Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

# Impacts of security climate on employees' sharing of security advice and troubleshooting: Empirical networks

**Duy Dang-Pham** *, **Siddhi Pittayachawan**, **Vince Bruno**

*School of Business IT & Logistics, RMIT University, 124 La Trobe Street, Melbourne, Victoria 3000, Australia*

**KEYWORDS**
Security behavior;
Security management;
Security climate;
Social network analysis;
Exponential random graph modeling (ERGM)

**Abstract** While extant research has studied the motivations of individualistic security compliance, this study explains what motivates employees to share security advice and troubleshoot with others. We argue that such findings are crucial for the development of people-centric security workplaces, where desirable security behaviors are disseminated amongst the employees. In this research, we applied network analysis techniques to perform two tasks. First, we explored the structural patterns of employees' sharing of security advice and troubleshooting. Second, we evaluated the effects of security climate perceptions, perceived accountability, and personal attributes on those sharing activities. While the sharing network was found to be thin and sparse, perceptions of a direct supervisor's security practices and accountability for security tasks can increase sharing. Age, seniority, and tenure—as well as having the same gender and department membership—can also motivate sharing. In contrast, security climate perceptions of coworkers and top management's security practices were found to discourage sharing. Our practical recommendations focus on the strategies to maximize security engagement in the workplace. Potential ideas for future research are also discussed in detail. Most importantly, we hope to offer this research as the foundation for future network studies in the behavioral security field.


## 1. Introduction

In recent years, security researchers and practitioners have been focusing on the concept of the people-centric security workplace, where voluntary and conscious security behaviors can be fostered and encouraged (Dang-Pham, Pittayachawan, & Bruno, 2015; Gartner, 2015). People-centric workplaces

* Corresponding author
*E-mail addresses:* duy.dang@rmit.edu.au (D. Dang-Pham), siddhi.pittayachawan@rmit.edu.au (S. Pittayachawan), vince.bruno@rmit.edu.au (V. Bruno)

0007-6813/$ — see front matter 
http://dx.doi.org/10.1016/j.bushor.2016.07.003

emphasize developing personal accountability for security, as well as a security culture which promotes employees assisting each other in performing security duties (Gartner, 2015). The theme of this people-centric workplace matches with discussions in recent researches regarding the interactions between employees and their security behaviors. For instance, Kirlappos, Parkin, and Sasse (2014) discovered the concept of shadow security: the security workarounds that are unknown to top management and disseminated within departments. Based on the premise that security behaviors are collective information practices (Dourish & Anderson, 2006), Dang-Pham, Pittayachawan, and Bruno (2014) proposed that behavioral security researches may employ social network analysis techniques to study in depth the relationships between security interactions and security-related factors.

The emerging research theme, which focuses on security workplace and interactions, highlights the importance of studying the security environment and its features. This motivated us to study security climate and its impacts on security behaviors. Security climate is considered an important construct in the behavioral security field, which holds knowledge about socio-organizational factors (Chan, Woon, & Kankanhalli, 2005; Goo, Yim, & Kim, 2014; Jaafar & Ajis, 2013). Furthermore, security climate and the socio-organizational factors have been overlooked by researches adopting the instrumental perspective to explain the mechanisms of security behaviors (Dang-Pham et al., 2015; Goo et al., 2014). This study aligns with the discussed research theme and employs network analysis techniques to examine the relationship between security climate and security engagement. Network researchers can examine the structural patterns of networks through visualization and study the network effects by conducting specialized statistical tests (Borgatti, Everett, & Johnson, 2013). This study aims to answer the following research questions:

**RQ1:** What are the impacts of the security environment
(i.e., security climate) on employees' security engagement
(i.e., sharing security advice and troubleshooting)?

**RQ2:** What are the structural patterns of the security engagement network?

## 2. Literature review

We review the relevant literature in the following subsections. First, we define security engagement in our study, which refers to employees' sharing of security advice and troubleshooting in the workplace. Second, we present our hypotheses, which are based on the concepts of security climate perceptions and accountability theory, as well as prior studies about personal attributes such as gender and department membership on network engagement.

### 2.1. Security engagement

Security engagement is defined in this research as including the sharing of security advice and security troubleshooting, which both are security interactions (Dang-Pham et al., 2014) and reflect the collective characteristics of security behaviors (Dourish & Anderson, 2006). Security troubleshooting can be delivered via security delegations between individuals, such as seeking out employees with technical knowledge to assist in setting up the others' computers (Dourish, Grinter, Delgado de la Flor, & Joseph, 2004). These forms of security engagement also conform with the previous findings of Kirlappos et al. (2014) about shadow security groups, where advice about security workarounds is communicated within the departments via informal induction by direct supervisors or via peers. Warkentin, Johnston, and Shropshire (2011) adapted social learning theory and found that situational support and verbal persuasion can improve employees' self-efficacy, which subsequently motivates their intention to perform security behaviors. Their findings suggest the importance of informal security advice and justify the inclusion of security advice sharing activity in this research. We argue that it is crucial to find the motivations that result in employees' active engagement in sharing security advice and troubleshooting. In the next sections we review the relevant constructs and hypothesize their impacts on security engagement.

### 2.2. Security climate

The construct of security climate arguably made its first appearance in Chan et al.'s (2005) research, which refers to employees' observation of the security practices performed by their coworkers, supervisors, and top-level managers. These dimensions of security climate have been subsequently refined and validated by later studies (Dang-Pham et al., 2015; Goo et al., 2014; Jaafar & Ajis, 2013). Security climate originates from safety climate (Chan et al., 2005), and it belongs to the larger family of different types of organizational climate (Dang-Pham et al., 2015). Organizational climate has been regarded as an important construct in the management research field since it was found to result in

various desirable strategic outcomes (e.g., improve customer service level and innovativeness, motivate safety performance) (Kuenzi & Schminke, 2009). Despite the implications of studying organizational climates, the construct is inherently fuzzy and ambiguous by itself (Guion, 1973) and thus requires the researchers to clarify the type of climate being studied (Schneider & Reichers, 1983). By doing so, climate researchers can enhance the practical utility of their findings by focusing on a strategic facet of the organization (Schneider & Reichers, 1983). Security climate in this case characterizes the observable security environment, which promotes the priority of security and encourages compliance as one of top management's strategic objectives (Dang-Pham et al., 2015).

