International Journal of Information Systems and Social Change
Volume 9 • Issue 1 • January-March 2018

Non-Compliant Mobile Device Usage and Information Systems Security: A Bystander Theory Perspective

Narasimha Paravastu, University of Central Missouri, Warrensburg, Missouri, United States

Claire A. Simmers, Saint Joseph's University, Philadelphia, Pennsylvania, United States

Murugan Anandarajan, Drexel University, Philadelphia, Pennsylvania, United States

ABSTRACT

This study tested the context of employees using their devices for both work and personal use, and non-compliant device usage of a person potentially resulting in Information Systems (IS) security threat to personal as well as work data and/or the devices. Integrating bystander and protection motivation theory (PMT) perspectives this paper studies bystanders' responses to IS security threats and the extent to which a perceived security threat motivates individual intention to act, in the context of non-compliant mobile device usage behaviors. It tests the role of an individual's threat perceptions to protect their own IS security, and as a bystander, protecting their peers or the IS security of their organization. Data collected from 431 individuals support the hypotheses that security awareness predicts perceived severity and protection motivation. Evaluation apprehension and diffusion of responsibility inhibit bystander's intentions to act against non-compliant mobile device usage behaviors, while awareness facilitates it. Theoretical contributions and practical implications of the research are discussed.

KEYWORDS

Bystander Theory, Diffusion of Responsibility, Evaluation Apprehension, IS Security, Partial Least Squares, Protection Motivation, Security Awareness

INTRODUCTION

Security breaches in organizations are a serious concern. Most of the security incidents are a result of employees' noncompliance (Stanton, Stam, Mastrangelo, & Jolton, 2005). In a context where the users may be using their personal mobile devices for work as well as personal use, this study examines individual responses to non-compliant mobile device usage behaviors by their fellow users, such as using unsecure wireless connections for work related purposes to understand the intentions of people, as bystanders, to take action against unsecure mobile device usage practices. In the absence of effectively acting against those unsecure usage practices, there may be a serious threat to IS security of the organization as well as that of personal devices and data of several other users in a BYOD context.

Past research used several behavioral approaches to study the compliance behaviors of employees and users of technology (Anandarajan, Paravastu, Arinze, & D'Ovidio, 2012; Cheng, Li, Li, Holm, & Zhai, 2013; Lim, 2014; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; M. Siponen & Vance, 2010; Sousa, MacDonald, & Fougere, 2012). These approaches are valuable, but do not address the important aspect of how employees as individual IT users in an organization can be a resource

DOI: 10.4018/IJISSC.2018010101

in preserving information systems (IS) security and ensuring compliance. This is a significant gap because employees can potentially act as guardians against violations by other employees, as well as protect themselves against IS security threats. To address this gap, this study uses bystander theory (Darley & Latane, 1968; Fischer, Krueger, et al., 2011; Latané & Darley, 1968, 1969) in the context of IS security and constructs from protection motivation theory (PMT) (Anandarajan, et al., 2012; Johnston & Warkentin, 2010; Ronald W. Rogers, 1975). Bystander theory (Darley & Latane, 1968; Latané & Darley, 1968) provides an insight into individual behaviors in situations of threat to others. Bystander theory suggests that those present at the time of an emergency are less willing to help a victim in the presence of other bystanders, and provides a theoretical framework to understand the facilitating and inhibiting conditions for bystander help. Protection motivation theory (Ronald W. Rogers, 1975; Ronald. W. Rogers, 1983) provides a framework for understanding how user's perceptions about the severity and vulnerability of threats influence user intentions and actions towards protecting themselves. PMT is considered appropriate for information systems security context for understanding of how individuals respond to IS security threats.

Applicability of PMT to the Context of Non-Compliant Mobile Device Usage

An essential condition for application of PMT is the existence of a perceived threat in order for the individual to be motivated to take protective measures (Johnston & Warkentin, 2010). In the context of this study, the users of mobiles devices have both their personal data as well as work related data because many users own the device and also use it for both personal and work purposes. Therefore, any unsecure use by a user whether for personal or work purposes may also threaten the safety of personal data of individual users. These perceptions of threat to their personal data or device in which they have a vested ownership interest. This in turn appeals to their fears motivating them to take protective action such as securing their own devices, usage behaviors (Dang-Pham & Pittayachawan, 2015). Therefore, in a BYOD context of this study where non-compliant usage behaviors of other users are perceived as a threat to their own data security, PMT is considered an appropriate and applicable.

Applicability of Bystander Theory to the Context of Non-Compliant Mobile Device Usage

In the context of this study, non-compliant mobile device usage behaviors by users are viewed as situations that could potentially cause a security situation that could potentially affect several parties: Firstly, the organization for which the users may be working could be exposed to risk of security compromise due to non-compliant usage because the device is being used for work purposes. Secondly, the personal data of the user him/herself may be at risk because the nature of BYOD. Thirdly, the non-compliant usage behaviors of a user can put several other individual BYOD users' personal data at risk indirectly because of the nature of Information Security risks such as infections that could spread across devices or networks rapidly (BPMForum, 2007; Mitra & Ransbotham, 2015). Therefore, other users within the organization who may know about such non-compliant or insecure usage practices from a bystander theory perspective could assume the role of bystanders or the individuals who are present and know about the risk situation to initiate some preventive action to safeguard IS security interests of the organization, and and protect the interests of other BYOD users whose data and/or device may be at risk.

Both PMT and bystander theories are extensively researched in multiple contexts. Within the IS discipline PMT has been tested in the context of IS security (Anandarajan, et al., 2012; Herath & Rao, 2009; Johnston & Warkentin, 2010). Bystander theory has been tested in the disciplines outside IS (Greitemeyer & Mügge, 2015; Harris & Robinson, 1973; Horowitz, 1971; Howard & Crano, 1974; Hurley & Allen, 1974; Latané & Darley, 1968, 1970; Levine, Cassidy, Brazier, & Reicher, 2002), but has not been tested in the context of IS security. However, the basis for both theoretical frameworks is existence of a threat that motivates action of either self-protection as explained by PMT (Rogers,

Exploring Blue- and White-Collar Employees' Well-Being at Work System: Differences in Indicators of Physical and Psychosocial Conditions of Occupational Groups

Seppo Tapio Vayrynenand Heli Katariina Kiema-Junes (2018). *International Journal of Sociotechnology and Knowledge Development (pp. 14-34).*

www.irma-international.org/article/exploring-blue--and-white-collar-employees-well-being-at-work-system/209406