Computers in Human Behavior xxx (2016) 1–11

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace

Duy Dang-Pham*, Siddhi Pittayachawan, Vince Bruno

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

ARTICLE INFO

Article history:
Received 16 March 2016
Received in revised form
1 October 2016
Accepted 25 October 2016
Available online xxx

Keywords:
Information security behaviour
Information security management
Knowledge sharing
Social network analysis
Exponential random graph modeling

ABSTRACT

As modern organisations are dealing with a growing amount of data and strategic information systems, the need to protect these vital assets becomes paramount. An emerging topic in behavioural security field is security advice sharing, which plays a crucial role in helping organisations develop people-centric security workplaces whereby the employees' information security awareness and personal accountability for security are fostered. This research employs social network analysis methods to explore why the employees are willing to share information security advice, as well as examines the structural patterns of this sharing network. We found favourable security attitude and engagement in daily activities have positive impacts on security advice sharing, whereas perceiving too much social pressure makes the employees deliberately refuse to share security advice. We also found security advice sharing is transitive and non-reciprocal, and there are a few dominant employees who control the flow of security advice. Practical recommendations about strategies to increase security advice sharing within the workplace are discussed, and by conducting this research we demonstrate the empirical adoption of social network analysis techniques in the behavioural security field.

1. Introduction

As modern organisations are relying more on their information systems, the need to protect confidential information and mitigate information security risks has become extremely vital (Bulgurcu, Cavusoglu, & Benbasat, 2010). More important, it has been recognised that the human employees are the weakest link in the organisational security chain (Crossler et al., 2013; Dang-Pham, Pittayachawan, & Bruno, 2014), and improving the employees' security awareness has always been a crucial task (Bulgurcu et al., 2010; Safa & Von Solms, 2016). There has been an emerging focus in the recent years on the development of "people-centric security workplaces", where the employees are encouraged to make informed security decisions on their own and actively engage in security activities, rather than simply complying with the policies (Gartner, 2015; Kirlappos, Beautement, & Sasse, 2013). The primary goal of people-centric security workplaces, which was discussed by practitioners in Gartner's (2015) latest Security & Risk Management Summit, aims to increase the employees' autonomy in performing security tasks. To achieve this goal, it was recommended that security managers need to focus on creating a group culture which reinforces personal accountability and security awareness, especially by having the employees understand how their inappropriate security actions may affect the others (Gartner, 2015).

Prior security researches have been focusing on the design and implementation of formal security training and education programmes delivered by top management, which aim to raise the employees' awareness about the aforementioned matters. Nevertheless, the informal security communications that take place within the departments were recently found to have great impacts on the security environment, and thus deserve more attention. For example, Kirlappos, Parkin, and Sasse (2014) found shadow security practices (or workarounds) were invented and disseminated within the departments via informal induction by the direct supervisors. Moreover, Safa and Von Solms (2016) argued that encouraging security knowledge sharing in the workplace, despite the challenges in this task, brings many benefits to the organisation's management of security. These benefits include effectively

* 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).

http://dx.doi.org/10.1016/j.chb.2016.10.025
0747-5632/© 2016 Elsevier Ltd. All rights reserved.

propagating security experiences, knowledge, and ideas amongst the employees, as well as preventing reinvention of the security wheel and allowing more time to spend on the development of better security solutions. We recognised this emerging theme, which focuses on the informal sharing of security knowledge, is a great research opportunity since it aligns well with the practitioners' aim to develop the people-centric security workplaces.

Our second motivation for conducting this research is to contribute a novel and practical research approach to the behavioural security field, by employing social network analysis methods. Dang-Pham et al. (2014) argued that existing behavioural security researches have been predominantly investigating the individualistic features such as people's perceptions of security matters, and suggested that moving beyond the individuals and examining their interactions would yield interesting findings. Their argument is consistent with the perspective that sees organisational security as consisting of collective information practices (Dourish & Anderson, 2006; Dourish, Grinter, Delgado de la Flor, & Joseph, 2004). In fact, Gartner (2015) also explicitly suggested making use of the workplace's social networks to develop the people-centric security workplaces. Since the social network analysis approach treats relational data (e.g. relations and interactions) as its main unit of analysis instead of the individualistic features, its methods are deemed suitable for our research goal. In addition, the lack of behavioural security researches adopting social network analysis methods (Dang-Pham et al., 2014) further motivates us to conduct this study. We capitalise on the strengths of social network analysis methods to answer the following research questions:

- **RQ1:** Why are employees willing to share information security advice?
- **RQ2:** What are the structural patterns of the information security advice sharing network?

