Exploring behavioral information security networks in an organizational context: an empirical case study

Duy Dang-Pham*, Siddhi Pittayachawan, and Vince Bruno
School of Business IT and Logistics, RMIT University

*Corresponding author’s e-mail address: duy.dang@rmit.edu.au

Abstract:

The purpose of this research is to propose network research as an alternative approach in the behavioral security field. A case study was conducted in a large interior contractor to explore eight organizational networks, four of which focus on security behaviors. The researchers employed social network analysis methods, including quantitative and qualitative ones, to analyze the case study’s data and demonstrate the analytical capability of the network analysis approach in the behavioral security field. Key features of the security networks’ structures include high transitivity, hierarchy, and centralization, whereas reciprocity and density are lower than other organizational networks. Moreover, work-related interactions were found to impact security influence, amongst which giving IT advice increases significantly one’s influential status in security matters. Practical implications include suggestions about the use of network analysis methods as a tool for security managers to monitor their behavioral security networks and devise appropriate strategies. Potential research directions are also elaborated, which future research can employ and promote the novel and practical use of network analysis techniques.

Keywords:

social network analysis; security behavior; security compliance; security influence; organizational behavior
1 INTRODUCTION

In recent years there has been a growing focus on the human and socio-organizational issues in information security. The end users are recognized as the “weakest link” in the security chain due to their vulnerability against a plethora of security threats, and modern organizations can no longer rely solely on technological security controls to protect their strategic information systems (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dang-Pham & Pittayachawan, 2015; Kirlappos, Parkin, & Sasse, 2014). As a result, a number of behavioral information security research emerged and formed their own important research field whose primary role is to investigate the end user’s security perceptions and behaviors (Crossler et al., 2013).

These behavioral information security studies have been contributing practical and theoretical implications to the body of knowledge. For instance, behavioral security researchers were able to determine important motivations of the employees’ intention to comply and actual compliance with security policy, such as security attitude and subjective norms (Bulgurcu et al., 2010; Herath & Rao, 2009), perceptions of security behaviors and threats (Dang-Pham & Pittayachawan, 2015; Siponen, Adam Mahmood, & Pahnila, 2014; Vance, Siponen, & Pahnila, 2012), or perceptions of security sanctions (Bulgurcu et al., 2010; Herath & Rao, 2009). It can also be observed that the predominant approach of prior studies involves testing hypotheses drawn from theories about the individual’s cognitive processes, such as Theory of Planned Behavior (Ajzen, 2011), Protection Motivation Theory (Maddux & Rogers, 1983; Norman, Boer, & Seydel, 2005), and General Deterrence Theory (Straub, 1990). This research approach, which focuses on the individualistic decision-making process, continues in more recent behavioral security studies. While the researchers fully acknowledge the contributions to security practices that came from this traditional research approach, its current focus overlooks the roles of the interactions and relationships amongst individuals in relation to behavioral security.

The objective of this research is to promote an alternative approach in the behavioral security field and advocate its future adoption. This proposed research approach, which places emphasis on the networks of security behaviors rather than the end-users’ individualistic cognitive processes, comprises concepts and methods that have not been adopted in the behavioral security field thus far. These concepts and methods will be empirically demonstrated in a case study, which provides practical recommendations about harnessing organizational networks to raise the end-users’ security awareness. Furthermore, the case study elaborates on the methodological considerations when conducting network analysis, as well as the potential directions that can be pursued by future research.

This paper begins with discussing the theoretical aspects of the network research approach in the literature review section, which include definitions of behavioral security and organizational networks and how they can be related to each other. The rest of this paper provides an empirical case study to demonstrate the potentials of the network research approach, and most importantly explore the characteristics of the networks and their implications. The paper concludes by discussing the practical and theoretical implications of the network research approach, as well as elaborating the directions for future behavioral security research interested in this approach.
2 LITERATURE REVIEW

2.1 The emerging theme in behavioral security field

As mentioned in the introduction section, recent behavioral security studies are employing theories and frameworks from other fields to explore the contingent factors of the end user’s security behaviors. For instance, Warkentin et al. (2011) employed Social Learning Theory and found that the employee’s self-efficacy to complete security tasks can be improved by having situational support (i.e. availability of help from colleagues and materials), verbal persuasion (i.e. instructions and feedback), and vicarious experience (i.e. indirect experience from observing or job shadowing). Ifinedo (2014) adopted Social Bonding Theory and found the four types of bonds (i.e. attachment, commitment, involvement, and belief) can motivate the employee’s intention to comply with security policy indirectly via attitude and subjective norm. Likewise, new theoretical frameworks about organizational injustices and work strains were examined empirically for their contributing effects towards malicious security behaviors (Dang, 2014; Posey, Bennett, & Roberts, 2011).

The abovementioned theories that were adopted by recent studies suggest a growing interest in the security environment of behavioral security researchers. On one hand, Social Learning Theory (Bandura, 1977) examines learning while emphasizing on factors of the social environment, while Social Bonding Theory (Hirschi, 1969) is related to the sociologist perspective and studies conformity achieved through people’s socialization with the community. With regards to the link between socialization and security behaviors, a number of recent studies (Goo, Yim, & Kim, 2014; Jaafar & Ajis, 2013) re-visit the concepts of information security climate and their impacts on compliance (Chan, Woon, & Kankanhalli, 2005). The focus on the environmental factors is visible in these security climate studies, as the formation of climate perceptions of the workplace’s attributes is driven by the employees socializing with their peers (Ashforth, 1985).