Security engagement, which consists of security advice and troubleshoot-sharing activities, is a part of the evolving security climate. In fact, security engagement encapsulates the interaction between employees and their direct supervisors, as described in the dimensions of security climate mentioned above. Security engagement develops and maintains security climate via informational influences, as explained with the interactionist perspective (Ashforth, 1985; Schneider & Reichers, 1983). In particular, activities such as sharing security advice and troubleshooting each other's security issues allow employees to make sense of their security environment by reducing uncertainty (Ashforth, 1985; Dang-Pham et al., 2015). Since positive security climate can result in positive security behaviors, we argue that employees will feel motivated to share security advice and troubleshoot as they perceive the surrounding security climate more clearly. There are also various explanations for why perceptions of security climate can lead to more security engagement. First, security climate can establish norms and social contracts regarding the sharing activities and demand that employees continue reciprocating such interactions (Liu, Keller, & Shih, 2011; Tohidinia & Mosakhani, 2010). Second, the contributing effect of leader-member exchange on employees' knowledge-sharing has been confirmed by prior studies (Carmeli, Atwater, & Levi, 2011). As a result, we hypothesize:

**H1:** Security climate perception of direct supervisors' security practices leads to security engagement.

**H2:** Security climate perception of coworkers' security practices leads to security engagement.

**H3:** Security climate perception of top management's security practices leads to security engagement.

## 2.3. Perceived accountability

In addition to the social influences caused by security climate that pressure reciprocity of security engagement, we employed accountability theory (Frink & Klimoski, 1998) to explain the motivation of voluntary security activities. Accountability theory has been applied widely in the management field to understand the driving force of extra role or organizational citizenship behaviors (Hall & Ferris, 2011; Nielsen, Hrivnak, & Shaw, 2009). Accountability theory has been recently applied in behavioral security context by Vance, Lowry, and Egget (2015), who found perceived accountability significantly reduced employees' intention to violate security policies. However, accountability theory has not been applied to predict desirable security behaviors. Hall and Ferris (2011) explain that employees who are sensitive to accountability perform extra role behaviors to increase their likability in the workplace. Likewise, we believe that employees perceiving high accountability for security tasks will actively share security advice and troubleshoot to receive positive evaluations from the others. Furthermore, the positive security climate, which promotes the priority of security via the practices of coworkers and direct supervisors, reinforces the positive impression of active security engagement. As a consequence, it is reasonable to hypothesize:

**H4:** Perceived accountability leads to security engagement.

## 2.4. Personal attributes

Besides the impact of the cognitive factors and processes on actual behaviors, individuals may engage in certain activities due to their personal attributes—such as age and gender. For example, Borgatti et al. (2013) discussed the well-supported homophily effect (e.g., people of the same gender tend to participate in common activities). Ibarra and Andrews (1993) explained that physical proximity and affiliation can also influence behaviors; employees working in the same department may find it more convenient to assist each other's work or ask for information. In fact, there is empirical evidence supporting the positive effect of physical proximity on information-seeking behaviors (Borgatti & Cross, 2003). Seniority and tenure can also affect information-sharing behaviors, especially when

employees in a senior position with a longer service record possess legitimate power and know more about the work (Borgatti & Cross, 2003; Wenger, 1998). Following these premises, we hypothesize:

**H5:** Employees tend to share security advice and troubleshoot with those of the same gender.

**H6:** Employees tend to share security advice and troubleshoot with those in the same department.

**H7:** Older employees are more likely to share security advice and troubleshoot.

**H8:** Employees holding senior positions are more likely to share security advice and troubleshoot.

**H9:** Employees having longer tenure are more likely to share security advice and troubleshoot.

## 3. Methods

In this section, we elaborate on our research design and strategy. Specifically, we provide a description of the research context, an overview of network analysis techniques, and details about our measures and data collection process.

### 3.1. Research context

To understand the formation of security climate and security engagement, we conducted our research in a large interior contractor in Vietnam, Southeast Asia. This organization, named ABC to safeguard its identity, has more than 300 employees and 1000 skilled workers, and has been delivering design and construction projects to both local and international clients since 1992. ABC has two offices located in the two most urban cities in Vietnam, as well as three factories where it manufactures chairs and other furniture being shipped worldwide. At the moment, ABC is opening a new office in Myanmar to expand the business. ABC is in the process of implementing its information security management system by following the ISO 27001 security standards.

### 3.2. Social network analysis and exponential random graph modeling

As this research focuses on security engagement, which is characterized by employees' sharing of security advice and troubleshooting, social network analysis (SNA) techniques provide the analytical capabilities to effectively investigate such interactions. SNA distinguishes itself from the traditional approaches by setting emphasis on the interactions and relations as the unit of analysis (termed 'edges' or 'ties'), rather than individualistic attributes such as perceptions or attitudes (Otte & Rousseau, 2002). Researches applying SNA can study more in depth the socio-organizational factors that have been mostly overlooked by other approaches (Otte & Rousseau, 2002), and thus is suitable for examining security climate. SNA techniques also allow both descriptive and inferential analyses, in which the prior case involves visualizing the complex networks and highlighting the influential actors or *nodes* (Borgatti et al., 2013; Dang-Pham et al., 2014). In this study we perform visual analysis to answer RQ2, which aims at examining the network patterns of security engagement.

More importantly, SNA methods provide statistical tests that accommodate the special nature of relational data, which violate the independence assumption of traditional tests and thus prevents their adoption (Borgatti et al., 2013). Amongst them, we employ exponential random graph modeling (ERGM) to test the proposed hypotheses about various motivations of security engagement. ERGM constructs statistical models which consist of terms that describe the features of an observed network (Robins, Pattison, Kalish, & Lusher, 2007). The role of the researchers is to add relevant terms that reflect the hypothesized causes which explain why the observed network is formed in such way. For instance, a potential term can explain that a network tie between two nodes is established due to one node having higher seniority value than the other (Morris, Handcock, & Hunter, 2008). In our case, our hypothesis H8—about the occurrence of security engagement activities between two employees due to the difference in seniority—can be empirically tested through ERGM.

