The figures in the rows of Table 2 report the number of security influence ties sent from one department to another. For example, the IT department has 78 influencing ties coming towards the construction department. Consequently, the columns denote how many “influences” a department receives from another. We observed in Table 2 that besides the IT department, the project management department influences the construction department more (23 incoming ties versus 5). The use of Table 2 provides more visibility since it is more challenging to make this observation by looking at the sociogram illustrated in Figure 2.

More interestingly, employees within the construction department influence each other’s information security behaviours as much as the IT employees influence them (i.e. 69 ties versus 78). It might be tempting to conclude that an environment such as the construction department, where each member is capable of influencing the others, would be ideal for security awareness diffusion. However, a careful examination of the departments’ densities of the influence ties can tell otherwise. The density of a network is the proportion of observed ties amongst all possible ties. Based on this definition, we would then ask ourselves whether 69 ties would be a significant number, provided the size of the construction department.

It turns out that the 69 ties of self-influence are only equal to 0.9% of all possible ties in the construction department (the total number of possible ties is 7832). Similarly, 10 self-influencing ties of the project management department only constitutes to 1.8% of its total ties. In fact, large networks tend to have small densities which make them less connected (Borgatti et al., 2013).

6 Select security champions for security awareness diffusion

The top management at ABC decided to select, train, and then place local security champions in all departments. They believe that doing so would help to decentralise the “command-and-control” security management model and diffuse security awareness more effectively and efficiently. Furthermore, they also aim to have the security champions engage with the isolated nodes in Figure 2. We considered departments with higher density as more ready and conducive for security awareness diffusion, since there already exists the group norm that accepts within-group security influence. Consequently, we expected the local employees in those departments would effectively serve as security champions once they are empowered.

6.1 Determine the antecedents of security influence

After assess the departments’ conduciveness for security awareness diffusion, we proceeded with determining the determinants of security influence so to select the suitable candidates possessing the desired traits. In network and social influence literatures, homophily effects are well known as one of the key explanations for why people change their behaviours or beliefs to match with others. Homophily effects refer to the tendency for people to connect with those who share the same social attributes (e.g. gender, race, or class), and these effects have been consistently supported (Borgatti et al., 2013).

Besides the commonalities in social attributes, there have been theoretical and empirical evidence that support other demographic factors’ impacts on social influence. For instance, French & Raven’s (1959) social power theory posits that influential individuals can change others’ behaviours and beliefs by possessing different power bases, including the powers to reward, coerce, legitimate, as well as to act as a reference or expert (French & Raven, 1959). In organisational context, seminal researches asserted that the former three power bases can
associate with formal seniority and tenure (Borgatti & Cross, 2003; Cialdini & Goldstein, 2004; Ibarra & Andrews, 1993). Such association is expected since high-ranked executives often have the authority to reward, coerce, and legitimate their actions. Moreover, there is a notion that employees having longer service records tend to know more about the company, and thus are sought for advice more by newcomers (Wenger, 1998).

We also anticipated security influence would take place more between employees who work in the same department. The underlying rationale is that employees of the same department can be tightly linked by similar positional (i.e. occupied roles and patterns of connections) and close spatial proximities (i.e. physical locations), which are the important network mechanisms that explain social influence (Rice & Aydin, 1991). These proximities boost the chance for other influence mechanisms such as contagion (i.e. direct persuasion) and comparison to occur (Leenders, 2002). By engaging with a group of connected people in daily work and being able to receive relevant information from them in a fast and convenient manner, the employees within their department would be influenced to develop a shared perception and conform with the group’s norms. In fact, the empirical research by Borgatti & Cross (2003) confirmed that employees enjoy the benefits of having close physical proximity, which provide more knowledge of and access to other colleagues’ skills and improve their learning.

We were also interested in examining the effect of consumer IT adoption influence on security influence. This anticipated effect is consistent with the findings from our diagnosis of the security problems at ABC with its top management, which suggested that several security incidents such as the “Locky” ransomware outbreak were caused by the employees’ careless adoption of IT solutions. Moreover, the close link between consumer IT adoption in organisations and security issues have been confirmed by prior studies (Harris et al., 2011).