On the other hand, Willison & Warkentin (2013) extended the well-known Security Action Cycle and explained that “pre-kinetic events”, which result from the interaction between the workplace and the employees, take place before the point where top management deters the malicious behaviors. As such, a security workplace being perceived as positive or negative subsequently influences the risk of creating motives for the potential perpetrators’ abusive actions (Willison & Warkentin, 2013). Dang's (2014) recent theoretical proposal of using General Strains Theory (Agnew, 2001) to explain malicious security behaviors by negative emotions and work strains follows such premise. Moreover, Posey et al.'s (2011) empirical research also found evidence supporting that organizational injustices, which lead to abusive behaviors, can result from environmental factors such as uncertain management style and organization’s hierarchical structure.

Finally, there was a recent discussion from the practitioner’s perspective which focuses on the development of “people-centric security workplaces”, where the employee’s proactive security behaviors and personal accountability for organizational security can be fostered (Gartner, 2015). In particular, security managers were suggested to make use of the workplace’s social networks to promote a group culture, which defines appropriate security behaviors and educates the end users about the collateral damages of inappropriate behaviors to their
colleagues (Gartner, 2015). As a result, the emerging theme of studying the security workplace is also evident in the industry in addition to academic interest.

2.2 Proposal of an alternative behavioral security research approach

Since humans operate within bounded rationality, there is a need to explore individual and situational variables that influence such decision-making process (Hu, Xu, Dinev, & Ling, 2011). Adopting new theories or extending current ones to identify contingent variables is thus an effective way to contribute to the body of knowledge. In addition to the aforementioned theories, there are three other theories that also focus on the individualistic cognitive processes of people and have been predominantly adopted by prior research, namely Theory of Planned Behavior, Protection Motivation Theory, and General Deterrence Theory. The main premise of these three theories and the aforementioned ones is that people evaluate factors associating with a behavior and themselves, before they decide whether or not the behavior should be performed. A summary table of the theories and their described individualistic cognitive processes is provided below (table 1).

Table 1: Summary of theories adopted by behavioral security research

<table>
<thead>
<tr>
<th>Theoretical frameworks</th>
<th>Described individualistic cognitive processes</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Learning Theory</td>
<td>Personal confidence in security skills (self-efficacy) can be enhanced by situational supports</td>
<td>Bandura (1977); Warkentin et al. (2011)</td>
</tr>
<tr>
<td>Social Bonding Theory</td>
<td>Personal perceptions of bonds with colleagues motivate security compliance</td>
<td>Hirschi (1969); Ifinedo (2014)</td>
</tr>
<tr>
<td>Organizational Injustice</td>
<td>Personal beliefs about organizational injustices by experiencing uncertainty in management style leads to security misbehaviors</td>
<td>Posey et al. (2011)</td>
</tr>
<tr>
<td>Information Security Climate</td>
<td>Personal perceptions gained from observing the features of security environment (e.g. co-workers and supervisors’ security actions) motivate security compliance</td>
<td>Chan et al. (2005); Goo et al. (2014); Jaafar &amp; Ajis (2013)</td>
</tr>
<tr>
<td>General Strains Theory</td>
<td>Personal work stress and perceived organizational injustices motivate security misbehaviors</td>
<td>Agnew (2001); Dang (2014)</td>
</tr>
<tr>
<td>Theory of Planned Behavior</td>
<td>Individuals receive information and evaluate their own self-efficacy, control over the behavior, and attitude towards the behavior, which motivate them to perform it</td>
<td>Ajzen (2011); see Sommestad, Hallberg, Lundholm, &amp; Bengtsson's (2014) systematic literature review for list of studies adopted this theory</td>
</tr>
<tr>
<td>Protection Motivation Theory</td>
<td>Individuals evaluate a threat and its countermeasure, which motivate their adoption of the countermeasure</td>
<td>Dang-Pham &amp; Pittayachawan (2015); Rogers (1975)</td>
</tr>
<tr>
<td>General Deterrence Theory</td>
<td>Individuals are aware of security policies and punishments, which discourage their intention to commit security misbehaviors</td>
<td>(D’Arcy, Hovav, &amp; Galletta, 2009; D’Arcy &amp; Hovav, 2008; Straub, 1990)</td>
</tr>
</tbody>
</table>
The researchers observed the commonalities in these theories and identified an untouched domain worth exploring. The theoretical assumptions of the three predominantly adopted theories are subsequently examined to further elaborate these issues, especially because their popular adoption could best represent the traditional theoretical stance of the extant studies. To begin, Ajzen (2011) discussed that Theory of Planned Behavior assumes people perform most behaviors without much cognitive effort, and they have different degrees of information processing which vary from shallow to deeper levels. General Deterrence Theory (Straub, 1990, p. 5) explicitly assumes that “potential violators become aware of efforts to control anti-social behaviors.” Another implicit assumption of this theory discussed by D’Arcy and Herath (2011) is that people interpret the same meaning from a punishment, which has been empirically confirmed otherwise (D’Arcy et al., 2009; D’Arcy & Hovav, 2008). Protection Motivation Theory assumes that people appeal to an existing fear and their motivation to perform the recommended behavior is mediated by the threat and coping solution appraisal processes (Rogers, 1975). Prior behavioral security research adopted these three theories have their findings subject to these theoretical assumptions, and this suggested an interesting research opportunity.

In particular, the focus of these theories on people’s individualistic cognitive processes for making security-related decisions has overlooked the interactions and relationships, which provide them the information necessary for their cognition. While the discussed theories could explain the consequences of exposing and having access to security resources, such as receiving situational cues could improve self-efficacy (Social Learning Theory) or socializing with co-workers could develop bonds that motivate compliance (Social Bonding Theory), security managers have not yet been able to maximize the practical values of these findings. Likewise, empirical findings from Theory of Planned Behavior, Protection Motivation Theory, and General Deterrence Theory, confirmed that security compliance can be motivated by factors such as employees’ attitude, perceived efficacy of their own security skills and the prescribed behavior, or misbehaviors can be deterred by perceived sanctions. However, they could not prescribe the specific catalysts that deliver the supports and help the employees to recognize the identified stimuli.