Once the necessary terms are added, the model is estimated using the Monte Carlo Markov Chain (MCMC) estimation method. Network researchers can then accept the model and interpret its estimated results if the networks being randomly simulated from that model resemble the initial observed network; in other words, the model is proven to fit the data and converge well in such a case. In this research, we develop and estimate the ERGM by using the statistical package statnet in R (Handcock, Hunter, Butts, Goodreau, & Morris, 2008). A list of the model's terms can be found in our results table (Table 1), and a full reference of all

**Table 1. Descriptive statistics of security engagement network**

| Statistics | Meanings | Values |
|---|---|---|
| Average Degree | The average number of degree (nominations) of all the nodes | 3.098 |
| Degree Centralization | The higher the value, the larger the gap between the lowest and the highest numbers of degrees | 0.038 |
| Out-degree Centralization | Has similar meaning to degree centralization, except that this value focuses on out-degree (i.e., seek security advice and troubleshoot from someone else) | 0.038 |
| In-degree Centralization | Has similar meaning to degree centralization, except that this value focuses on in-degree (i.e., send security advice and troubleshoot to someone else) | 0.61 |
| Density | Number of existing ties divided by maximum number possible | 0.012 |
| Average Distance | Average geodesic (shortest) distance amongst reachable pairs of nodes | 1.67 |

available terms is documented in the article by Morris et al. (2008).

### 3.3. Measures and data collection

To capture a security engagement network, we asked the participants to nominate a maximum number of seven of their colleagues in ABC who give them security advice (e.g., how to perform a prescribed security procedure or use a security technology), and another seven colleagues who provide them security troubleshooting help in daily work. The limit of seven nominations conforms to Merluzzi and Burt's (2013) suggestion, which recommends that capturing five to six names per node is necessary for detecting clear effects from the commonly thin and sparse networks in Asian organizations. The separate 'seek security advice' and 'seek security troubleshoot' network were combined to create the composite 'security engagement' network.

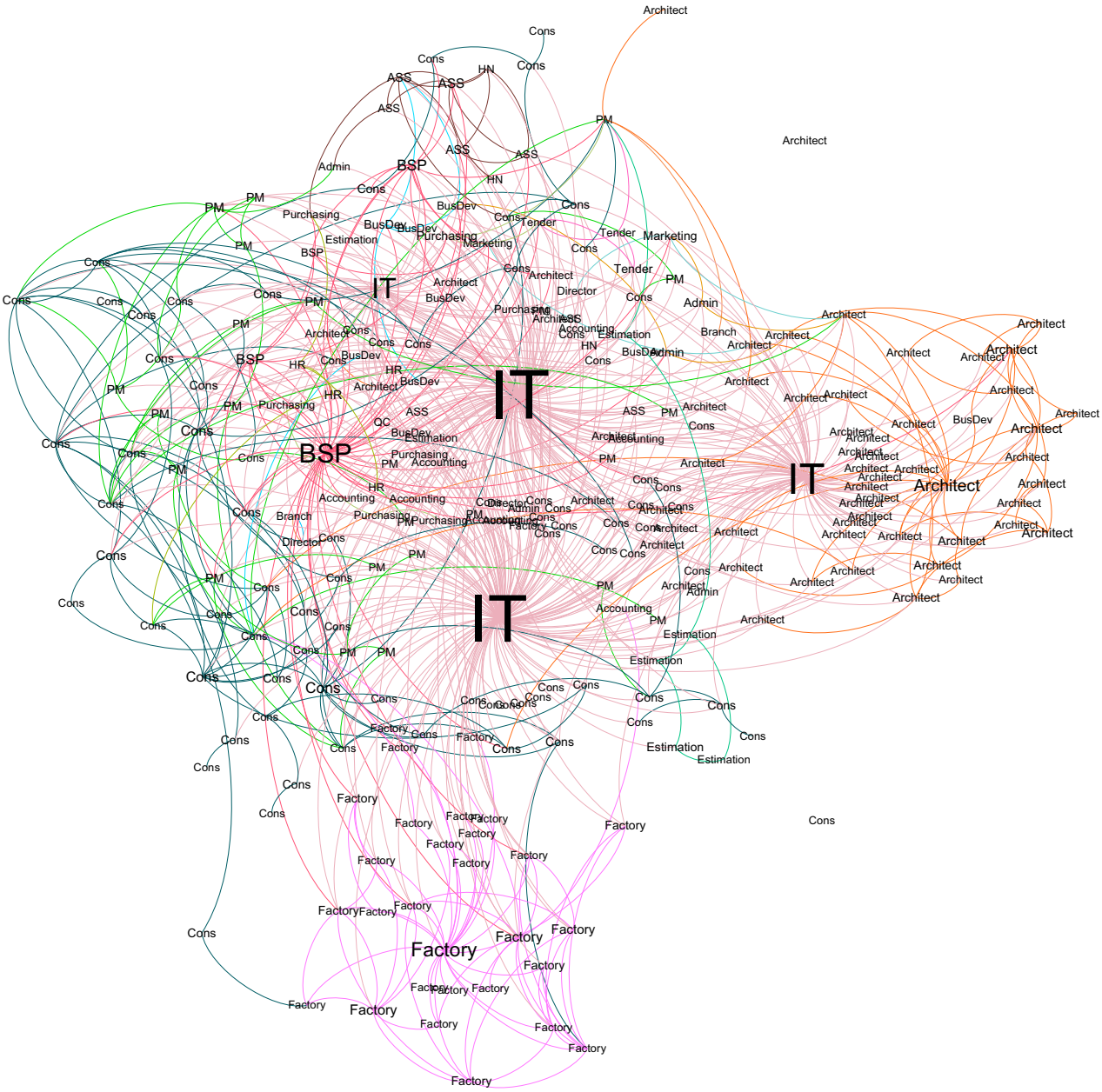
Four sets of questions were also included in the questionnaire to capture latent constructs, such as security climate perceptions and perceived accountability. For the security climate perceptions of direct supervisor and coworker practices, we used pre-validated questions from security climate studies (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013). In contrast, items for measuring security climate perception of top management security practices included both questions adapted from the mentioned studies and self-developed ones. These questions were co-written with ABC's staff to relate accurately to the security measures being implemented in the organization. For perceived accountability construct, we adapted the questions from Nielsen et al.'s (2009) research. Each latent construct was measured by two sets of items of different scales to reduce common method biases (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Personal attributes, including gender, age, department membership, seniority, and tenure, were extracted from ABC's human resource database. The web-based survey was sent to 373 office workers in ABC in one month and we received back 264 usable responses (i.e., response rate was 71%).