With the employees’ demographics extracted from the human resource database, we can apply network statistical tests to examine the anticipated effects and determine the mechanisms of security influence. Prior to performing such tests, a quick visual inspection of the influence security network can provide evidence that may intuitively support our hypotheses. In influence security network’s sociogram in Figure 3 below, the nodes were separated by their genders, where male employees are blue and locate at the top of Figure 3 and female employees are pink and located at the bottom of the figure. Moreover, only ties between nodes of the same gender were displayed to highlight same-gender influences. Furthermore, the shapes of the nodes represent their formal seniority (i.e. circle=operational staff; square=manager; triangle=director). Managers and directors were coloured as yellow and red respectively.

The homophily effect that encourage security influence to occur between nodes of the same gender is clearly visible in the male group. In contrast, the female employees do not appear to influence each other much but receive influences from the IT employees (ties are not displayed in the figure). The managers tend to have slightly higher degree centrality than operational staff, which hints that formal seniority may play a role in exerting security influence. With regard to the effect of sharing department membership on security influence, Figure 2 of the whole network discussed in the previous section has provided a visual confirmation. In particular, the clustered departments, which appear to have more security influence ties within than in-between, suggest that sharing the same department membership can affect the occurrence of security influence ties.
Provided with the findings that come from prior studies and our visual inspection, we proceeded with running the multiple regression QAP procedure (MR-QAP) which uses one or more networks to predict another. We transformed the employees’ demographics into matrices to be analysed with influence security network. For example, we generated matrices that describe the employees’ similarities and differences in age (difference between two nodes’ ages), gender (1=same gender, 0=different gender), or tenure years. It is important to note that researchers need to employ permutation tests such as MR-QAP for testing hypotheses that involve network, since the nature of the network data violates the independence assumption of tradition statistical tests (Borgatti et al., 2013). In this analysis, we ran Double Decker Semi-Partialing MR-QAP procedure with 5000 random permutations. The model fits well ($p$-value=0.000) with an adjusted $R^2$ of 30 per cent. The results are reported in Table 4.

The model’s results supported all anticipated mechanisms of the occurrence of security influence except the homophily effect of gender. Of most importance is the statistically significant and high predicting effect size of influence consumer IT adoption network ($\beta=0.542$). Employees who influence the others’ adoption of consumer IT solutions also influence their security perceptions and behaviours. Moreover, employees who have longer tenure years at ABC and higher-ranked positions tend to influence others ($\beta=0.028$ and $\beta=0.024$ respectively). Similarly, sharing the same department membership also tends to result in security influence ties ($\beta=0.011$). In contrast, having the same gender is not a significant predictor of security influence.

With the conduciveness for security awareness diffusion of the environments evaluated and the mechanisms of security influence confirmed, we proceeded with selecting the potential security champions. As mentioned previously, ABC plans to select security champions from 18 work units and have them diffuse security awareness in their local units. Due to the space constraint, we only discuss the selection process for the construction department in this paper. We went through the same process with ABC’s top management to select the security champions for the rest of the departments.

Similar to the top-down approach that we have adopted so far, we began with visualising the influence security network of the construction department to gain an overview of the situation.

The influence security network of the construction department in Figure 4 appears fragmented and consists of four main components: the central red actors, the grey pair, the blue group, and the black isolated nodes on the left. The black nodes’ isolation could be due to either (1) they did not answer the survey or (2) they did not receive nominations as influential from those who participated in the survey. In any case, they appear not very influential in this network. It is clear that one of the important goals of the security awareness diffusion in the construction department would be linking these isolated nodes with the rest. Moreover, there are interesting patterns within the central component. Specifically, we have two senior staff (squared shape) on both sides of the red component, and in between are a few operational staff (rounded shape) of notable sizes. In this sociogram, the nodes’ sizes reflect their sum of outgoing ties (termed “out-degree”), or the number of people they could directly influence security behaviours.
6.2 Evaluate the prominent statuses of employees in influence security network

Identifying the influential employees requires calculations of the network measures that we have discussed in Table 1. Besides the nodes’ out-degree measures, we examine their “Beta” and “flow betweenness” centrality measures (Table 5). It is worth mentioning that while it may be tempting to use “closeness” centrality to incorporate the actors’ indirect influencing ties, the use of this measure would not be appropriate in our case. The main reason being that closeness centrality assumes the flows to travel via shortest paths only, whereas influences could take any directions in parallel (Borgatti, 2005).