The researchers had in mind several questions related to the employees’ acquisition of security resources and their security behaviors, such as: what happen to the employees who do not have access to the organizational resources to improve their security self-efficacy (Theory of Planned Behavior), or to raise their awareness of the security threats (Protection Motivation Theory) or the punishment for neglecting security duties (General Deterrence Theory)? Or, how can receiving too much or too little access to the resources impact security behaviors?

The variation in the employees’ access to organizational resources due to their social positions in the organizational networks has been a major issue and research topic in management studies (Ibarra & Andrews, 1993). The persistent challenge of the employees ignore security policies and procedures have also been examined by prior research (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Wood, 2000). Poorly designed and burdensome security policies and procedures have been often documented as a primary reason, which explains why the
employees refuse to read the policies (e.g. Boss et al., 2009; Dang-Pham & Pittayachawan, 2015). Furthermore, Kirlappos, Parkin, & Sasse (2014) recently found unsafe security workarounds are invented and diffused by the employees within their work groups.

The spread of these “shadow security” can be explained by Theory of Planned Behavior and similar others as the influence of social norms. Nevertheless, what appear to hold practical values are about identifying the sources that diffuse shadow security and devising strategies to stop such diffusion. The knowledge about the specific diffusing sources/isolated employees and the ways they transfer/acquire security-related information is also necessary for raising the employees’ awareness about the prescribed practices, security threats, and the sanctions for neglecting security duties. These knowledge remains unexplored by the traditional approach which simply examines the general perceptions of social norms, or how much the employees perceive supports and sanctions.

Furthermore, since the aforementioned studies focused on the individualistic attributes such as perceptions and attitudes, they treated individual employees as the main unit of analysis. It appears rather challenging for conceptualizing the security interactions. The discussions insofar warrant the need for a new research approach focusing on the interactions and relationships, which help the end-users to recognize the critical factors of security behaviors already confirmed by prior studies. As such, this approach is developed on top of the theoretical foundation provided by the discussed prominent theories, including their assumptions and methodological considerations. The researchers suggest adopting the social network analysis methods, which can satisfy the raised issues pertaining to the lack of focus on the information security interactions and relationships by treating them as the main unit of analysis. More importantly, this social network analysis approach has neither been recorded in recent systematic literature reviews (e.g. Padayachee, 2012; Sommestad et al., 2014) nor empirically employed in the behavioral security field (Dang-Pham, Pittayachawan, & Bruno, 2014).

3 METHODS
3.1 Social network analysis methods

The term “network” in social network analysis (SNA) is defined as the structures of social interactions and relationships between network actors (Otte & Rousseau, 2002), which may include human and non-human entities (Dang-Pham et al., 2014). As the rest of this paper will elaborate later, the networks examined in this research focus on the common organizational and particularly information security behaviors such as giving work advice, trust, security advice, and security troubleshoot. There are two main components in social network analysis including the network actors (termed nodes) and the networks/interactions/relationship (termed ties) between those actors. While network researchers examine both the nodes and their ties, SNA emphasizes more on the ties and usually treat relational data as the main unit of analysis (Otte & Rousseau, 2002). This methodological concern contradicts the traditional approach (which was also discussed above) and thus allows an in-depth analysis on the social context which is usually overlooked (Otte & Rousseau, 2002). SNA methods have a wide array of analytical capabilities which range from descriptive (e.g. reporting network statistics and visualization) to inferential (e.g. networks correlation and prediction) (Borgatti, Everett, &
The level of analysis can be a complete network (e.g. networks within an organization), an ego network (e.g. personal network of security influence sources surrounding an individual), or simply a node or tie (e.g. node’s centrality or tie’s strength).

Depending on the researcher’s analytical objectives, individualistic attributes of the nodes (e.g. gender, age, attitude, or behaviors) can be used in conjunction with the relational data. For example, researchers can visualize networks with the node’s size proportional to its influential status to assist visual analysis. There have also been innovative combinations of these types of data such as Sykes, Venkatesh, & Gosain (2009), who computed ego network’s density and used it as an independent variable to predict individual’s intention to adopt information systems with other Technology Acceptance Model’s factors. At the moment, more advanced SNA techniques were developed to accommodate the researcher’s need to test empirically network hypotheses. For instance, the uses of exponential random graph modeling (ERGM) and actor-based modeling to examine empirically formation of network ties and longitudinal changes in the node’s behaviors due to social influences have been growing in popularity.

This case study employs both descriptive and inferential analysis techniques. In particular, the analysis and discussion sections will visualize the networks and analyze their descriptive statistics, then statistical tests will be employed to empirically examine the relationships between the networks.

3.2 Network ties

Relational data about the network ties can be collected in different ways which depend on the research design (e.g. whether it is complete or ego network). This case study follows the complete network design since it is more suitable for the research purpose which investigates organizational information security behaviors, especially because the researchers can examine security influence more accurately and in greater details within an environment with specific contextual attributes (e.g. physical locations of staff, management style, or hierarchical level). Moreover, such design will also allow future comparisons between different research contexts.

There is a plethora of interactions and relations within an organization that can be collected and analyzed. Ibarra & Andrews (1993) in their seminal paper discussed that network ties can be categorized as instrumental (e.g. exchange work advice) and expressive (e.g. friendship), and they found different effects of these networks on the employee’s work perceptions. Furthermore, Cross, Johnson-Cramer, & Parise (2009) provided examples of the networks that have been empirically examined, such as task-related communication, workflow, material or monetary resources (instrumental networks), or friendship, personal support, and trust (expressive networks). The networks of exchanging work advice and friendship are considered salient ties in organizational contexts (Saint-Charles & Mongeau, 2009). More specifically, these researchers found that employees tend to rely on their instrumental network to reduce uncertainty in the workplace, whereas friends and trusted colleagues (i.e. expressive networks) are sought more to make sense of the workplace’s ambiguous meanings.

