Chapter 84
Effects of Team Collaboration on Sharing Information Security Advice:
Insights from Network Analysis

Duy Dang-Pham
RMIT University, School of Business IT and Logistics, Melbourne, Australia

Mathews Nkhoma
RMIT Vietnam, Department of Business IT and Logistics, Ho Chi Minh City, Vietnam

ABSTRACT

Active sharing of information security advice among the employees has undeniable implications for developing a sustainable security environment. This research examines this topic from the network perspective, and focuses on the work relationships that promote sharing security advice. Exponential random graph modeling technique was employed to evaluate the relationship between team collaborative activities and sharing security advice. The findings revealed that those who share security advice also tend to give work- and IT-related knowledge. Moreover, employees who have similar tenure tend to exchange security advice with each other more. Furthermore, the network of sharing security advice is transitive and has a tendency to form separate clusters. Security managers are suggested to take into account the research findings to identify key employees who frequently share security advice in the workplace and devise appropriate strategies to manage them.

INTRODUCTION

Protecting information security has been a critical business objective of modern organisations (Crossler et al., 2013). However, this objective is also commonly perceived by the employees as a non-task that is irrelevant to their daily work, thus discourages their security duties and actions (M. Siponen & Vance, 2010; von Solms & von Solms, 2004). Worse still, employees facing with a dilemma of achieving job

DOI: 10.4018/978-1-7998-7705-9.ch084

performance and being required to comply with security policy were even found to engage in security violations in exchange for getting their main job done (Guo, Yuan, Archer, & Connelly, 2011). Therefore, the end-users have remained as a weakest link in the security chain, and organisations are advised to leverage the end-users' security awareness to prevent information security incidents (Bulgurcu, Cavusoglu, & Benbasat, 2010; Safa & Von Solms, 2016; Sommestad, Karlzén, & Hallberg, 2015).

Among a plethora of the factors that contribute to end-users' security compliance, sharing information security advice is an emerging topic that holds important implications (Dang-Pham, Pittayachawan, & Bruno, 2016; Safa & Von Solms, 2016; Tamjidyamcholo, Bin Baba, Shuib, & Rohani, 2014). For instance, Tamjidyamcholo et al. (2014) discussed that sharing security advice between organisations may reduce their expenses in information security. At the individual-level, active sharing security advice in a workplace helps to diffuse security awareness as well as prevent re-inventing the same security practices, so that security managers can better invest their time and budget in more important matters (Dang-Pham et al., 2016; Safa & Von Solms, 2016).

Prior research has investigated sharing security advice in two different approaches. For example, (Tamjidyamcholo et al., 2014) and (Safa & Von Solms, 2016) determined the contributing factors of the sharing act by testing theoretically-based models that focus on the end-user's cognition and behaviour. In contrast, (Dang-Pham et al., 2016) analysed the sharing act in the network form of interactions between individuals. They explored and compared the structural features of sharing security advice network with core organisational networks such as exchange of work advice and trust, and used network regression test to assess the networks' relationships (Dang-Pham et al., 2016).

This study employs exponential random graph modeling method to test theoretically-based hypotheses and predict the occurrence of sharing security advice based on team collaboration among the employees in multiple teams of an international university. We aim to evaluate the effects of the salient team collaborative activities that result in sharing security advice, as well as statistically assess the structural features of the sharing security advice network. Ultimately, we will answer the following research questions:

RQ1: What are the structural features of the sharing security advice network?
RQ2: What workplace relationships that encourage sharing security advice among the employees?

LITERATURE REVIEW

Prior behavioural security studies have recognised that end-users are the weakest link of the organisational information security chain (Bulgurcu et al., 2010). In fact, people are considered a critical component of many security governance frameworks (Wu & Saunders, 2011). Baird, Jamieson, & Cerpa (2003) suggested that end-users can intentional or unintentionally cause information security violations, which explains why many technical approaches are bound to fail to prevent security breaches and frauds (Anderson & Anderson, 2001). End-users with the intention to harm information systems, such as stealing and selling information for their own benefit, are labelled malicious insiders (Baird et al., 2003). On the contrary, unintended violations result from end-users who feel uncertain about information security regulations (Dang-Pham, Pittayachawan, & Bruno, 2014; Saint-Charles & Mongeau, 2009), and misuse or misinterpret secure practices (M. M. Siponen, 2000). In fact, ineffective and low collaboration among employees can lead to many security vulnerabilities that are attractive to malicious acts (Schechter &