Table 5 summarises the centrality measures and demographics of 10 influential employees within the construction department. Since out-degree reflecting an employee’s ability to influence the others’ security behaviours directly, TH#5 (out-degree=6) is the most prominent actor who received six direct nominations from her peers. While ABC can consider TH when they want to diffuse information security perceptions within the construction department, we advised them to evaluate the measures of flow betweeness and Beta centrality.

An actor has high Beta centrality when he or she has connections with others who are well connected. Even though TC#1 has fewer direct out-degree than TH#5, she can influence people who can then continue to influence even more people in the network (Beta cent=902.24). Another actor with high Beta centrality is TL#2 (Beta cent=598.01). However, as shown in Figure 5 below, TL#2’s position is rather isolated and has his influence completely controlled by the gatekeeper above him. In this case, LH#3, which has the third-ranked Beta centrality, is a better candidate since she has more routes and freedom to reach the rest of the network. We recommended using both TC#1 and LH#3 as the sources of influence in the construction department.

Flow betweeness counts the times that a node lies in between any paths. Employees having high flow betweeness could control the contents of the flows that go through them and potentially alter these contents. As a result, while TC#1 and LH#3 send out the original messages and ideas about information security, they have the risk of having their messages intercepted and changed by in-between employees such as TH#5 or AN#9 (flow betweeness=0.20 and 0.21 respectively). Consequently, we advised ABC’s management about the roles of these network interceptors and suggested them to cooperate with the main influencers TC#1 and LH#3.

Finally, we calculated another measure called “Reach centrality”, which describes how far a node can reach other nodes in the network. This Reach centrality measure is shown in Figure 5 as proportional to size of the node’s labels. The larger a node’s label is, the further it can reach. As seen, TH#5 has a wide reach (Reach centrality=8.67) which is equivalent to LH#3 (9.17) and TC#1 (7.50), and TH#5 intercepts influences that come from LH#3. From the management’s perspective, the support role of TH#5 is much valuable than AN#9.

However, TH#5 has a disadvantage of not being able to influence prominent actors (i.e. low Beta centrality), so her influences may stop somewhere before they can reach the rest. While TC#1 may reach fewer nodes than TH#5 (label’s size is slightly smaller), she clearly has more alternative routes and levers (i.e. TP#7 and AN#9). As a result, the selection of influential employees for the security champion’s role needs to balance both of these.
measures. We proposed a list of criteria to ABC’s top management, which they can use to profile the potential security champions, after performing the discussed analyses so far. The criteria and their meanings are summarised in Table 6 below.

7 Discussion

We identified several practical and theoretical implications in our paper and particularly from the case study about security awareness diffusion at ABC. Specifically, practical contributions include the confirmed determinants of security influence between employees and a systematic guideline about applying SNA methods to diffuse security awareness. Theoretical implications include the review of the core network concepts and future directions for a completely unexplored area of network research in behavioural security field.

7.1 Applications of SNA in security awareness diffusion and compliance

As demonstrated throughout our case study, ABC’s top management was satisfied with the network analysis results, especially the visualised networks of security and consumer IT adoption influences that are inherently invisible to them. By examining the illustrated networks and their statistics, the top management was able to identify the workgroups that are conducive for security awareness diffusion, as well as the suitable candidates to serve as effective security champions.

Despite the growing importance of selecting security champions (Gabriel & Furnell, 2011) and developing a user-centric security workplace (Dang-Pham et al., 2015; Kirlappos et al., 2013), the number of contributions in these areas remain limited. We found only the work of Gabriel & Furnell (2011) which provided a scientific guideline for identifying security champions by using a psychometric personality test. In practice, many security managers such as ABC rely on subjective expert judgements to select security champions, which often base on the candidates’ formal seniority in the workplace. While formal seniority is not the only criterion for influencing security behaviours and scoring highly on a personality test does not guarantee the person’s influential status, our study complements these existing approaches by offering a direct way to capture security influence in the workplace and profile security champions according to their networks and social positions.

However, a caveat of this network analysis approach is that security managers need to ensure the selected security champions must be empowered and have the skills to diffuse security awareness. In fact, some of the security champions selected at ABC expressed their concerns that they would not have the time and skills to do presentation and hold training workshops. We had to conduct a workshop for these security champions to train their diffusion skills, so that they can feel more comfortable at performing the assigned tasks. In addition, we also had ABC’s top management supports in allocating time for the security champions’ tasks and setting up key performance indices for recording and rewarding their contributions.