In this analysis, the researchers collected eight networks in total, amongst which there are two pairs of instrumental and expressive networks. The remaining four are behavioral information security networks, which were conceptualized from prior studies. Similar to the organizational
network studies reviewed above, the instrumental networks consist of “give work advice” and “give organizational updates” ties, while the expressive ones consist of “give life advice” and “trust” ties. The rationale of collecting relational data about the instrumental and expressive ties is due to their key roles that have been widely investigated by organizational network research, such as those studies mentioned above. Since behavioral security networks have not been examined before (as evident in the literature review), these instrumental and expressive networks can serve as the baseline for the purposes of comparing and revealing the nature of the security networks. Furthermore, salient relationships and interactions such as trust and exchanging work advice take place in every organization. Therefore, findings derived from this analysis about their potential impacts on security networks (e.g. as predictors) could be generally harnessed to manipulate the security networks.

In regards to the behavioral information security networks, the researchers collected network data about “give security advice” and “give security troubleshoot” ties. Furthermore, relational data about “information security influence” and “technologies influence” networks were also collected. The exchange of security knowledge has been a recent and important topic in the behavioral security field (Kirlappos et al., 2014; Safa & Von Solms, 2016), whereas the provision of security troubleshoot amongst non-IT employees was studied as a form of security delegation (Dourish, Grinter, Delgado de la Flor, & Joseph, 2004). Unlike the exchanges of security advice and troubleshoot which can be recorded and audited, the interpersonal influence (i.e. social norms) is more difficult to observe in the workplace (Dang-Pham et al., 2014), despite its role as a key contributing factor of security behaviors. Therefore, it is worth to collect data about this network and analyze it together with the others. IT consumerization, or the end-users’ adoption of technologies not prescribed by IT management for work purposes, is rapidly taking place in modern organizations and argued to associate with many information security risks (Gens, Levitas, & Sega, 2011). Similar to information security influence, the researchers considered this technologies influence network as an important security-related network to be captured and investigated.

3.3 Research context

This network research took place in XYZ, a large interior contractor in Vietnam, South East Asia. XYZ has been delivering interior design and fit-out projects to many local and international clients. In addition, it also has three factories and a sister company which focus on manufacturing and supplying furniture worldwide. As a result, the major work forces of XYZ include the construction and project management departments, as well as the architect and factory divisions. At the moment, XYZ is implementing their information security management system by following ISO 27001 security standard. Moreover, the researchers’ interview with XYZ’s top management and information security team during the initial meeting suggested that the company is adopting a “command-and-control” security management model, which IT and information security issues are managed and supported by centralized authority.

3.4 Data collection

The researchers conducted a web-based survey in one month and sent the questionnaire to 373 employees in XYZ, who are located in the headquarter as well as other facilities. The
researchers then retrieved back 264 responses, which is equivalent to a response rate of 71 per cent. Table 2 summarizes the survey’s questions which were used to capture the eight mentioned networks. These questions asked the participants to nominate maximum seven colleagues who they will find in the question’s context. The maximum number of nominations is based on the study of Merluzzi & Burt (2013), which suggested that asking seven contacts per actor could reflect more accurately the segmented networks of Asian-Pacific organizations. To assist interpretation, all networks were transposed except “give work advice” and “trust”. For example, “seek organizational updates” network was transposed and became “give organizational updates” network.

Table 2: Network questions

<table>
<thead>
<tr>
<th>Network questions: List out maximum seven colleagues who fit the below descriptions</th>
<th>Networks</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>To whom do you usually give advice (e.g. improve solutions, give referrals or confirmation, point to a policy) about work?</td>
<td>Give work advice</td>
<td>Instrumental networks</td>
</tr>
<tr>
<td>Who do you usually ask for advice (e.g. look for or improve solutions, get referrals or confirmation, cite a policy) about work?</td>
<td>Seek organizational updates</td>
<td></td>
</tr>
<tr>
<td>From whom do you usually get the latest updates or changes (e.g. new policies, process, system) that are happening or coming in XYZ?</td>
<td>Seek organizational updates</td>
<td></td>
</tr>
<tr>
<td>When you want to discuss or ask for advice about personal life issues, whom would you talk to?</td>
<td>Seek life advice</td>
<td>Expressive networks</td>
</tr>
<tr>
<td>Who do you think would be most able (because of education, experience, qualities) to take over your work if you were too busy or absent?</td>
<td>Seek security advice</td>
<td></td>
</tr>
<tr>
<td>Who would explain the importance of information security to you and/or teach you how to perform security behaviors and/or use security technologies?</td>
<td>Seek security advice</td>
<td></td>
</tr>
<tr>
<td>When you encountered a security problem e.g. lost or damaged data, computer virus infection etc., whom would you seek help from?</td>
<td>Seek security troubleshoot</td>
<td>Behavioral security networks</td>
</tr>
<tr>
<td>In general, your decision to perform security behavior, use security technologies and/or exercise security care etc. in daily work would be influenced by whom?</td>
<td>Nominated for security influence</td>
<td></td>
</tr>
<tr>
<td>Who would influence your decision to use technologies &amp; devices (e.g. software, online storage, smartphones, tablets, laptops, portable HDDs etc.) that can improve your work performance or solve work issues but are not prescribed by XYZ / IT department?</td>
<td>Nominated for technologies influence</td>
<td>Technologies influence network</td>
</tr>
</tbody>
</table>

4 Analysis and findings

The analysis commences with performing visual analysis on the eight illustrated networks, followed by examining descriptive statistics at network level including triad statistics. Then, inferential analyses including network correlation and prediction are elaborated. To improve interpretation of the results, the networks that asked the employees to provide nominations (i.e. the “seek” networks) had their matrices transposed. For example, “seek organizational updates” network was transposed to become “give organizational updates”, or “nominated for security influence” network was transposed to become “security influence” network.
4.1 Visual analysis

