Chapter 28
Towards a Model of Social Media Impacts on Cybersecurity Knowledge Transfer: An Exploration

Nainika Patnayakuni
Calhoun Community College, USA

Ravi Patnayakuni
University of Alabama – Huntsville, USA

Jatinder N. D. Gupta
University of Alabama – Huntsville, USA

ABSTRACT

Technical solutions to security have been suggested but found lacking and it has been recognized that security is a people issue as well, and behavioral research on information security is critical. Individual learning about cybersecurity is not formal and linear, but complex and network based. In this paper we develop a model of how social media characteristics impact cybersecurity knowledge transfer using technology threat avoidance theory. In developing the conceptual model we seek to answer the following questions. How do users discover cybersecurity knowledge on social media platforms? What are the platform and interaction characteristics that enable them to find cybersecurity knowledge and share this knowledge with others? In doing so we consider the impact of the threat and protection context on cybersecurity knowledge transfer which is different from knowledge transfer in the other contexts.

INTRODUCTION

Information Systems (IS) security is a major concern for organizations as cyber-attacks continue to escalate. Technical solutions to security have been suggested but found lacking and it has been recognized that security is a people and organizational issue as well (Hinde, 2003) and behavioral research on information security is critical (Crossler et al., 2013). People in organizations perform actions that influence an

DOI: 10.4018/978-1-5225-5634-3.ch028

organization cyber security posture and these actions are influenced by policies, procedures, and tools. These policies, procedures and guidelines constitute an organizations knowledge about cybersecurity which may be explicit and managed by a knowledge management systems or tacit and distributed at different horizontal and vertical levels of an organization.

The way knowledge is created and shared is changing in the digital age. While cyber security was the domain of experts and cyber-attacks on organizations were few and far between it was easier for organizations to control what and how cyber-attacks were reported. To believe that learning and behavior of individual and organizations about cyber security is primarily impacted by the formal mechanisms through which an organization approaches cybersecurity is to take objective approach to learning (Driscoll, 2000). New models of learning and knowledge creation suggest that learning is not linear, but complex and network based and "the capacity to form connections" between people, ideas and knowledge is the key to learning in the digital age (Siemens, 2014). At the same time as the half-life of knowledge is falling rapidly the role of social networks and weak ties in creating and distributing knowledge is being recognized (Siemens, 2005).

Social media provides us such affordances of linking with people and their ideas and just as the prevalence of cyber-attacks increases so do social media reports, rumor and hysteria about these attacks. While Edward Snowden and Wiki-Leaks used mainstream and online media for their security leak revelations, ISIS has continually used social media effectively to propagate their threats. And the role of social media in influencing political action such as the Arab Spring cannot be underestimated. As every teenage hacker and script kiddie can find information about creating new attacks online and through social media, and news of cyber-attacks spreads through social networks like wildfire, it becomes difficult to distinguish fact from rumor.

End users are key to information security and their actions are influenced by the information they consume, for example it has been reported that the NSA snooping program changed user online behavior (Hattern, 2014). However, research on the role of social media in influencing perception and actions related to information security does not exist. We develop an exploratory model of the influence of social media on cybersecurity knowledge transfer and how the characteristics of the social media as well as their social networks are likely to influence knowledge transfer. To develop this exploratory theoretical model we draw upon research on social media characteristics (Kietzmann, Hermkens, McCarthy & Silvestre, 2011), individual learning in the digital age (Siemens, 2005), theories on the process of knowledge creation (Nonaka, 1994; Nonaka & Takeuchi, 1995; Gao, Li, & Nakamori, 2002) and social network theories (Granovetter, 1973). In addition we draw upon the Technology Threat Avoidance Theory (Liang & Xue, 2009) to delineate how users' response to perceptions of threat, specifically threat appraisal and coping appraisal mediate the relationship between social media and knowledge transfer about cybersecurity.

In developing the conceptual model we seek to answer the following questions. How do users discover cybersecurity knowledge on social media platforms? What are the platform and interaction characteristics that enable them to find cybersecurity knowledge and share this this knowledge with others? Further what characteristics of the platform or the relational interactions enhance the ability of the users to personalize this knowledge which is likely to impact whether they will change their cybersecurity behaviors. We argue that social influences affect how users acquire cybersecurity knowledge and investigate the characteristics of the platform and relationships that enable knowledge transfer. In doing so, we consider the impact of the threat and protection context on cybersecurity knowledge transfer which is different than knowledge transfer in the other contexts. Consideration of the role of individual characteristics,