7.2 Applications of SNA in preventing violations and malware outbreak

In behavioural security research, good and bad security behaviours are of equal importance. One of the crucial research topics is about human vulnerabilities, which include intentionally misbehaviours and careless mistakes such as downloading virus-embedded files from phishing e-mails, circulating harmful files, or sharing accounts and passwords in daily work. Several recent behavioural security studies have investigated concepts such as shadow security and shadow IT that result from the diffusion of misleading or false information security practices and beliefs (Fuerstenau & Rothe, 2014; Kirlappos et al., 2014; Silic & Back, 2014). As discussed in our case study, the uncontrolled diffusion and adoption of
consumer IT solutions is also a vital human vulnerabilities in many modern workplaces (Harris et al., 2011; Ortbach, Koeffer, Bode, & Niehaves, 2013).

For instance, Kirlappos et al. (2014) found from their interviews that there are employees who are interested in protecting the organisation’s information security but fail to cope with the prescribed security practices and policies. Consequently, they invent their own security workarounds and propagate them within the workplace (usually via the immediate supervisors), which contain security vulnerabilities. Similarly, it is very challenging for IT/security managers to detect to what extent their end-users have adopted unapproved IT solutions or shadow IT in the workplace (Fuerstenau & Rothe, 2014; Silic & Back, 2014). Moreover, the effect of norms spreads the adoption of such IT solutions and their security vulnerabilities even further (Ortbach et al., 2013).

For controlling the adoption of consumer IT and their security vulnerabilities, security researchers and practitioners have been developing monitoring systems and applications that can automatically capture and analyse the organisation’s network traffic. With network analysis techniques, we have found a few recent studies such as the work of Fuerstenau & Rothe (2014), which treated the system modules and applications as nodes and their co-occurrence in the workplace as ties. Similar to the proposed approach in this paper, they calculated and evaluated the applications’ centrality measures to identify shadow IT amongst them. Such example demonstrates how practitioners can combine the analytical capabilities of network approach with the existing automatic monitoring systems and tools to manage the human vulnerabilities caused by their consumer IT adoption better.

Nevertheless, there are networks that will be more challenging if not impossible to capture. Furthermore, different types of networks require careful uses of relevant network measures and interventions to make use of them. In the following section, we elaborate the detailed strategies for conducting network analysis in security management and research.

7.3 Strategies for behavioural security SNA in practice and research

Figure 6 illustrates our recommended strategies and pathways to conduct behavioural network analysis, which starts from identifying the networks of interest and objectives to the specific software for each type of analysis.

First, there are three types of behavioural security networks of different visible natures, which network analysts can capture by using automatic monitoring tools, questionnaire, or interview. As seen in the flowchart, the sharing of accounts or circulation of suspicious files in the Intranet can be captured easily by network traffic monitoring tools. Such tools can also capture the employees’ exchange of security advice, but we expect they would have limited use since there would be more ad-hoc security advice that are communicated verbally in daily work (Dang-Pham et al., 2015; Kirlappos et al., 2014; Yoo & Lawrence Sanders, 2013). Likewise, capturing actual provision of security troubleshoot between employees or more extreme behaviours such as whistle blowing security violations will require using questionnaire or interview to ask the employees directly. For networks of sensitive behaviours such as whistle blowing security violations of others, we recommend using vignette-based survey as employed by prior studies about malicious security behaviours (Siponen & Vance, 2010).

Finally, we have the networks that are inherently invisible to observation, such as interpersonal influences and personal awareness of others’ skills and knowledge. For these networks, the uses of questionnaire and interview are recommended (Borgatti et al., 2013). Our case study is the closest example of how to capture security influence, which asked
directly the employees to nominate colleagues who can influence their security behaviours. For the awareness of others’ skills network or termed “cognitive social structure” (Heald, Contractor, Koehly, & Wasserman, 1998), we suggest asking the employees list out the colleagues who possess different security skills. Such analysis will reveal whether the employees know where to seek security supports and advice from, and security managers can adjust the organisation’s security resources accordingly.

After cleaning the network’s data, the network analyst decides which objectives to pursue and select the appropriate network analysis methods. For security awareness diffusion, our case study has performed all three types of analysis including identifying key players, clustering nodes, and performing inferential analysis such as the use of QAP regression. However, we did not discuss the latest clustering techniques in our case study such as latent position cluster modeling due to the space constraint.