The network diagrams (termed *sociograms*) illustrated in the analysis contains nodes whose sizes are proportional to their degree centrality measures. Degree centrality is one of the basic network measures used to characterize the node’s direct influential status, which can be calculated by taking the sum of all ties coming in and out of a node (Borgatti et al., 2013). Degree centrality is further classified as in-degree and out-degree centralities, which the former sums only the incoming ties while the latter sums the outgoing ties. This research describes the node’s prominence in a network by calculating their out-degree values (except “trust” network), which bigger nodes send out more ties to the others. For instance, a node having high out-degree in the “security influence” network means that it can influence security behaviors of many other nodes, or having high out-degree in the “give work advice” network means that a node gives work advice to many other nodes. In contrast, a node with high in-degree in the “trust” network means that it is trusted by many others and thus signifies its prominent status. The instrumental networks in figure 1 and 2 describe the flow of work-related information and communication within XYZ. In addition, figures 3 and 4 illustrate the expressive networks comprising give life advice and trust ties.

![Figure 1: Give work advice network](image1)
![Figure 2: Give organizational updates network](image2)

![Figure 3: Give life advice network](image3)
![Figure 4: Trust network](image4)
Researchers performing visual analysis can determine the density of the networks. As seen in figure 1, the “give work advice” network is much denser than the rest. Network’s density can be examined visually by eye-scanning the number of isolated nodes as well as the number of peripheral nodes that have only one connection. For instance, “give organizational updates” network in figure 2 has quite a number of nodes with degree equals to one only, such as those in the at the architect division at the bottom of the sociogram, or those belong to the construction (Cons) department in the top right corner.

Network researchers can evaluate the degree centrality of the nodes and the network’s degree centralization in overall. As mentioned above, degree centrality of each node characterizes its sum of connections and reflects the prominent status of a node. Degree centralization (overall, in- and out-degrees) of a network describes the variation of degree centrality measures amongst all the nodes.

These centrality degrees and network patterns reflect organizational activities within the company, which the core departments and divisions such as construction, PM, architect, and factory, actively engage in exchanging work advice to deliver projects. The intense exchanges of work advice between the employees in these departments and divisions also bring them together and create three major clusters as shown in figure 1. Moreover, these clusters appear to be linked by another cluster in the middle of figure 1, which comprises numerous departments of smaller sizes. While the researchers did not focus on exploring qualitatively the reasons of such clustering, it is consistent to the established work flows in XYZ.

Prior to any fit out projects at XYZ, the business development (BusDev) department is in charge of meeting the clients and presenting to them XYZ’s designs, so that the clients can select or customize for their building. Once a client has selected the design, a project can be initiated and transferred to the PM department. As a result, the business development nodes (i.e. those with dark colors in the center of figure 1) lie in between the PM department and the architect division. Similar to the architect division, the factory division works on their own pace to produce frequently used as well as on-demand furniture for projects, and these tasks require them to liaise with the estimation and accounting departments for sourcing materials and recording manufacturing costs. These are the reasons why the factory nodes are isolated in figure 1, and are linked with the rest via their closest neighbors that include the estimation and accounting nodes. During projects, the PM and construction departments collaborate with each other on a daily basis, which the PM employees often have controls over the projects and send directives to the construction employees working at on-site offices. This is the reason why these two departments are mixed together in figure 1. Moreover, there is the dark yellow after sale services (ASS) department that locates next to the PM and construction departments, and one employee of the ASS department even mixes in the cluster of those two departments. The roles of the ASS department include fixing defects, as well as providing consultancy and services about maintenance. Therefore, they need to liaise with the PM and construction departments but only after the project has been signed off and the client can move in.

The centrality degrees of the nodes also highlight the unique natures of the networks. For instance, the “give organizational updates” network in figure 2 shows that the human resource department’s employees provide advice about organizational updates the most. Similarly, an
employee in the administration department also gives out many updates to their colleagues. Since the roles of the human resource and administration departments are about reviewing policies and distributing them, this phenomenon is quite understandable. More interestingly, while the construction department’s employees give work advice more than those in the PM department (i.e. more nodes with large sizes in figure 1), the PM department’s employees give out more organizational updates. This pattern is consistent with the roles of the departments as discussed previously, which the PM department is responsible for managing projects and updating the policies and changes to employees working in the construction department.

While the instrumental networks (figures 1 and 2) have only a few central nodes, the degree centrality measures are more evenly distributed in the expressive networks (figures 3 and 4). Likewise, the degree centralization of the expressive networks is lower than the instrumental networks. It means that there are more employees who are capable of giving life advice or trusted by their colleagues, than giving work advice or organizational updates. The “trust” network in figure 4 has distinctive clusters of all the departments and divisions. It highlights the fact that employees trust the most colleagues in the same department, since they would have developed solid rapport with these colleagues and known well the colleagues’ capability in handling the tasks. While the readers may be interested in understanding why some departments are more prominent than others in the expressive networks in figures 3 and 4, the researchers believe that such prominence would be better explored by in-depth ethnographic studies that focus on the employees’ personalities and behaviors in the departments. Nevertheless, this is outside of this study’s scope which only aims to examine the structural features of the networks, particularly in relation to information security networks.