### 3.4. Descriptive analysis

By visualizing the network diagram (Figure 1), we can quickly examine the structural patterns of the network, as well as identify the influential employees who actively share security advice and troubleshoot with others. The influential status is proportional to the size of the nodes, the larger size of which indicates receiving more nominations from peers. The colors of the ties (or edges) are based on the target nodes. For instance, the bright-green tie between the construction (Cons) and project management (PM) staff on the top left of the diagram means that the Cons employee nominated the PM employee for giving him/her security advice and troubleshooting help.

It can be seen that there are four IT staff who dominate security engagement in the network. The Business Solutions Provider's (BSP) vice director also appears to share security advice and troubleshoot with project management and construction departments. More important, there are emerging influential non-IT staff that are active in sharing security advice and troubleshooting. Some of these notable staff reside in the factory and architect divisions, as well as the after sales services (ASS) department on the top part of the diagram. While security engagement occurs between construction and project management staff, the divisions of factory and architect have their distinctive colors (pink and orange) and appear isolated from the rest. One primary factor accounting for this observation can be due to the fact that the construction and project management departments are located in ABC's headquarters, whereas the architects and factory staff have their own separate offices. This hints to the effect of physical proximity on security engagement.

**Figure 1. Security engagement network (i.e., seek security advice and security troubleshoot) in ABC (n=264)**




We computed descriptive statistics (Table 1) to further analyze the network structural patterns and answer RQ2. Overall, the network is thin and sparse (density = 0.012). Different networks recommend varied thresholds of desirable density. Despite this, values that are lower than 0.15 can be considered as too unconnected (Gesell, Barkin, & Valente, 2013). The employees in this network nominated on average three other colleagues who can give them security advice and troubleshooting help (Average Degree = 3.098). Most of them enjoy immediate support (average distance = 1.67) rather than requiring the supporter nodes to jump multiple hops to reach them. The centralization statistics suggest there are dominant nodes in the network that receive significantly more nominations than the average. This is consistent with the visual analysis above, which identifies the IT and BSP staff as the dominant ones. In contrast, the out-degree centralization is low (0.038) and suggests the high similarity in the number of nominations each node has submitted to the survey.

## 4. ERGM analysis

The analyses in this section aim to answer RQ1 by testing the hypotheses proposed in our literature

review. First, factor analysis is performed to validate and generate the factor scores of the latent constructs, which are included in the subsequent ERGM process. We then proceed to evaluate the quality of our model and conclude this section by interpreting the model's findings.

### 4.1. Factor analysis

Exploratory and confirmatory factor analyses were employed to analyze the structure of latent constructs, such as security climate perceptions and perceived accountability. Exploratory factor analysis (EFA) provides an early detection of the common patterns amongst the items, which group them together as latent constructs (Brown, 2006). To remain consistent with the confirmatory factor analysis, the maximum likelihood extraction method was employed. We also used direct oblimin rotation method to extract more accurately the constructs and their related items (Brown, 2006). We used IBM SPSS statistical software package (version 21) to perform EFA. The EFA results and details of the items are shown in Table 2. The value of KMO measures equal to 0.884 and Barlett's test achieves statistical significance at 0.000, indicating that factorability is acceptable (Hair, Black, Babin, & Anderson, 2010). Items that are displayed in Table 2 must have loading exceeding the recommended threshold of 0.35, otherwise it will be removed (Lewis, Templeton, & Byrd, 2005).

Confirmatory factor analysis (CFA) was performed to evaluate the theoretical structures of the latent constructs as suggested by EFA's results. As shown in Table 3, the measurement model of each construct was fitted to achieve the desired convergent validity indices. It can also be seen that several items were removed when we fitted the measurement models. The fitting process and computation of the factor scores (by using Bayesian imputation) were performed using IBM AMOS software.

### 4.2. Exponential random graph model estimation and evaluation

We specified the initial model based on the nine hypotheses. To increase the robustness of the model, we incorporated three additional terms to capture the numbers of isolated nodes (i.e., those neither seek nor share security advice and troubleshoot), "sinks" (i.e., those only seek security advice and troubleshoot), and "sources" (i.e., those only share security advice and troubleshoot) (Robins, Pattison, & Wang, 2009). Furthermore, adding these terms enables the MCMC estimation process, which sample size and interval was set at 20,000 and 2,000 respectively. The second model with the additional terms converged at the fifth iteration out of 20 (whereas the previous one converged at the ninth iteration), and helps reduce Akaike Information Criterion (AIC) (from 6,867 to 6,806) and Bayesian Information Criterion (BIC) (from 6,959 to 6,925). Goodness-of-fit of this model is visualized in Figure 2 and can be evaluated by examining whether the black line (represents the observed network) falls into the area between the two grey lines (represents the 95% bounds of the distributions). The model captures the distributions of in- and out-degrees in the network relatively well, but not edge-wise shared partners and minimum geodesic distance. However, these limitations do not hold important implications since the number of edge-wise shared partners and minimum geodesic distance as higher-order aspects of the network are not our focus (Kim, Holman, & Goodreau, 2015; Lusher, Koskinen, & Robins, 2012).

### 4.3. Findings

The ERGM estimated coefficients are summarized in Table 4 below. The coefficients are reported in log-odds and can be converted to probability values. The corresponding probability for a security engagement tie to occur between two random employees, with a given log-odd of -3.426, is 3.15%. As the other effects with positive signs are added, the log-odd and its probability value can be increased. For example, the occurrence of security engagement between employees who work in the same department receives an increased log-odd of 1.31, which results in a probability of 10.76% (log-odd = -2.116).

