Information & Management xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace

Duy Dang-Pham*, Siddhi Pittayachawan, Vince Bruno

School of Business IT and Logistics, RMIT University, Australia

ARTICLE INFO

Article history:
Received 18 March 2016
Received in revised form 13 November 2016
Accepted 8 December 2016
Available online xxx

Keywords:
Security compliance
Security behaviour
Security management
Interpersonal influence
Social network analysis
Exponential random graph modelling

ABSTRACT

As organisations are developing people-centric security workplaces, where proactive security behaviours are fostered, it is important to understand more about the sources of security influence. This research applied social network analysis methods to investigate security influence within a large interior contractor in Vietnam. The findings revealed that security influence occurs between employees in the same department, particularly those in senior positions, have longer tenure or younger age. Engagement in daily work and security-related activities can also increase the likelihood of influencing security behaviours. Moreover, the security influence network is transitive and has a hierarchical structure.

1. Introduction

In the most recent Risk Management Summit [1], security practitioners were discussing the concepts of people-centric workplaces where security controls are relaxed, whereas top management focuses on reinforcing employees' sense of security duties and accountability. This people-centric security workplace puts emphasis on trust and collaboration between the top management and the employees, who are empowered by the training and security communities' culture to make their own informed risk decisions [1]. Even though the security culture of trust and personal accountability was mentioned by Williams [2], Gartner [1] emphasised the importance of these concepts by arguing that preventive and restrictive security controls will be less feasible in the modern digital businesses that demand frequent access to large volume of data. In addition, Kirlappos et al. [3] conducted 118 interviews with employees and managers in a large multinational organisation and found 'shadow security' practices frequently occurred, particularly at a team level. According to these researchers, 'shadow security' practices are security workarounds invented and propagated among the employees within the department, and these practices emerged because of the lack of collaboration and high security burden in daily operations.

The above discussions suggest high dependency of one employee's security behaviours on another. In fact, security practices were argued to involve collective information practices and perceptions of risk that are shared and codeveloped by the communities [4]. Examples of dependency of security behaviours were also documented in research studies, such as the end user's delegation of security responsibility to other individual, technological controls or the organisation [5]. Moreover, Dang-Pham et al. [6] found that a large number of researches have been predominantly testing for the effects of individualistic cognition on the end user's security performance while overlooking the social interactions between them. Therefore, it was suggested that the adoption of social network analysis techniques needs to be explored further.

This study has two key motivations. One is the need to gain more knowledge about security interactions and dependency among the employees. The second motivation is the lack of social network analysis in behavioural security domain. Specifically, we examined the formation of security influence ties or the likelihood of an employee influences another's security behaviours by performing network analysis in a large organisation in South East Asia. The exploratory visual analysis on the network structure and use of exponential random graph modelling (ERGM) technique sheds light on the factors that lead to such formation of security influence. To our knowledge, our study is the first to conduct empirical network analysis in a behavioural security domain. Thus,

* Corresponding author.
E-mail addresses: duy.dang@rmit.edu.au, dtdangpham@gmail.com (D. Dang-Pham).

http://dx.doi.org/10.1016/j.im.2016.12.003
0378-7206/

this study contributes both practical and theoretical implications to the current body of knowledge, particularly by proposing a set of criteria to identify the sources of security influence in the workplace and a demonstration of network analysis in this domain.

2. Literature review

Furnell and Rajendran [7] discussed that security behaviours can be influenced by three workplace-related factors, among which we focus on the factor workplace interactions. They further suggested that security interactions consist of supervisor/management leadership and colleague behaviours, in which the latter was deemed to have more significant direct influence. However, they warned that such weighting based on the focus group could be subjective and vary depending on different cases. Leach [8] also argued that the employees' security behaviours can be affected by senior management and colleagues, and by another interaction between the employees and their employer conceptualised as a psychological contract. These studies provided us the directions to review relevant literatures on security influences that come from supervisor and colleagues' practices.

There are various explanations for why supervisor and colleagues' behaviours could influence security behaviours. For example, researches on security climate have argued that the presence of such practices in the workplace gives rise to the employees' perceptions of information security being treated seriously and prioritised that subsequently motivate their compliance [9–12]. Another way to study the influence of the work communities on one's security behaviours is through subjective norms, which was found as one of the best predictors of security compliance by the systematic literature review of Sommestad et al. [13]. However, both subjective norms and security climate inform little about the specific mechanisms that explain why and how an employee interact with and follow their immediate environment's practices.