Another technique of visual analysis is inspecting how the nodes of the same attributes are clustered together, which looks at the department membership in XYZ’s case. As shown from figures 1 to 4, the architect and factory divisions are separate from the clusters of other departments. In addition, the construction and project management departments also appear consistently mixed in these four sociograms. While the cluster of construction and PM departments can be explained by their closely collaborative nature, the architect and factory divisions are isolated due to their physical locations. The architect division resides in another office building away from XYZ’s headquarter (which hosts the rest of the departments), whereas the factory division is located in the suburb of the city. As a result, the physical proximity could result in more intense exchanges and communications, such as the employees would find it more convenient to seek advice from colleagues who sit next to them.
Figures 5 to 8 illustrate the behavioral security and technologies influence networks. A quick scan of these sociograms shows that employees in the IT and business solutions provider (BSP) departments can influence other colleagues the most. Subsequently, the researchers expect these networks’ degree centralization is also high due to the large variations in the nodes’ centrality measures (i.e. only a few central IT employees while the rest have small centrality values). The highly central IT and BSP employees indicate that XYZ adopts the “command-and-control” model to manage technologies and security, which highlights that all technical queries and issues are transferred to the IT department for handling. Similar to the four sociograms discussed previously (figures 1 to 4), the architect and factory divisions remain isolated from the rest and are linked with one or two IT employees. More interesting, there appear some employees in the architect and factory divisions that also have high degree centrality as compared to the headquarter office, where all the departments are located in the
same location with the IT and BSP departments. The researchers believe that the physical isolation is one of the reasons why those non-technical employees with high centrality emerged, since it may be more convenient to ask for IT or security advice from the local colleagues rather than from the technical employees located in the headquarter building. Finally, the colors of the ties inform that the IT and BSP employees in the technologies influence network (figure 8) have the least influence as compared to figures 5 to 7. Unlike security matters that require specialized knowledge and rigid regulations which only a few IT employees can provide support, topics about technologies are more ubiquitous in the workplace and there are more non-technical employees can become influential.

4.2 Network statistics

To assist visual inspection of the networks, the researchers calculated the network statistics that describe the structural features of the eight networks as shown in table 3. The figures in both bold and italic are the highest values in a network statistic, and those in bold are the second-highest.

In terms of average number of connections possessed by a node, “give work advice” network has the highest value which indicates that employees in XYZ are most active in giving work advice to their colleagues. In contrast, an employee can only influence about two people in terms of their technologies adoption (avg. degree=1.716).

Table 3: Network statistics

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg Degree</td>
<td>5.496</td>
<td>2.375</td>
<td>2.242</td>
<td>2.394</td>
<td>2.568</td>
<td>2.428</td>
<td>2.045</td>
<td>1.716</td>
</tr>
<tr>
<td>Out-Central</td>
<td>0.120</td>
<td>0.147</td>
<td>0.033</td>
<td>0.018</td>
<td><strong>0.528</strong></td>
<td><strong>0.556</strong></td>
<td>0.351</td>
<td>0.261</td>
</tr>
<tr>
<td>Density</td>
<td><strong>0.021</strong></td>
<td>0.009</td>
<td>0.009</td>
<td>0.009</td>
<td>0.010</td>
<td>0.009</td>
<td>0.008</td>
<td>0.007</td>
</tr>
<tr>
<td>Avg Distance</td>
<td>4.308</td>
<td>3.226</td>
<td><strong>5.731</strong></td>
<td>6.469</td>
<td>1.599</td>
<td>1.470</td>
<td>1.650</td>
<td>1.975</td>
</tr>
<tr>
<td>Reciprocity</td>
<td>0.354</td>
<td>0.051</td>
<td><strong>0.247</strong></td>
<td><strong>0.297</strong></td>
<td>0.009</td>
<td>0.006</td>
<td>0.007</td>
<td>0.018</td>
</tr>
<tr>
<td>Transitivity</td>
<td>0.231</td>
<td>0.170</td>
<td>0.172</td>
<td>0.123</td>
<td><strong>0.446</strong></td>
<td><strong>0.458</strong></td>
<td><strong>0.305</strong></td>
<td><strong>0.279</strong></td>
</tr>
</tbody>
</table>

Out-centralization statistics describe the variation in the out-degree values amongst all the nodes in a network. “Give security advice” and “give security troubleshoot” networks have the highest out-centralization, which means that there are some employees who give security advice and troubleshoot to many of their colleagues (e.g. IT and BSP employees) while others may give very little, or not at all, those advices and troubleshoot. These statistics are consistent with the visual inspection above which found a few number of influential IT and BSP employees.
Density characterizes the connectedness of a network since it compares the proportions of actual ties and all possible ties. In this aspect, “give work advice” network is most connected with density statistic equals to 0.021 (2.1 per cent). While interpretation of how much dense is considered connected can vary according to specific contexts, Gesell, Barkin, & Valente (2013) argued that a 0.15 threshold of density statistic reasonably signifies a connected network. As such, the most connected network is still far from the recommended threshold, and this suggests in practicality that XYZ’s daily operations are quite silo-based.

Average distance describes the shortest (geodesic) distance between reachable pairs on average. “Trust” network has the longest distance which takes on average six hops for an employee to trust another colleague. In contrast, the “give security advice” and “give security troubleshoot” networks take only about two hops, which suggest that employees in XYZ can receive immediate security supports. Reciprocity and transitivity statistics also characterize the network flows effectively. The researchers observe that provision of work advice and trust are reciprocated well, whereas security and technical supports or influences travel in one direction only. Moreover, these flows are also more transitive, which the next section will elaborate them in more details.

4.3 Network triads

Network researchers examining triadic configurations are interested in the network’s structural features such as balance and hierarchy (Hanneman & Riddle, 2005). Moreover, triads are formed by triples of actors and considered the simplest structures in a network (Hanneman & Riddle, 2005). The triadic configurations of this case study’s eight networks are displayed in figures 9, 10, and 11. The names of the triadic configurations are displayed under the illustrations. For instance, form “021U” in figure 9 describes the triadic relationships of A→B←C).

Figure 5: Local triadic configurations
While the networks share the amount of disconnected triads (i.e. form “003” in figure 9), the researchers observe several patterns of interest in these figures. For example in figure 9, forms “012” and “102” depict the network flow between two out of three nodes in a triad, which the latter describes reciprocity. It can be seen that “give work advice” network has the highest number of the reciprocated form, followed by “trust” and “give life advice” networks. More interestingly, form “021D” describes dominancy, which “give security advice”, “give security troubleshoot”, and “security influence” networks all possess large amounts of these forms. This is consistent with the previous findings from the visual inspection which display that there are only a few IT and BSP employees giving security advice and troubleshoots to others. Similarly, the network statistics in table 2 also show that there are large out-centralization in those two networks.