The negative and significant log-odd of the term 'edges' (-3.426) indicates that the likelihood for security engagement to occur in the workplace is low. In other words, it is rare for any random pair of employees to share security advice or troubleshoot with each other.

Employees who perceive direct supervisors' security practices tend more to share security advice and troubleshoot (log-odd = 0.181). In contrast, the more they perceive the security practices performed by coworkers and top management, the less likely they want to share security advice and troubleshoot (log-odds = -0.590 and -0.694 respectively). Hypothesis H1 was thus supported, whereas H2 and H3 were not—despite the significant results.

H2 and H3's negative results have interesting interpretations. Instead of actively sharing security advice and troubleshooting when perceiving coworkers doing so, these employees with high security climate perceptions chose to stop sharing.

**Table 2. Exploratory factor analysis results**

| Items | Scales | Questions | Loadings | Sources |
|---|---|---|---|---|
| SUP1_1 | Not at all Very much 0 to 6 (7) | How frequently does he/she talk about ISS throughout the work week? | -0.935 | (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013) |
| SUP1_2 | | To what extent does he/she insist that employees need to ensure ISS in daily work? | -0.903 | |
| SUP1_3 | | How frequently does he/she tell employees about the ISS threats in daily work? | -0.867 | |
| SUP1_4 | | To what extent is he/she strict about ISS in daily work? | -0.795 | |
| SUP2_5 | Strongly disagree Strongly agree -3 to 3 (6) | He/she uses explanations to get us to perform security behavior | 0.907 | |
| SUP2_4 | | He/she discusses how to improve ISS with us | 0.901 | |
| SUP2_2 | | He/she spends time helping us learn to see ISS problems before they arise | 0.844 | |
| SUP2_6 | | He/she updates us on changes of ISS procedures | 0.797 | |
| SUP2_1 | | He/she says a good word to employees who pay special attention to ISS | 0.768 | |
| SUP2_3 | | He/she makes sure we follow all ISS procedures (not just the important ones) | 0.758 | |
| COL1_5 | Not at all Very much 0 to 6 (7) | To what extent do they care about or ensure ISS when not being supervised/monitored? | 0.907 | |
| COL1_1 | | To what extent are they committed to ensuring ISS? | 0.905 | |
| COL1_2 | | How seriously do they take ISS? | 0.899 | |
| COL1_4 | | To what extent do they care about or ensure ISS when rushing deadlines? | 0.729 | |
| CLI1_5 | Not at all Very much 0 to 6 (7) | How strictly does ABC enforce the written ISS rules and policies? | 0.840 | Self-developed (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013) |
| CLI1_2 | | To what extent does ABC encourage (if not enforce) managers to improve ISS in their departments? | 0.737 | |
| CLI1_3 | | To what extent does ABC implement physical protection (e.g., lockers, CCTVs, security guards etc.)? | 0.711 | |
| CLI1_1 | | To what extent does ABC encourage (if not enforce) employees to participate in ISS training? | 0.701 | |
| CLI1_4 | | To what extent does ABC implement technological protection (e.g., allocation of access rights, anti-virus software, spam filter, backup & archival system, etc.)? | 0.626 | |
| CLI1_6 | | To what extent are entries and visits from the outside (e.g., cleaners, non-ABC staff, customers, interviewees, etc.) monitored in your office? | 0.621 | |
| CLI2_6 | Strongly disagree Strongly agree -3 to 3 (6) | Posters, newsletters, emails, etc. about ISS awareness are frequently updated and communicated | 0.928 | |
| CLI2_5 | | ABC implements a variety of communications (posters, notices, newsletters, emails, etc.) | 0.862 | |
| CLI2_2 | | ABC provides specific training about the security behavior and technologies required in daily work | 0.729 | |
| CLI2_8 | | Audits are conducted periodically to check for compliance and ISS risks | 0.717 | |
| CLI2_1 | | ABC provides us sufficient training to improve our ISS awareness | 0.713 | |

**Table 2** (*Continued*)

| Items | Scales | Questions | Loadings | Sources |
|---|---|---|---|---|
| CLI2_4 | | ISS formal supports are timely and helpful in general | 0.675 | |
| CLI2_10 | | ISS policies are readily available for our reference | 0.656 | |
| CLI2_7 | | ABC implements continuous monitoring mechanisms to monitor and review ISS efforts and risks | 0.619 | |
| CLI2_12 | | ABC ensures managers are able to ensure ISS in their departments | 0.584 | |
| ACC1_2 | Not at all Very much 0 to 6 (7) | In the grand scheme of things, how important are your ISS efforts at work? | 0.885 | (Hall & Ferris, 2011; Nielsen et al., 2009) |
| ACC1_3 | | To what extent the protection of ABC's confidential and important information assets depends on your ISS behavior? | 0.863 | |
| ACC1_1 | | How accountable you are held for your ISS behavior? | 0.637 | |
| ACC2_2 | Strongly disagree Strongly agree -3 to 3 (6) | If ISS issues occur or don't go the way they should, I will hear about it from top management | 0.770 | |
| ACC2_1 | | Top management holds me accountable for all of my ISS behavior | 0.686 | |
| ACC2_4 | | Coworkers, subordinates, and bosses closely scrutinize my ISS efforts at work | 0.526 | |
| ACC2_3 | | The protection of my department's confidential and important assets depends on my ISS behavior | 0.509 | |

One possible explanation is that because these employees found the security climate in their department is positive (i.e., security is prioritized and coworkers are aware of the priority), they perceived that any more sharing would be redundant and chose to discontinue sharing.

Hypothesis H4 was supported with a positive and significant estimated coefficient (log-odd = 2.869). In fact, perceived accountability has the highest coefficient amongst the others. This result indicates that employees who perceive high personal accountability for security tasks are more likely to share security advice and troubleshoot with others.

