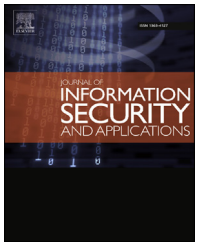
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

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



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

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

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

ARTICLE INFO

Article history:
Available online

Keywords:
Social network analysis
Security behavior
Security compliance
Security influence
Organizational behavior

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, among 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.

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 et al., 2010; Dang-Pham and Pittayachawan, 2015; Kirlappos et al., 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 and Rao, 2009), perceptions of security behaviors and threats (Dang-Pham and Pittayachawan, 2015; Siponen et al., 2014; Vance et al., 2012), or perceptions of security sanctions (Bulgurcu et al., 2010; Herath and 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 and Rogers, 1983; Norman et al., 2005), and General Deterrence

* Corresponding author. School of Business IT and Logistics, RMIT University, Melbourne, Australia.
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.jisa.2016.06.002
2214-2126/

Please cite this article in press as: Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno, Exploring behavioral information security networks in an organizational context: An empirical case study, Journal of Information and Applications (2016), doi: 10.1016/j.jisa.2016.06.002

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 among 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 that 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 et al., 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 regard to the link between socialization and security behaviors, a number of recent studies (Goo et al., 2014; Jaafar and Ajis, 2013) re-visit the concepts of information security climate and their impacts on compliance (Chan et al., 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 and 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 and 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 et al., 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).

The researchers observed the commonalities in these theories and identified an untouched domain worth exploring. The

Please cite this article in press as: Duy Dang-Pham, Siddhi Pittayachawan, Vince Bruno, Exploring behavioral information security networks in an organizational context: An empirical case study, Journal of Information and Applications (2016), doi: 10.1016/j.jisa.2016.06.002