Similar to the agenda of Dang-Pham et al. (2014) discussed at the beginning of this paper, network analysis techniques can be readily combined with traditional analysis such as structural equation modeling (SEM) or partial least squares path modeling (PLS-PM). We have also mentioned a few empirical examples which used network measures as predictors and predicted variables in regression analyses (Sykes et al., 2009; Zheng et al., 2010). We recommended future studies about behavioural security networks to adopt more advanced inferential analysis methods such as exponential random graph modeling (ERGM) and actor-based modeling.

8 Limitations and conclusion

While SNA as a research approach provides the analytical capabilities to explore the socio-organisational topics in behavioural information security research, there are several limitations and challenges. Whole-network analysis which focuses solely on one company would have limited generalisability (Zheng et al. 2010), and thus would bring more values when being conducted in a form of an experiment, case study, or action research (which aims at inducing and evaluating changes). In fact, many well-known network studies are experiments and quasi-experiments which consist of at least two stages of pre- and post-tests (Borgatti et al., 2013). Moreover, advanced SNA techniques such as ERGM could overcome generalisability issues by producing estimated findings based on simulations. Behavioural security network researchers can also take the ego network analysis approach which employs the traditional survey method combined with random sampling to increase generalisability (Borgatti et al., 2013). In addition, SNA focuses more on understanding the structural features of the networks rather than their in-depth stories and meanings, thus invites the use of qualitative methods to complement SNA’s findings (Hoppe & Reinelt, 2010).

Collecting network data has several challenges in terms of reliability, validity, and ethical issues (Borgatti et al., 2013), especially for whole-network research. Specifically, potential issues include omission of nodes/ties (due to the defined boundary of the network) or retrospective errors (i.e. asking about interactions and relations that are hard to recall) that could affect the study’s reliability or validity. More important, we found the intrusive nature of network surveys especially concerning in behavioural security research. For example, employees would feel reluctant to report interactions such as delegating security responsibilities or sharing passwords and access rights, since these behaviours are labelled as negative by the management and they could trace back to the real names of the employees who provided the answers. While this issue can be minimised in traditional survey research by anonymising the participants or using vignettes (e.g. Siponen and Vance 2010), whole-network studies require the participants to provide their real names to map their connections.
As a result, this highlights the importance of wording the questions appropriately, as well as having the industry partners and researchers fully committed in safeguarding the data’s confidentiality to improve the participants’ confidence in completing the survey.

Throughout this paper, we have firstly reviewed the existing behavioural security network studies and elaborated the core concepts, then demonstrated empirically how SNA can be practically applied in a real case study to assist its security awareness diffusion. Within the space limit, we have shown three network analysis directions which include identifying security champions, detecting the workgroups conducive for security awareness diffusion, and determining the antecedents of security influence in the workplace. Practical implications such as a systematic approach to select and make use of security champions were presented, and future studies can consider performing the mentioned inferential analyses to test network theories that extend our knowledge of security behaviours. As discussed previously in the flowchart, our proposed network analysis approach is not limited to end-users’ security compliance but also malicious security behaviours and human vulnerabilities.

With the rapid digital transformation in modern organisations that require innovative adoption of new IT solutions to handle large amount of data in daily work, there is a demand for new ways of thinking and novel approaches in the behavioural security domain. Moreover, it would eventually reach the point where the traditional “command and control” model of security management becomes inapplicable, if not even obstructive to effective daily operations. While the traditional perspective that focuses on the individualistic end-users will remain vital for revealing the factors that motivate or discourage people to perform good or bad security behaviours, the network perspective contributes knowledge of the mechanisms in the environment that put those factors in practice. Furthermore, it brings new paradigms, methods, and concepts to the current discussions and helps to enrich our knowledge. We anticipate the adoption of SNA approach would produce radical and exciting contributions that can complement or even challenge current theories in the behavioural security field, and we wish to offer this paper as the foundation for future adoption of the SNA approach.

REFERENCES


Information Management & Computer Security, 22(1), 42–75.