2. Literature review

We begin with Section 2.1 that reviews contemporary literature in relation to information sharing practices in the organisational context, with a special focus on information security-related advice. To answer research question 1 and explain the traits that motivate the employees to share security advice, we consulted potential explanations for such behaviour from theory of planned behaviour and accountability theory. These theories are elaborated in Sections 2.2 And 2.3.

2.1. Related work

Besides compliant behaviours, an emerging number of behavioural security studies are focusing on the employees' sharing of information security-related knowledge and advice. This is due to one of the critical issues in this research field that many end-users in organisations do not possess the sufficient knowledge for mitigating information security risks (Rocha Flores, Antonsen, & Ekstedt, 2014). As a result, it became imperative to determine the mechanisms that motivate security knowledge sharing, which is defined as the “provision of task information and know how to help others and to collaborate with others to solve problems, develop new ideas, or implement policies or procedures” (Rocha Flores et al., 2014, p. 92). Active sharing of security advice and knowledge not only helps to develop individual self-efficacy and compliance, but also prevents development of duplicating security practices or “reinventing the security wheel” (Safa & Von Solms, 2016, p. 442). The exchange of information security advice between companies can even enhance expert knowledge and potentially optimise security budget (Tamjidyamcholo, Bin Baba, Shuib, & Rohani, 2014), even though our study is not focusing on this level of security knowledge exchange.

A number of studies focusing on security advice sharing at the employee-level have empirically determined a number of factors that encourage the sharing act. Despite information sharing has been an established theme in organisational research, its importance was recently highlighted in the study of Kirlappos et al. (2013), which proposed training security-aware employees and align security duties with the modern collaborative organisations. For instance, Theory of Reasoned Action and Social Cognitive Theory were employed in the research by Tamjidyamcholo, Bin Baba, Tamjid, & Gholipour (2013) to determine the drivers of the employees' intention to share security knowledge, in which they found trust, norms of reciprocity, and attitude reinforce such intention. Furthermore, Rocha Flores et al. (2014) investigated the same phenomenon but at the organisation-level, where they found formal organisational structures and information security processes result in greater level of sharing security knowledge. Safa and Von Solms (2016) tested hypotheses drawn from Theory of Planned Behaviour and Motivation Theory, and they found that individual's intention to share security knowledge is motivated by attitude, subjective norms, and perceived behavioural control.

Our present research aims to contribute to this emerging area of sharing information security knowledge, especially by employing the novel social network analysis approach to investigate the mechanisms of such sharing. Our methodological choice is closely aligned with the recent research by Dang-Pham, Pittayachawan, and Bruno (2016), which argued that network analysis can make important contributions to the field, where many behavioural security studies have been predominantly focusing on the individualistic variables such as attitude and perceptions. Similarly, it can be observed that the reviewed studies above (Rocha Flores et al., 2014; Safa & Von Solms, 2016; Tamjidyamcholo et al., 2013) all focused on the individual's personal attributes, and thus overlooked the effects that result from relationships and interactions among the individuals.

Moreover, the adoption of network analysis methods allow us to explore the structural features of the security advice sharing network such as reciprocity, which could only be examined as an employee's perception by prior study (Tamjidyamcholo et al., 2013). Since performing social network analysis can reveal the informal structures within an organisation (Borgatti, Everett, & Johnson, 2013), we also anticipate our findings to complement Rocha Flores et al.'s (2014) research, which solely focused on formal structures. Last but not least, we aim to identify the mechanisms of actual sharing behaviour, rather than intention, which was addressed only by the study of Safa and Von Solms (2016).

2.2. Theory of planned behaviour

According to Sommestad, Hallberg, Lundholm, & Bengtsson's (2014) systematic literature review on the contributing factors of security compliance, theory of planned behaviour was found to be one of the most widely adopted theories by behavioural security researches. Theory of planned behaviour was an extension of the well known theory of reasoned action (Ajzen, 2011), and its central premise posits that human behaviour can be driven by three forms of beliefs: behavioural, normative, and control (Ajzen, 2002). The theory argues that people are inclined to perform a behaviour which they evaluate as favourable, or because they perceive the social pressure from their important people which urges them to perform the behaviour. The important extension of theory of planned behaviour is the perception of control over the behaviour (Ajzen, 2011), which dimensionality has been argued to include