![Transitive Triads Diagram](image)

Figure 6: Transitive triadic configurations

Figure 10 consists of the transitive triads which allow resources to flow amongst the triples of nodes. The dominancy and hierarchical structure of “give security advice” and “give security troubleshoot” is visible in the high amount of form “030T”, in which the flows of security advice and troubleshoot travel in one way and there are no returns to the senders. This form is different from “120D”, which can describe a scenario when an IT employee (at the top) gives security advice to two other employees and they also exchange security advice. As seen in figure 10, the reality in XYZ is that a majority of employees receive security advice and troubleshoot only from the IT and BSP employees, thus results in the low amounts of this form in the “give security advice” and “give security troubleshoot” networks. In contrast, form “120U” has higher amounts in these two networks, which describe the situation when two IT employees exchange security advice amongst themselves then both provide the security advice to another employee. Interestingly, the expressive networks have a high amount of form “120D”, which means that two employees receive trust and life advice from each other, as well
as from another common source. This situation is quite understandable since matters such as trust and life advice should be consulted and verified with a bystander. Finally, “give work advice” once again stands out from the rest by its highest amount of complete triads (form 300), which describes high reciprocity in this network.

![Intransitive Triads](image)

Figure 7: Intransitive triadic configurations

Figure 11 consists of triadic configurations that are intransitive and do not allow resources to flow freely amongst the triples of nodes. These configurations do not focus on dominancy but rather highlight the in-between nodes that bridge the network flow. Apart from the “give work advice” network, “trust” network stands out by having a relatively high amount of form “030C”. This form depicts the “bridging” relationship in which A trusts B, B trusts C, then C trusts A. Similarly, the amounts of forms possessed by “give life advice” network are visibly higher than the rest. In contrast, behavioral security networks (i.e. “give security advice” and “give troubleshoot” networks) only have forms “021C” and “111U” which are the different versions of forms “030T” and “120U” in figure 10.

4.4 Inferential network analyses

Having performed descriptive analysis on the eight networks individually, the researchers proceed with examining the relationships amongst them by using statistical tests. As mentioned in the Methods section, the relational data violates the independence assumption of traditional tests and thus demands specialized approaches (Borgatti et al., 2013). One of the basic approaches is the permutation tests family, which allows researchers to test hypotheses related to networks correlation and prediction. For this case study, UCINET software is used (Borgatti, Everett, & Freeman, 2002) to perform QAP (quadratic assignment procedure) correlation and regression tests.
### Table 4: QAP correlation results

<table>
<thead>
<tr>
<th></th>
<th>Instrumental networks</th>
<th>Expressive networks</th>
<th>Behavioral security networks</th>
<th>Tech. Influence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Give Work Advice</td>
<td>Give Org. Updates</td>
<td>Give Life Advice</td>
<td>Give Sec. Advice</td>
</tr>
<tr>
<td>Instrumental networks</td>
<td>1.000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.332</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expressive networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.361</td>
<td>0.304</td>
<td>1.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.383</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behavioral security networks</td>
<td>0.124</td>
<td>0.181</td>
<td>0.141</td>
<td>0.128</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.101</td>
<td>0.152</td>
<td>0.106</td>
<td>0.758</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.000</td>
</tr>
<tr>
<td></td>
<td>0.169</td>
<td>0.236</td>
<td>0.158</td>
<td>0.591</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.593</td>
</tr>
<tr>
<td></td>
<td>0.195</td>
<td>0.225</td>
<td>0.216</td>
<td>0.194</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.456</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.484</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.545</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.000</td>
</tr>
</tbody>
</table>

There are two blocks of QAP correlation results in table 4, which include the groups of highly correlated (i.e. green colors) instrumental/expressive networks (the top four rows) and security/technical networks (the bottom four rows). Moreover, all the correlation results in table 4 achieve statistical significance at lower than 0.005 with number of permutations set to 5,000.

“Give work advice” appears to correlate well with the expressive networks (r > 0.35), whereas “give organizational updates” correlate evenly with all networks, including those about security and technical supports. “Security influence” network correlates highly (r > 0.5) with “technologies influence” and the other two security networks. “Seek security advice” and “seek security troubleshoot” correlates with each other the most (r = 0.758). A positive and statistically significant network correlation result can determine the degree of relatedness between two networks being examined. For instance, “give security advice” and “give security troubleshoot” are highly related to “security influence”, whereas “give work advice” is not very much related. Consequently, the correlation results suggest directions for prediction, since the researchers expect that there would be a higher chance for the existence of “give security advice” or “give security troubleshoot” than “give work advice” to impact “security influence” network ties.

A network of the case study’s research interest is “security influence” network, since interpersonal influences between employees often hold vital implications yet are difficult to manipulate in practicality. For instance, security managers can create incentives to empower employees’ security knowledge and stimulate exchanges of security advice and troubleshoot in the workplace, but it is more challenging to tell whether an individual is more influential in security than another. Using other organizational and security-related networks to predict security influence ties between employees in XYZ’s case allows strategic manipulation of daily activities to create key persons who can influence others’ security behaviors.
Table 5: QAP regression results