Figure 1: Action plan of network analysis project to diffuse security awareness in ABC

Figure 2: Influence security network at ABC (n=264)
Figure 3: Influence security network separated by genders

Figure 4: "Influence security network" of Construction department (n=89)
Figure 5: "Information security influence" network of Construction department (node’s size=Beta centrality; label’s size=Reach centrality; green=high flow betweenness)
Figure 6: Strategies for conducting behavioural security network analysis
<table>
<thead>
<tr>
<th>Network measure</th>
<th>Meaning</th>
<th>Potential application</th>
<th>Example</th>
<th>Reference of example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whole network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cohesion</td>
<td>A set of measures that denote the connectedness of a network</td>
<td>Depends on the nature of the network, cohesion measures can have different meanings. For instance, dense and connected “security advice” network allows security directives to flow more freely. A dense “influence security” network may describe a workplace where anyone (not necessarily with formal authority) could influence each other’s security behaviour.</td>
<td>Measure the accessibility of knowledge sources in a workplace</td>
<td>Cross, Laseter, Parker, &amp; Velasquez (2004)</td>
</tr>
<tr>
<td>Triad census</td>
<td>The number of different configurations that involve three nodes and their ties</td>
<td>This statistic allows practitioners to analyse transitivity in the network. For instance, practitioner can detect relationships such as A and B influences each other’s security behaviour, then both influence C. This might be interpreted as characterising the relationship where two superiors A and B discussing security directives and pass them down to the junior employee C. Similar to cohesion measures, triad censuses are most informative when they are compared amongst different networks (Borgatti et al., 2013).</td>
<td>Count “gossip” triads between every combination of one supervisor and two subordinates to understand gossiping behaviour</td>
<td>Ellwardt, Wittek, &amp; Wielers (2012)</td>
</tr>
<tr>
<td>Node</td>
<td>The sum of direct connections coming towards (in-degree) or out (out-degree) from a node</td>
<td>Practitioners can use degree centrality to detect influential actors in the network. For example, the actors having a high out-degree in the “give security advice” network are those who are commonly</td>
<td>Select “go-to” people in expertise network</td>
<td>Cross et al. (2004)</td>
</tr>
<tr>
<td>Centrality</td>
<td>Definition</td>
<td>Details</td>
<td>Select/Measure</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Closeness centrality</td>
<td>The sum of shortest distances from a node to all other nodes</td>
<td>Practitioners can use closeness centrality to detect actors who can quickly reach or send information to the others (i.e. those whose raw sum of shortest distances is small). However, it was noted that the practical use of closeness centrality is more limited in directed and/or fragmented graphs (Borgatti et al., 2013; Butts, 2008).</td>
<td>Select actors who would receive novel information early</td>
<td>Borgatti (2005)</td>
</tr>
<tr>
<td>Betweenness centrality</td>
<td>The sum of shortest paths that pass through a node</td>
<td>Betweenness centrality counts the times that a node lies in between two other nodes. These in-between nodes gain power in the social network as they can intercept information flows and receive unique information from different sources. The common betweenness centrality (Freeman betweenness) was argued unsuitable for information or influence networks due to its assumption which only takes into account the shortest paths, whereas the diffusion of information or influence does not necessarily follow the shortest paths (Borgatti, 2005). An alternative measure which takes into account all possible paths, termed “Flow betweenness”, is more preferred for diffusion of information or influence (Sparrowe &amp;</td>
<td>Determine actors with high betweenness centrality, who are the vulnerabilities that disrupt information flow if removed</td>
<td>Hatala (2006)</td>
</tr>
<tr>
<td>Measure</td>
<td>Description</td>
<td>Example</td>
<td>Reference</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>Eigenvector centrality</td>
<td>Denotes the importance of a node based on its direct connections with other nodes, and takes into account how well connected these nodes are</td>
<td>An actor with high eigenvector centrality would be potential for diffusing security directives or influence to a wider audience (out-eigenvector centrality). For directed graph, the use of Bonacich or beta centrality is preferred (Borgatti et al., 2013).</td>
<td>Measure actors’ power in a network about giving helps for information system adoption</td>
<td>Sykes, Venkatesh, &amp; Gosain (2009)</td>
</tr>
<tr>
<td>Structural equivalence</td>
<td>Denotes the similarities between nodes based on their similar connections to a set of nodes</td>
<td>Practitioners can use structural equivalence to identify roles of actors in the social network, and predict whether nodes connected to similar people would develop similar perceptions and behaviours as well.</td>
<td>Evaluate peer comparison process in information system adoption</td>
<td>Zheng et al. (2010)</td>
</tr>
<tr>
<td>Cohesion</td>
<td>Similar to whole network’s cohesion</td>
<td>Similar to whole network’s cohesion</td>
<td>Determine the number of information resources controlled by an actor</td>
<td>Sykes, Venkatesh, &amp; Gosain (2009)</td>
</tr>
<tr>
<td>Structural hole’s measures</td>
<td>A set of measures that concern the missing ties between the alters (i.e., neighbours) of the focal node (i.e. ego)</td>
<td>When there are many interrelationships amongst the focal node’s neighbours, these neighbours are redundant because they may provide low-value (duplicated) information to the focal node. Effective size is a measure that takes into account this redundancy and informs the value of the ego network. Another measure for detecting structural holes is termed constraint. Practitioners can use these measures to examine how valuable an ego network is in relation to the others.</td>
<td>Identify actors who may commit unethical behaviours in the workplace due to having many structural holes</td>
<td>Brass, Butterfield, &amp; Skaggs (1998)</td>
</tr>
<tr>
<td>Brokerage role</td>
<td>Similar to triad census, this measure reports the types of roles of a node</td>
<td>Depends on a node’s attributes and ties with the others, that node can fall into five roles: coordinator, gatekeeper, representative, consultant, and liaison. For instance, node B is a gatekeeper if B is in the same department with C, and B receives information from A. In contrast, B is a consultant if B liaises between A and C, and B belongs to a department different than A and C.</td>
<td>Identify and optimise organisational knowledge paths by employing actors of different brokerage roles</td>
<td>Kim, Yang, Hau, Seo, &amp; Ghim (2009)</td>
</tr>
</tbody>
</table>
Table 2: Ties amongst departments