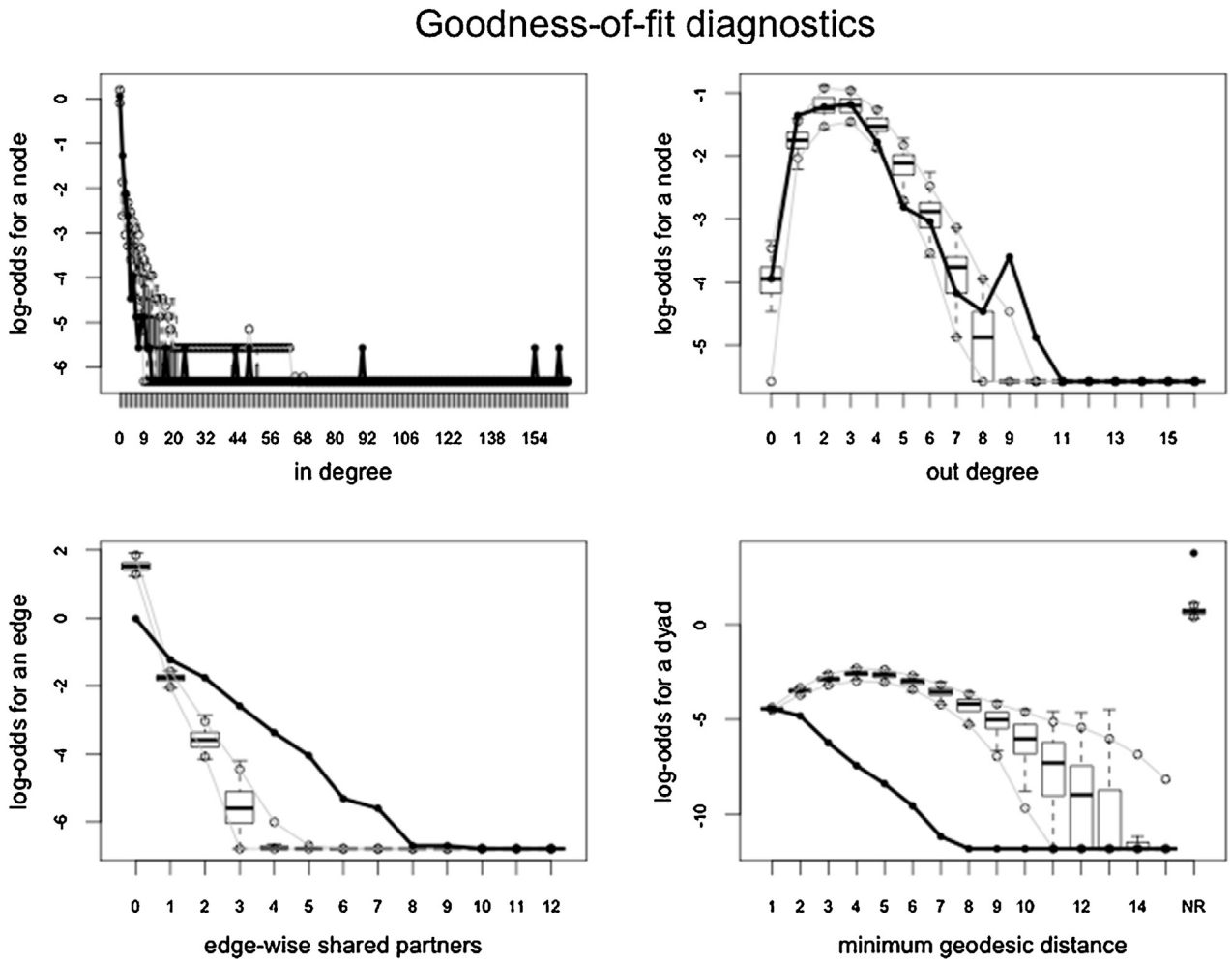
All hypotheses about the motivational effects of personal attributes on security engagement were supported except H7. It appears that homophily effects play an important role in making the employees share security advice and troubleshoot, especially between those of the same gender who work in the same department. Employees holding senior positions and longer tenure were also found to share security advice and troubleshoot with others more. In contrast to our expectation, younger employees tend to share security advice and troubleshoot more. As a result, H7 was not supported despite its statistically significant result.

## 5. Discussion and implications

The discussed findings are most useful for identifying the staff who are active in sharing security advice and troubleshooting in the workplace. First, security managers can select the security-active employees by considering inherent personal attributes such as age, gender, department membership, seniority, and tenure. The advantage of using these personal attributes is that they are easy to recognize by the managers. Security managers aiming to conduct security awareness programs may prioritize the involvement of employees who are young or hold senior positions (e.g., department heads, team leaders), or have worked in the company for a long time. Moreover, employees of the same gender and department membership can also be paired together in a security awareness program to maximize its effectiveness.

The second set of attributes contain those that are more difficult to recognize without asking psychometric questions. These include the security climate perceptions of security practices performed by coworkers, direct supervisors, and top-level managers. Our finding suggests that the observation of direct supervisors' security practices significantly

**Figure 2. Goodness-of-fit of ERGM**




motivates employees to share security advice and troubleshoot with each other. This finding is aligned with those about seniority and tenure levels which we discussed above. In addition to the bottom-up approach, which involves pairing suitable employees, we recommend security managers use supports from the direct supervisors of employees, especially by asking them to serve as role models in performing security tasks.

We found that employees who observe security practices being frequently performed by coworkers and top-level managers are less likely to share security advice and troubleshoot. These findings may characterize a security workplace in which active security engagement is perceived as no longer necessary. While security managers may consider this as an indicator determining a security environment has been developed, we recommend that security activities should be continuously maintained. Doing so helps to prevent development of the false belief of a secured environment. Furthermore, there is a risk of forming collectives where unsafe security workarounds are invented and disseminated without continuous monitoring. Even though we advised that security managers may rely on the direct supervisors of employees to disseminate security directives, it is warned that unsafe workarounds can also be effectively transferred from these supervisors should they neglect security.

Finally, our finding emphasizes the importance of educating employees about personal accountability for the organization's security. The effect of perceived accountability on active security engagement is both statistically significant and strong. Besides improving employees' security knowledge and skills, we recommend that security managers should highlight that every employee is accountable for any security issues resulting from their daily work. We also suggest that accountability can be reinforced by clear and comprehensive security policies, job descriptions, and procedures.

