Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Investigation into the formation of information security influence: Network analysis of an emerging organisation

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

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

ARTICLE INFO

Article history:
Received 27 August 2016
Received in revised form 18 May 2017
Accepted 25 May 2017
Available online 1 June 2017

Keywords:
Information security influence
Behavioural security
Information security behaviour
Information security management
Social network analysis

ABSTRACT

While prior research has been examining information security behaviours in mature environments with formal policies and practices, there is less attention paid to new or transforming environments that lack security controls. It is crucial to understand what factors affect the formation of an emerging information security environment, so that security managers can make use of the forming mechanisms to improve the security environment without relying too much on enforcement. This research adopts exponential random graph modelling to predict the occurrence of information security influence among 114 employees in a recently established construction organisation. Our empirical findings show that physically co-locating, as well as having specific senior levels and similar tenure can result in more security influence. Other contributing work relationships include the exchange of work-related advice, interpersonal trust, and seeing others as role model and long-term collaborators. The structural features of the information security influence network were also examined, which offer strategies for security managers to diffuse security behaviours within the workplace. Furthermore, specific directions for future network research were elaborated in detail.

1. Background

The need to protect organisational information security has been growing rapidly over the past decades due to heavy reliance of modern organisations on their information systems (Bulgurcu et al., 2010). More importantly, it was realised that technological measures alone cannot protect organisational information security, and organisations require a great amount of the end-users' efforts to perform information security behaviours (Crossler et al., 2013). As a result, the end-users hold a critical role in reducing information systems' risks, while at the same time being the weakest link in the organisation's information security chain (Bulgurcu et al., 2010). Behavioural information security research thus emerged as an important field, which has been contributing to theoretical knowledge and practices with regard to promoting desirable information security behaviours and deterring malicious ones (Crossler et al., 2013).

Empirical evidence has pointed out that information security behaviours differ across contexts and physical locations, even when the same behaviours are examined (Dang-Pham and Pittayachawan, 2015; D'Arcy and Devaraj, 2012; Li and Siponen, 2011). Such differences can be explained by the environmental factors affecting the end-users' cognitive processes that determine how they will perform security behaviours, including

* *Corresponding author.*
E-mail address: duy.dang@rmit.edu.au (D. Dang-Pham).
http://dx.doi.org/10.1016/j.cose.2017.05.010

the availability of adequate security protection, supportive learning resources, or social pressure, just to name a few (D'Arcy and Devaraj, 2012; Ifinedo, 2014; Li and Siponen, 2011; Warkentin et al., 2011). To analyse the contextual differences, prior behavioural security studies have examined information security environments with contrasting features such as public space and home (Dang-Pham and Pittayachawan, 2015), workplace and home (Li and Siponen, 2011), or virtual teams and employees who are physically co-located (D'Arcy and Devaraj, 2012).

Nevertheless, even a formal workplace that has implemented security protection can struggle to maintain its information security workplace, especially during and after organisational transformation processes such as mergers and acquisitions (M&A) (Dhillon et al., 2016; Huang and Chuang, 2007). In fact, organisations could encounter tremendous impacts on its business processes and information systems during such transformation (Robbins and Stylianou, 1999), and organisational failure can be common (Creasy et al., 2009). The transformed environmental factors, such as re-written policies and processes, norms, and technical infrastructure (Dhillon et al., 2016; Huang and Chuang, 2007), or the employees' different perceptions of organisational supports and fit (Creasy et al., 2009), can affect how they perform information security behaviours.

1.1. *Impacts of the workplace on information security behaviours*

Various factors that contribute to the end-users' information security behaviours have been explored by empirical research (Siponen et al., 2014; Sommestad et al., 2014). Most recently, behavioural information security studies focused on the impacts of the workplace's features on the employees' information security behaviours (Dang-Pham et al., 2016). For instance, Warkentin et al. (2011) found that the employees' self-efficacy in performing secure practices can be enhanced by having access to learning resources, such as situational support and verbal persuasion. Furnell and Rajendran (2012) and Padayachee (2012) argued that the employees' information security behaviours can be influenced by their socialisation with supervisors and colleagues. Ifinedo (2014) found evidence supporting that the employees' social bonds in the workplace contribute to their intention to comply with information security policy.

It must be highlighted that while end-users greatly contribute to organisational information security, in other circumstances their information security behaviours can result in dreadful and undesirable consequences. Stanton et al. (2005) identified six types of end-users' information security behaviours, which can be classified based on the end-users' expertise (i.e. novice or expert) and intentions (i.e. malicious, neutral, or benevolent). Information security behaviours carried out with benevolent intention, such as personal compliance with policy (Bulgurcu et al., 2010; Siponen et al., 2014; Vance et al., 2012) or mentoring others on their information security practices (Safa et al., 2016; Warkentin et al., 2011), constitute a secure workplace.

With regard to malicious information security behaviours, Baskerville et al. (2014) postulated that information security abuses occur when the perpetrators find the opportunities to do so by evaluating the security environment. Willison and Warkentin (2013) and Dang (2014) argued that malicious information security behaviours can be caused by work strains and can be prevented early by reducing the workplace stress. Kirlappos et al. (2014) found information security workarounds, or shadow security, are created and diffused at the department level by the employees' supervisors via informal induction. Guo and Yuan (2012) discussed that the intention to perform misbehaviours is not discouraged directly by organisational punishment but rather indirectly via the group social sanction.

The reviewed studies explain how employees can be influenced to perform both desirable and malicious information security behaviours by their peers and supervisors (Furnell and Rajendran, 2012; Ifinedo, 2014; Kirlappos et al., 2014; Padayachee, 2012). In fact, subjective norm, or a form of social influence that comes from the important people of a person, is one of the factors that affect information security behaviours across the studies (Sommestad et al., 2014). Given the impacts of interpersonal influence caused by environmental cues on individuals' security behaviours and organisational security as a whole, further research is needed to explore in-depth for such an influence (Warkentin et al., 2011).

1.2. *Research motivations*

There are limitations in the current body of knowledge that motivated us to conduct this research. First, as the recent research of Dhillon et al. (2016) has pointed out in their literature review, there are few studies that have investigated into the turbulent information security environment that undergo workplace's transformation process. Second, most studies have focused much on the individualistic cognition of the employees, thereby overlooking the dynamics that take place between these employees and in the information security environment.

For instance, behavioural theories such as Theory of Planned Behaviour (Ajzen, 2011) and General Sanction Theory (Straub and Welke, 1998) have been widely employed to understand the mechanisms of the end-users' information security behaviours that are affected by factors of the work environment like subjective norms, perceived behavioural control, or perceived sanction (Padayachee, 2012; Sommestad et al., 2014). However, end-users operate with bounded rationality and limited information (Ajzen, 2011), while environmental factors such as effective sanctions require the end-users to be aware of the sanctions first before perceiving their effects (Straub and Welke, 1998). With the traditional research approach, the end-users' different types of access to organisational resources with different levels of intensity are hard to be captured and analysed in detail (Dang-Pham et al., 2016; Otte and Rousseau, 2002; Sykes et al., 2009). Social network analysis (SNA) techniques have been recently employed in information systems studies to overcome such limitations and to explore in-depth the characteristics of interpersonal influence (Sykes et al., 2009; Zheng et al., 2010). In the behavioural security research field, Dang-Pham et al. (2016) conducted an exploratory study that compared information security networks with other core organisational networks. Nevertheless, their study is exploratory in nature and thus lacks the theoretical perspective.