<table>
<thead>
<tr>
<th></th>
<th>Factory</th>
<th>BusDev</th>
<th>Architect</th>
<th>Construction</th>
<th>HR</th>
<th>IT</th>
<th>PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory</td>
<td>57</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>BusDev</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Architect</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Construction</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>69</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>HR</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IT</td>
<td>17</td>
<td>7</td>
<td>59</td>
<td>78</td>
<td>4</td>
<td>5</td>
<td>27</td>
</tr>
<tr>
<td>PM</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 3: Ties and density of departments

<table>
<thead>
<tr>
<th></th>
<th>Number of ties</th>
<th>Density</th>
<th>Density (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory</td>
<td>57</td>
<td>0.048</td>
<td>4.8%</td>
</tr>
<tr>
<td>Business development</td>
<td>1</td>
<td>0.011</td>
<td>1.1%</td>
</tr>
<tr>
<td>Architect</td>
<td>43</td>
<td>0.011</td>
<td>1.1%</td>
</tr>
<tr>
<td>Construction</td>
<td>69</td>
<td>0.009</td>
<td>0.9%</td>
</tr>
<tr>
<td>Human resource</td>
<td>0</td>
<td>0.000</td>
<td>0.0%</td>
</tr>
<tr>
<td>IT</td>
<td>5</td>
<td>0.417</td>
<td>41.7%</td>
</tr>
<tr>
<td>Project management</td>
<td>10</td>
<td>0.018</td>
<td>1.8%</td>
</tr>
</tbody>
</table>

Table 4: MR-QAP results (bolded figures are statistically significant results having p-value lower than 0.05)

<table>
<thead>
<tr>
<th></th>
<th>Un-Std</th>
<th>Std Coef</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>0.003</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>Consumer IT adoption influence ties</td>
<td>0.592</td>
<td>0.542</td>
<td>0.000</td>
</tr>
<tr>
<td>Differences in seniority</td>
<td>0.005</td>
<td>0.028</td>
<td>0.021</td>
</tr>
<tr>
<td>Differences in tenure</td>
<td>0.000</td>
<td>0.024</td>
<td>0.029</td>
</tr>
<tr>
<td>Same department</td>
<td>0.003</td>
<td>0.011</td>
<td>0.021</td>
</tr>
<tr>
<td>Same gender</td>
<td>0.000</td>
<td>0.002</td>
<td>0.321</td>
</tr>
</tbody>
</table>
Table 5: Centrality measures