Our research contributes to the emerging research focus that examines the influences of the security workplace on security behaviors, especially

**Table 3. Confirmatory factor analysis results**

| Constructs | Items | Cronbach α | *p*-value | RMSEA | SRMR | CFI |
|---|---|---|---|---|---|---|
| Direct supervisor's security practices | SUP1_1 | 0.910 | 0.314 | 0.021 | 0.0246 | 0.998 |
| | SUP1_2 | | | | | |
| | SUP1_3 | | | | | |
| | SUP1_4 | | | | | |
| | SUP2_5 | | | | | |
| | SUP2_4 | | | | | |
| | SUP2_2 | | | | | |
| | SUP2_6 | | | | | |
| | SUP2_1 | | | | | |
| | SUP2_3 | | | | | |
| Coworker's security practices | COL1_5 | 0.949 | 0.686 | 0.000 | 0.0074 | 1.000 |
| | COL1_1 | | | | | |
| | COL1_2 | | | | | |
| | COL1_4 | | | | | |
| Top management's security practices | CLI1_5 | 0.884 | 0.542 | 0.000 | 0.0257 | 1.000 |
| | CLI1_2 | | | | | |
| | CLI1_3 | | | | | |
| | CLI1_1 | | | | | |
| | CLI1_6 | | | | | |
| | CLI2_2 | | | | | |
| | CLI2_10 | | | | | |
| | CLI2_1 | | | | | |
| Perceived accountability | ACC1_2 | 0.836 | 0.647 | 0.000 | 0.0219 | 1.000 |
| | ACC1_3 | | | | | |
| | ACC1_1 | | | | | |
| | ACC2_2 | | | | | |
| | ACC2_1 | | | | | |
| | ACC2_4 | | | | | |
| | **Criteria** | >0.7 | >0.05 | <0.06 | <0.07 | >0.96 |

by investigating the phenomena from the unique network perspective. First, the finding about the motivational effect of security climate perception of supervisor practices on security engagement supports prior results about leader-member exchange's impact on knowledge sharing (Carmeli et al., 2011). It also mirrored the qualitative finding of Kirlappos et al. (2014) about security workarounds being created and disseminated primarily by direct supervisors to other employees via informal induction. Given the important role of the direct supervisors in communicating security, we are interested in exploring the influential status of the direct supervisors in security. French and Raven's (1959) theory about the bases of power suggested individuals appear influential as they display legitimate authority and expert knowledge. We therefore question which bases of power would be stronger in terms of influencing security decisions and how individuals may develop these power bases. Such understanding would be crucial for security managers to identify and train security champions in the workplace. We anticipate network research that replicates our study with a focus on security influence tie to answer these questions.

While prior security climate studies found perceptions of coworkers and top management security practices motivate compliance (Chan et al., 2005; Goo et al., 2014; Jaafar & Ajis, 2013), our findings suggest these perceptions actually reduce sharing of

**Table 4. ERGM findings**

| | Terms | Terms' effects | Coefficients | Std. Errors | Outcomes |
|---|---|---|---|---|---|
| | edges | Occurrence of security engagement activities between two employees | -3.426*** | 0.246 | |
| H1 | nodeicov.SUP | Employee perceives *supervisor's security practices* more tend to share security advice/troubleshoot | 0.181*** | 0.059 | Supported |
| H2 | nodeicov.COL | Employee perceives *coworker's security practices* more tend to share security advice/troubleshoot | -0.590*** | 0.125 | Not supported |
| H3 | nodeicov.CLI | Employee perceives *top management's security practices* more tend to share security advice/troubleshoot | -0.694*** | 0.032 | Not supported |
| H4 | nodeicov.ACC | Employee perceives *accountability for security* more tend to share security advice/troubleshoot | 2.869*** | 0.137 | Supported |
| H5 | nodematch.Gender | Employees of the *same gender* tend to share security advice/troubleshoot more | 0.386*** | 0.075 | Supported |
| H6 | nodematch. Department | Employees in the *same department* tend to share security advice/troubleshoot more | 1.310*** | 0.085 | Supported |
| H7 | nodeicov.Age | Employees *older in age* tend to share security advice/troubleshoot | -0.104*** | 0.009 | Not supported |
| H8 | nodeicov.Seniority | Employees with *higher seniority* tend to share security advice/troubleshoot | 0.542*** | 0.079 | Supported |
| H9 | nodeicov.Tenure | Employees with *longer tenure* tend to share security advice/troubleshoot | 0.154*** | 0.011 | Supported |
| | isolates | Employees who neither share nor seek security advice/troubleshoot | -0.41 | 0.924 | |
| | idegree(0) | Employees who only seek security advice/troubleshoot | 1.809*** | 0.238 | |
| | odegree(0) | Employees who only share security advice/troubleshoot | -0.754 | 0.602 | |

security advice and troubleshooting. One possible explanation is that employees who observe security practices performed frequently by coworkers and top management do not see the need to share security advice and troubleshoot anymore. It will be interesting for future studies to examine this phenomenon more in depth, and perhaps determine a threshold which informs when and how much security engagement is considered sufficient. Such findings will be useful for security managers to evaluate their security workplace better.

We confirmed the effects of personal attributes such as age, gender, department membership, seniority, and tenure on network engagement (Borgatti et al., 2013). Future qualitative studies are desired to elaborate on why these attributes can result in more sharing of security advice and troubleshooting. For instance, we inferred the influence of physical proximity on security engagement via the significant effect of department membership rather than studying physical proximity directly. One way to analyze physical proximity is to take into account the floorplan of the workplace, such as positions of work desks, floors, and cubicles. Conducting such a study will reveal how the physical arrangements in the workplace can affect security engagement. For example, we can evaluate whether open plan or enclosed offices would be more conducive for diffusion of security awareness.

Most importantly, we offer our study as an empirical demonstration of how to conduct network research in the behavioral security field. We also showed how the traditional approach (i.e., using factor analyses to compute factor scores to be used in ERGM) can be used with network analysis techniques. Future researches may consider examining a plethora of network ties that can be meaningful in a security context such as trust, friendship, security influence, security enforcement, and monitoring networks.

