Information & Management 52 (2015) 506–517

Contents lists available at ScienceDirect

Information & Management

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

Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination

Zhiling Tu [a,*], Ofir Turel [b,c], Yufei Yuan [a,1], Norm Archer [a,2]

[a] DeGroote School of Business, McMaster University, 1280 Main St. W., Hamilton, ON, Canada L8S 4M4
[b] Steven G. Mihaylo College of Business and Economics, California State University, Fullerton, PO Box 6848, Fullerton, CA 92834-6848, USA
[c] Department of Psychology, Brain and Creativity Institute, University of Southern California, Los Angeles, CA, USA

ARTICLE INFO

Article history:
Received 22 August 2012
Received in revised form 30 January 2015
Accepted 18 March 2015
Available online 30 March 2015

Keywords:
Mobile device loss or theft
Protection motivation
Social learning

ABSTRACT

The loss and theft of mobile devices is a growing risk that has yet to be addressed in detail by the IS community. This study extends the literature significantly by examining the roles of key information sources in coping and threat appraisal development. This is accomplished by integrating protection–motivation with social learning theories. Through an email interview ($n = 12$) and two surveys (pilot, $n = 115$ and main, $n = 339$), the study identifies and shows how key information sources (knowledge regarding countermeasures, social influences, and experience of the threat) influence users' coping and threat appraisals and, ultimately, coping intentions.

1. Introduction

Given the growing severity and prevalence of information security risks, a growing body of research on users' intentions to apply security measures to cope with such risks has developed [15,16,25,30,31,59,62]. These works largely focus on the emotional (e.g., fear) and rational (e.g., threat severity and likelihood and ability to engage in coping behavior) drivers of users' intentions to engage in coping behaviors. These behaviors include, for example, changing passwords frequently, complying with organizational security standards, and installing software against malicious attacks [2]. Protection motivation theory (PMT) addresses the information sources that are used as a basis upon which threat and coping appraisals are developed, and the Information Systems (IS) literature is relatively silent about such factors. An understanding of the factors and learning processes that lead to threat and coping appraisals is important because it (1) extends the current and partial view of the PMT process in the IS literature and (2) can point to useful practical recommendations. Specifically, by manipulating such antecedents of PMT assessments, companies can improve their users' security compliance or reduce their security deviance. This study, therefore, extends the literature significantly by examining the roles of key information sources in coping and threat appraisal development.

To accomplish this objective, our study integrates protection motivation theory (PMT, [53]) with the social learning theory (SLT, [55]) aspect of social cognitive theory [8]. This integration relies on the premise that coping and threat appraisals are, at least in part, rational and are based on cognitive deliberation that takes into account various information sources. This assumption is reasonable because PMT explicitly relies on such sources of information in the appraisal process, and research has shown that information sources can be a basis upon which coping assessments are formed [65]. The use of SLT for explaining learning processes is also reasonable because it describes learning processes across situations [55], presumably also in the case of mobile device loss and theft. As per PMT, such processes inform the development of the appraisals that people use as a basis for their coping decisions. The viability of this integrative view was supported in the results from a limited set of email interviews, which we describe in Section 4. The results show that users rely on various sources of information (e.g., personal experiences of the threat, which in many cases serve as wake-up calls, and social influences from colleagues, such as co-workers) when developing threat and coping appraisals. In addition, users learn about coping strategies from magazines, media coverage, IT departments, and colleagues.

Consequently, in our model, we argue that coping and threat appraisals are based, in part, on such information sources. Specifically, we posit that users' coping appraisals (self-efficacy

* Corresponding author. Tel.: +1 905 525 9140x26034.
E-mail addresses: tuz3@mcmaster.ca (Z. Tu), oturel@fullerton.edu, ot_739@usc.edu (O. Turel), yuanyuf@mcmaster.ca (Y. Yuan), archer@mcmaster.ca (N. Archer).
[1] Tel.: +1 905 525 9140x23982.
[2] Tel.: +1 905 525 9140x23944.

http://dx.doi.org/10.1016/j.im.2015.03.002
0378-7206/

and response-efficacy) are based, in part, on accumulated knowledge regarding the response and that threat appraisals (perceived threat) are based on past personal experience of threats and the social influence of peers. Consistent with theories that explain IS coping behaviors, we further argue that social influences can also directly drive coping intentions [40]. The remainder of the model replicates past research and posits that coping and threat appraisals increase coping intentions.

The proposed model is tested in the context of mobile devices and focuses on the threat of device loss and theft. These unique contexts and threats differ from those typically examined in the IS literature. This is a distinctive feature of the current study that adds to its contribution. These unique foci were selected for practical and research reasons.