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Out-degree</th>
<th>Flow btw</th>
<th>Beta cent</th>
<th>Reach cent</th>
<th>Age</th>
<th>Tenure at ABC</th>
<th>Seniority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TC</td>
<td>5</td>
<td>0</td>
<td>902.24</td>
<td>7.50</td>
<td>26</td>
<td>1</td>
<td>Staff</td>
</tr>
<tr>
<td>2</td>
<td>TL</td>
<td>2</td>
<td>0</td>
<td>598.01</td>
<td>3.83</td>
<td>24</td>
<td>0</td>
<td>Staff</td>
</tr>
<tr>
<td>3</td>
<td>LH</td>
<td>4</td>
<td>0</td>
<td>309.71</td>
<td>9.17</td>
<td>43</td>
<td>20</td>
<td>Manager</td>
</tr>
<tr>
<td>4</td>
<td>SM</td>
<td>3</td>
<td>0</td>
<td>306.72</td>
<td>7.67</td>
<td>26</td>
<td>4</td>
<td>Staff</td>
</tr>
<tr>
<td>5</td>
<td>TH</td>
<td>6</td>
<td>0.20</td>
<td>305.25</td>
<td>8.67</td>
<td>38</td>
<td>1</td>
<td>Staff</td>
</tr>
<tr>
<td>6</td>
<td>AL</td>
<td>5</td>
<td>0</td>
<td>302.75</td>
<td>7.08</td>
<td>33</td>
<td>12</td>
<td>Staff</td>
</tr>
<tr>
<td>7</td>
<td>TP</td>
<td>2</td>
<td>0.14</td>
<td>300.75</td>
<td>4.00</td>
<td>32</td>
<td>1</td>
<td>Staff</td>
</tr>
<tr>
<td>8</td>
<td>QN</td>
<td>2</td>
<td>0</td>
<td>300.75</td>
<td>4.00</td>
<td>35</td>
<td>2</td>
<td>Staff</td>
</tr>
<tr>
<td>9</td>
<td>AN</td>
<td>2</td>
<td>0.21</td>
<td>300.25</td>
<td>3.00</td>
<td>27</td>
<td>0</td>
<td>Staff</td>
</tr>
<tr>
<td>10</td>
<td>QH</td>
<td>1</td>
<td>0.10</td>
<td>299.75</td>
<td>3.00</td>
<td>26</td>
<td>0</td>
<td>Staff</td>
</tr>
</tbody>
</table>
Table 6: Criteria for selecting security champions at ABC

<table>
<thead>
<tr>
<th>Criteria for selecting security champions</th>
<th>Meanings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work in the department targeted for security awareness diffusion</td>
<td>Confirmed positive effect of sharing department membership suggested that local security champions could diffuse security awareness more effectively.</td>
</tr>
<tr>
<td>Have formal seniority (i.e. manager or director)</td>
<td>Confirmed positive effects of seniority and tenure suggested that these traits can increase security influence.</td>
</tr>
<tr>
<td>Have tenure longer than the average tenure in the target work unit</td>
<td>Often give advice or can influence the others’ adoption of IT solutions</td>
</tr>
<tr>
<td>Confirmed positive effect suggested that individuals who influence others’ adoption of consumer IT solutions tend to influence their security behaviours and perceptions as well. While qualitative findings are required to understand the underlying reasons, it can be due to the influences of consumer IT and security both require technical knowledge. As a result, the technical-savvy employees at ABC may persuade their colleagues more.</td>
<td></td>
</tr>
<tr>
<td>Have high degree centrality in influence security network</td>
<td>Number of employees that the security champion can most likely and directly influence security behaviours and perceptions</td>
</tr>
<tr>
<td>Have high Beta centrality in influence security network</td>
<td>Potential of the security champion in influencing indirectly the others’ security behaviours and perceptions</td>
</tr>
<tr>
<td>[Optional] Have high flow betweenness in influence security network</td>
<td>Ability of the security champion to control and manipulate the flow of security information and influence ABC’s top management can convince the employees with high flow betweenness to leverage the security champions’ influence and prevent them from intercepting the influence’s flow.</td>
</tr>
<tr>
<td>[Optional] Have high reach centrality in influence security network</td>
<td>Potential of the security champion in influencing all employees in a work unit Beta centrality may provide a more practical measure for such potential, or ABC’s top management can consider appointing more than one security champion per work unit.</td>
</tr>
</tbody>
</table>