## 6. Limitations and conclusion

Our findings were drawn from ABC's unique context and based on theoretical frameworks such as security climate and accountability theory. Therefore, the findings and their implications are limited to settings similar to ABC or to where the theoretical frameworks can be extended. We expect that the effects may vary in different contexts. For example, security climate perception of coworkers' security practices may hold a more important role in stimulating security engagement in workplaces that lack formal security leadership. Those limitations further justify the need for future studies to validate and extend our research.

Throughout this study we have answered two research questions stated at the beginning. First, we found the security engagement network to be thin and sparse and it contains a few influential nodes that can be technical or non-technical staff. Security groups are also visible in the network diagram and separated by physical location and department membership (e.g., factory and architect divisions). Second, we found security climate perceptions to have statistically significant effects on security engagement, as do perceived accountability and personal attributes. Practical implications of this research primarily focus on strategies to maximize security engagement in the workplace via direct supervisors and education of personal accountability. Furthermore, we hope to offer this research as the foundation for future network studies in the behavioral security field, and we look forward to seeing interesting and practical outcomes from those studies.

## References

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

Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science, 49*(4), 432—445.

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2013). *Analyzing social networks*. Los Angeles: Sage Publications.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research*. New York: Guilford Press.

Carmeli, A., Atwater, L., & Levi, A. (2011). How leadership enhances employees' knowledge sharing: The intervening roles of relational and organizational identification. *Journal of Technology Transfer, 36*(3), 257—274.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy & Security, 1*(3), 18—41.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2014). Towards a complete understanding of information security misbehaviours: A proposal for future research with social network approach. *25th Australasian conference on information systems*. Available at: http://works.bepress.com/siddhi/30/

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2015). Factors of people-centric security climate: Conceptual model and exploratory study in Vietnam. *Australasian Conference on Information Systems*. Available at: http://works.bepress.com/siddhi/39/

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*(3), 319—342.

Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*(6), 391—401.

French, R. P. J., & Raven, B. (1959). The bases of social power. In D. Cartwright (Ed.), *Studies in social power* (pp. 150—167). Oxford: University of Michigan.

Frink, D. D., & Klimoski, R. J. (1998). Toward a theory of accountability in organizations and human resource management. *Research in Personnel and Human Resources Management, 16*(1), 1—51.

Gartner. (2015). *Gartner security & risk management summit*. National Harbor, MD. Retrieved from http://www.gartner.com/binaries/content/assets/events/keywords/security/sec22/sec21tripreport.pdf

Gesell, S. B., Barkin, S. L., & Valente, T. W. (2013). Social network diagnostics: A tool for monitoring group interventions. *Implementation Science, 8*(1), 116—128.

Goo, J., Yim, M., & Kim, D. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication, 57*(4), 1—24.

Guion, R. (1973). A note on organizational climate. *Organizational Behavior and Human Performance, 9*(1), 120—125.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Hall, A. T., & Ferris, G. R. (2011). Accountability and extra-role behavior. *Employee Responsibilities and Rights Journal, 23*(2), 131—144.

Handcock, M. S., Hunter, D. R., Butts, C. T., Goodreau, S. M., & Morris, M. (2008). statnet: Software tools for the representation, visualization, analysis and simulation of network data. *Journal of Statistical Software, 24*(1), 1—11.

Ibarra, H., & Andrews, S. B. (1993). Power, social influence, and sense making: Effects of network centrality and proximity on employee perceptions. *Administrative Science Quarterly, 38*(2), 277—303.

Jaafar, N. I., & Ajis, A. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science, 4*(10), 118—130.

Kim, J.-H., Holman, D. J., & Goodreau, S. M. (2015). Using social network methods to test for assortment of prosociality among Korean high school students. *PLoS ONE, 10*(4.) Retrieved from http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0125333#abstract0

Kirlappos, I., Parkin, S., & Sasse, M.A. (2014). Learning from 'Shadow Security:' Why understanding non-compliant behaviors provides the basis for effective security. *USEC'14 Workshop on Usable Security*. Available at http://www.internetsociety.org/sites/default/files/01_4-paper.pdf

Kuenzi, M., & Schminke, M. (2009). Assembling fragments into a lens: A review, critique, and proposed research agenda for the organizational work climate literature. *Journal of Management, 35*(3), 634—717.

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

Liu, Y., Keller, R. T., & Shih, H. A. (2011). The impact of team-member exchange, differentiation, team commitment, and knowledge sharing on R&D project team performance. *R&D Management, 41*(3), 274—287.

Lusher, D., Koskinen, J., & Robins, G. (2012). *Exponential random graph models for social networks: Theory, methods, and applications*. Cambridge, England: Cambridge University Press.

Merluzzi, J., & Burt, R. S. (2013). How many names are enough? Identifying network effects with the least set of listed contacts. *Social Networks, 35*(3), 331—337.

Morris, M., Handcock, M. S., & Hunter, D. R. (2008). Specification of exponential-family random graph models: Terms and computational aspects. *Journal of Statistical Software, 24*(4), 1548—7660.

Nielsen, T. M., Hrivnak, G. A., & Shaw, M. (2009). Organizational citizenship behavior and performance. *Small Group Research, 40*(5), 555—577.

Otte, E., & Rousseau, R. (2002). Social network analysis: a powerful strategy, also for the information sciences. *Journal of Information Science, 28*(6), 441—453.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology, 88*(5), 879—903.

Robins, G., Pattison, P., Kalish, Y., & Lusher, D. (2007). An introduction to exponential random graph (p*) models for social networks. *Social Networks, 29*(2), 173—191.

Robins, G., Pattison, P., & Wang, P. (2009). Closure, connectivity and degree distributions: Exponential random graph (p*) models for directed social networks. *Social Networks, 31*(2), 105—117.

Schneider, B., & Reichers, A. (1983). On the etiology of climates. *Personnel Psychology, 6*(1), 19—40.

Tohidinia, Z., & Mosakhani, M. (2010). Knowledge sharing behaviour and its predictors. *Industrial Management & Data Systems, 110*(4), 611—631.

Vance, A., Lowry, P. B., & Eggett, D. L. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly, 39*(3), 345—366.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267—284.

Wenger, E. (1998). Community of practice: A brief introduction. *Learning in Doing, 15*(4), 1—7.