<table>
<thead>
<tr>
<th></th>
<th>Un-Std. Coef</th>
<th>Std. Coef</th>
<th>p-value</th>
<th>Std Err</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>Give work advice</td>
<td>0.018</td>
<td>0.030***</td>
<td>0.000</td>
<td>0.002</td>
</tr>
<tr>
<td>Give organizational updates</td>
<td>0.072</td>
<td>0.077***</td>
<td>0.000</td>
<td>0.003</td>
</tr>
<tr>
<td>Give life advice</td>
<td>-0.003</td>
<td>-0.004</td>
<td>0.118</td>
<td>0.003</td>
</tr>
<tr>
<td>Trust</td>
<td>0.008</td>
<td>0.009***</td>
<td>0.007</td>
<td>0.003</td>
</tr>
<tr>
<td>Give security advice</td>
<td>0.231</td>
<td>0.258***</td>
<td>0.000</td>
<td>0.004</td>
</tr>
<tr>
<td>Give troubleshoot</td>
<td>0.225</td>
<td>0.245***</td>
<td>0.000</td>
<td>0.004</td>
</tr>
<tr>
<td>Technologies influence</td>
<td>0.310</td>
<td>0.285***</td>
<td>0.000</td>
<td>0.004</td>
</tr>
</tbody>
</table>

QAP regression test was employed (number of permutations = 3,000) to predict “security influence” network by the other seven networks. As shown in table 4, all networks except “seek life advice” were found to influence positively “security influence” network. The prediction model actually explains 47.68 per cent of “security influence” network’s variance. Amongst the positive effects, “technologies influence” network impacts “security influence” the most with beta value equals to 0.285. In second rank are “seek security advice” and “seek security troubleshoot” networks, which yielded beta values of 0.258 and 0.245 respectively. These findings can be interpreted that employees who are sought for security advice and troubleshoot have a better chance of being nominated as influential in security as well. Similarly, employees who influence others’ technologies adoption can also influence their security behaviors. Unlike the security-related and technical networks, the contributing effects of the instrumental and expressive networks are minimal despite their statistical significance. As a result, they hold little managerial implications in practicality.

5 DISCUSSION AND CONCLUSION

The case study has employed descriptive and inferential social network analysis techniques to investigate eight organizational networks in a large interior contractor in South-east Asia. From a practical perspective, the network research approach has several implications for information security management. For instance, security managers can perform visual inspection to monitor the effects of the “command-and-control” security management model, such as by observing employees in IT and BSP departments take centralized controls over security and technical supports or influences. Security managers may employ SNA methods to evaluate the implementation of their strategic security model. It is also displayed that even though security supports are centralized in IT and BSP departments, there are still influential and supportive employees in non-technical departments such as architect and factory divisions. Security managers can either make use of these employees to diffuse security awareness or monitor their social influences which may have the risk of propagating false information. Using SNA methods to identify these key players is feasible and more objective than other methods that are based on expert judgements.

Even though this case study focuses on a particular work setting, the differences between behavioral security and other organizational networks are shown quite clearly. Reciprocity is
one important statistics which not only illustrates such difference but also hold practical implications. In XYZ’s case, the reciprocity’s rates in the behavioral security networks are low in general and indicate that the flows of security advice or troubleshooting are generally one-way. Furthermore, the average shortest distance measures whether the employees can receive immediate security supports or not. By examining these statistics, security managers may choose to foster reciprocity in security supports or reduce the average shortest distance. The researchers also observed that behavioral security networks are transitive since they possess high amount of transitive triad forms that focus on dominancy and hierarchy. These features add more information to describe the nature of the “command-and-control” model.

The QAP statistical tests analyze the relationships amongst the networks and suggest ways to increase the predicted network ties of interest. For instance, the results indicated that an employee can increase his or her security influential status by giving out security and technologies-related advice and troubleshoot. Moreover, those actively engage in exchanging work advice, organizational updates, and being trusted by colleagues can also increase their security influence. Since the low effects of these networks in this case study may reflect the nature of the “command-and-control” model, security managers aiming to decentralize security authority and develop people-centric security workplaces can rely on these findings to build communities of security practices. Some activities to improve diffusion of security awareness by making use of organizational networks can include job rotation, participation in cross-functional projects, or mentoring system.

There are also theoretical implications from this case study. Given that there are many more organizational and security-related networks that the researchers have not examined, and that the case study focuses only on one work setting, future research can extend this study to other contexts. Furthermore, the researchers anticipate that different findings may be found when replicating this network research approach in other contexts. Specifically, the empirical findings from this case study revealed that information security-related networks are influenced by other organizational interactions such as exchanging work advice and trust relationship. Since these organizational interactions can be affected by the cultural values that vary according to the regions and workplaces, the information security-related networks may also be unique.

The case study discussed in this project is situated in an interior contractor in Vietnam, South East Asia, which shares certain Asian cultural values. One of the prevalent cultural values in Vietnam is high collectivism, which emphasizes on the strong relationship between group members and the high concern about losing “face” (Hofstede, 2001). Furthermore, the power distance in Vietnam is extremely high, which implies that people would accept hierarchy without much justification (Hofstede, 2001). Even though this research neither collected data about the employees’ cultural values nor aims to examine the relationship between cultures and networks’ features, these inherent Vietnamese cultural traits may provide a reason why the networks took the illustrated shapes. For example, the high collectivism and reliance on groups could have resulted in the silo-based structure, in addition to the work proximity between the employees, which had fewer security advice and troubleshoot exchanged across departments. In addition to the “command-and-control” security management model being adopted by XYZ,
the great power distance may discourage informal exchanges of security advice and troubleshoot amongst XYZ’s employees, and encourage them to seek official supports from the IT authority instead. This could explain why the IT employees hold prominent positions in the security networks.

The researchers anticipate that the security networks in another context may have different density, transitivity, and reciprocity rates. Such security networks should also correlate more with other networks, due to the unique contextual factors such as the cultural traits mentioned above. To assist future research, the theoretical concepts and social network analysis methods have been elaborated throughout this study. To the researchers’ best knowledge, this case study is the first to investigate security behaviors empirically with social network analysis techniques. The researchers look forward to seeing more interesting network studies in behavioral security field, perhaps a new network theory that explains further security behaviors.

REFERENCES