First, from a practical standpoint, the loss and theft of mobile devices is a growing risk that has yet to be addressed by the IS community. Mobile devices are much more likely to be lost or stolen than are desktop computers. Approximately 70 million smartphones are lost each year, and one laptop is stolen every 53 seconds [34]. In the U.S., 113 cell phones are lost or stolen every minute [4]. One in every six users experiences loss, theft or damage to mobile devices such as laptops, smartphones and tablets in a period of 12 months [33]. Theft or loss of mobile devices can also lead to the loss of valuable data assets (e.g., personal information or critical files) and access to vital applications (e.g., email or organizational applications) [43]. Consequently, lost and stolen mobile devices are a great security concern for users and IS professionals [50]. Nevertheless, this threat has not yet received much attention in IS research. Hence, we see an opportunity to examine this issue and to offer practical solutions that may reduce the harm caused by this severe threat.

Second, the unique combination of IT artifact and threat can provide fertile ground for examining the integration of social learning information sources with PMT. The context of mobile device use is significantly different from the context of organizational, stationary information system use [59] and from stationary home environments [2], which have been the foci in past IS research. Mobile devices are mainly owned by individuals, contain much personal information, often allow access to organizational systems, and can be used anywhere. Thus, they present a unique risk profile and, thus, threat severity and coping strategies that may differ from those common in stationary work and home environments. The threat is not only organizational but also very personal, and it can manifest itself anytime and anywhere. In addition, when devices are personally owned, coping may require more self-reliance than reliance on technical support provided by an organization.

Lastly, social factors, including pressures from the work environment, can play an important role in users' security protection in this context. When devices are personally owned, users typically do not receive formal security education and training. Their learning is therefore mainly based on informal information sources such as colleagues, personal experience, and popular media. This effect may be augmented due to the visibility of mobile devices—people can easily see what others have or do on their devices. Consequently, social learning can be salient in mobile environments and arguably represents a highly relevant and unique characteristic of this setting. Moreover, because personally owned mobile devices can be used for both work and non-work-related purposes and we spend a large portion of our waking hours at work and/or addressing work issues, it is reasonable to assume that social influences from the work environment (e.g., colleagues, IT departments) are salient.

Ultimately, the integration of PMT and SLT extends our understanding of the learning mechanisms that drive users' threat and coping assessments and, ultimately, their security behaviors. Moreover, the unique focus on mobile device loss and theft risks extends the breadth of risks and user populations that are examined in the IS literature and offers practical implications for the acute, yet understudied, issue of mobile device loss or theft. The remainder of this paper is structured as follows. In the next section, the theoretical background is given, followed by the development of hypotheses. Next, the paper describes the methods and results. Finally, discussion and conclusion sections are provided.

2. Conceptual background

This study suggests that protection motivation theory (PMT, [53]) and social learning theory [55] can be combined and used as a theoretical lens for explaining users' intentions to employ measures to reduce or prevent damage from the loss or theft of mobile devices. Thus, in this section, we provide background information regarding the context (mobile device loss or theft), followed by a detailed description of the abovementioned theories.

2.1. Mobile device loss or theft

Users carry mobile devices, such as smartphones, laptops and tablets, with them nearly everywhere they go. While such devices are small in size and easy to carry, they can also be easily forgotten, mislaid, or stolen if left unsupervised. Consequently, such devices are vulnerable to a unique risk of loss or theft, which may result in a range of adverse outcomes, as follows: (1) loss of the device (i.e., the potential for physical property loss), (2) loss of data (i.e., the potential of being unable to access needed data and giving others potential access to such data), and (3) loss of service access (i.e., losing the ability to remotely access needed applications and potentially allowing unauthorized access to such applications).

All of these adverse outcomes can cause a major inconvenience. For example, when a mobile device is lost or stolen, a user may be unable to address urgent work. Moreover, replacement costs could be high. In addition, large volumes of very personal data can be lost or fall into the wrong hands. These data may include personal photos and videos (76%), personal email correspondence (64%), passwords to social network and email accounts (22%), work emails (32%), business documents (20%), and financial information, specifically, passwords to online banking accounts (10%) [33][3]. If sensitive personal or corporate data are stored in a device without any protective measures, the data could be misused. This could lead to tarnished reputations, loss of competitive position, and potential litigation [42]. If the device has remote access to other systems, such as banking services, social networks, or enterprise networks, the lost or stolen device may allow unauthorized access to such systems. Consequently, mobile device loss and theft have become a severe security threat to individuals and organizations.

Given the above threat severity, many solutions for preventing or alleviating such damage have been developed. First, some measures are targeted toward *avoidance*. These measures include actions or tools that can eliminate the possibility of mobile device loss or theft (e.g., storing devices in safe areas, not carrying them around, restricting the storage of sensitive information on devices through policies or technologies, and not enabling remote access to sensitive services or networks). Second, if the threat of loss or theft cannot be avoided, *prevention* countermeasures can be used to reduce the likelihood that mobile devices might be lost or stolen and to prevent other people from accessing and maliciously using the devices, data, and remote services. Passwords and data encryption are the most widely applied prevention countermeasures. Many vendors can provide other countermeasures, such

[3] Numbers in parentheses represent the percent of users who have each of these types of information stored on their devices.