By integrating different theories, recent empirical researches elaborated the group's mechanisms that influence the employees' security behaviours, especially through social learning and bonding. For instance, Warkentin et al. [14] adapted Social Learning Theory's perspective and found that situational support, verbal persuasion and vicarious experience have positive impacts on the employees' self-efficacy that motivates their intention to perform security practices. Furthermore, they suggested that organisations may increase security feedback and implement a mentoring system to encourage social learning. In another study, Ifinedo [15] tested Social Bonding Theory's hypotheses and found that increased attachment and involvement lead to higher compliance through positive attitude and subjective norms towards security policies. Most recently, Safa and Von Solms [16] found that subjective norms drove intention to share information security knowledge that arguably mitigated information security risks. With the empirical evidences suggesting the mechanisms of influence in organisational security context, we proceed to consult the theoretical perspectives for additional insights and establish our hypotheses in the next section.

3. Hypothesis development

In network studies, social learning and bonding can be described in the forms of interactions and relations. Furthermore, network interactions and relations, or termed *ties* in general, can be categorised as instrumental (e.g., seek/give work advice) and expressive ties (e.g., be friend with, social support) [17] according to the network theory. Instrumental ties involve the exchange of resources that enable an employee to complete their work-related tasks, whereas expressive ties refer to interpersonal affect and influence [17,18]. Instrumental and expressive ties hold important roles in the workplace, as Saint-Charles and Mongeau [18] found that employees tend to seek the experts in their instrumental network when in uncertain situations (i.e. do not know how to do), whereas trusted friends are more commonly sought in ambiguous situations (i.e. do not know what to do). These findings are consistent with Ashforth [19] theory about the formation of organisational climate, which also involves the process of informational and normative influences that clarify uncertainty and ambiguity and allow the employees to reach a consensus of the meanings of their workplace.

3.1. Instrumental ties and information security influence

An important instrumental network that has been commonly studied is the exchange of work-related advice that contributes to problem-solving and enhancing work processes [17,18]. Besides the 'work advice' network, we consider another instrumental network that facilitates the sharing of organisational updates, such as new procedures and policies. This network is included because information security matter is commonly introduced to the workplace as a component embedded in work procedures and regulations [20].

Previous studies have overlooked the effects of instrumental networks on information security influence, despite their crucial roles in facilitating and maintaining the organisation's operations. When information security priorities are communicated to the employees, some would encounter uncertainty because of their unfamiliarity with the technical requirements and security practices [20]. As reducing workplace uncertainty is one of the employees' basic needs [21], they are expected to clarify their confusion about information security with the colleagues who often collaborate with them in completing daily work tasks [18]. Similarly, seeking advice from sources that often update them with the latest policies or procedures would be useful for reducing such uncertainty as well. Because it demands both specialised (about information security) and job procedural knowledge to perform security behaviours while fulfilling primary work duties, the information sources in the 'work advice' and 'organisational updates' networks could provide relevant advice.

To explain the links between these instrumental networks and information security influence, we reflect on French and Raven [22] theory about the five bases of social power. In particular, this theory posits that a person is perceived as influential when they can make themselves appear as knowledgeable and demonstrate expert power to others. Consequently, the employees in the mentioned instrumental networks, who are sought by others for work-related advice and organisational updates that clarify their uncertainty about security, would hold influential power over the others' security behaviours as well. Thus, we proposed the following hypotheses.

- **H1a**: Employees who give work advice tend to influence others' security behaviours.
- **H1b**: Employees who are sought for organisational updates tend to influence others' security behaviours.

In the behavioural security context, sharing advice about information security [14,16] and providing security troubleshooting [5] can be considered as instrumental ties, because these interactions help the employees to resolve information security issues in their work. It is worth mentioning here that while providing security advice and troubleshooting may appear as two similar behaviours, we will treat them separately in our subsequent analysis. This is because while sharing information security

Please cite this article in press as: D. Dang-Pham, et al., Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace, Inf. Manage. (2016), http://dx.doi.org/10.1016/j.im.2016.12.003