Coping with potential mobile device loss or theft risks: A social learning and self-protection perspective

Abstract

The loss and theft of mobile devices is a new type of security threat faced by many users of mobile devices. Unlike employee behavior regarding organizational information system security issues, mobile user security coping behavior is by and large affected by a social learning environment and motivated by self-protection concerns. This study relies on a combination of social learning and protection-motivation theory to explain mobile user behaviors in coping with risks of mobile device loss or theft. We found that user intentions to employ countermeasures are influenced by their self- and coping-efficacy appraisals of threats; and that such appraisals are based in part on various sources of information, including knowledge regarding possible countermeasures, social influences, and past experience. These findings support the proposed model and demonstrate how social learning and protection motivation can be intertwined, ultimately explaining intentions to employ countermeasures against harm from device loss or theft.

Keywords: Mobile device loss or theft, Protection motivation, social learning

Coping with potential mobile device loss or theft risks: A social learning and self-protection perspective

1. Introduction

With the continuing advance and wide-spread use of wireless networks, mobile devices, such as smartphones, laptops and tablets, allow users to access, process and store important information anytime and anywhere. However, mobile devices differ from desk computers, in that they are much more likely to be lost or stolen. About 70 million smartphones are lost each year, and one laptop is stolen every 53 seconds [37]. In the U.S. 113 cell phones are lost or stolen every minute [4]. One in every six users has experienced loss, theft or damage to mobile devices such as laptops, smartphones and tablets in the last 12 months [36]. 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). As pointed out in a recent industry survey, 26 percent of respondents said their organization had data loss or leakage on a smartphone, and 23 percent said they had data loss or leakage on a tablet [45]. Lost and stolen mobile devices are seen among consumers and information systems (IS) professionals as the greatest security concern in the mobile computing environment [55].

Employee security behaviors such as security policy violations have been widely studied in the setting of management information systems [15; 18; 29; 66]. However, when we study mobile user security behavior, the context of mobile device use is significantly different from the context of organizational information system use. A comparison is summarized in Table 1 and reviewed in detail below.

Table 1. Comparison of Organizational Information Systems and Mobile Device Contexts

Security study context	**Organizational information system**	**Mobile device**
Ownership	Organization owned	Mainly privately owned
Usage	For organizational use only	Mainly personal use, with some mix of both personal and business use.
Social environment	Work environment, influenced by colleagues and supervisors	Used anywhere, influenced by family, friends, and colleagues
Security training	Formal policy and security training	Social influence and self-learning
Security responsibility	Organization and IT department	Mostly device owner
Security breach consequence	Organization bears the consequence	Mostly the device owner bears the consequence
Relevant theory for behavior study	Deterrence theory, neutralization theory	Protection motivation theory, social learning theory

Ownership: Management information systems including hardware and software are owned by companies. However, mobile devices are mainly owned by individuals. Although some companies do buy mobile devices for their employees, ownership is often transferred to individuals. The BYOD (Bring Your Own Device) phenomenon also reinforces the legal use of privately owned devices such as smartphones and tablets in a working environment for business purposes [49]. Industry surveys reveal that 89 percent of employees have their mobile devices connected to corporate networks, and 65 percent of corporations allow employees to connect their personal mobile devices to corporate networks [21].

Usage: Management information systems are used by organizations for operations and decision making. However, mobile devices are mainly used by individuals for personal purposes. Although some special mobile devices are used for business only, such as the devices used for police or delivery services, many general purpose mobile devices such as smartphones and notebook

computers are often used for both personal and business purposes. While many employees use their personal devices to handle work-related tasks, such as accessing corporate email and viewing documents, nearly 63 percent of work-issued mobile devices are used by employees for personal activities [56]. "Devices are no longer just consumer devices or business devices. They are both" [55]. As pointed out in a recent report [16], “There appears to be a disconnect between what employees think they can do with their company-issued devices and what policies IT actually dictates about personal usage.”

Social Environment: Management information systems are mainly used in organizational working environments. Any related social influence for workers is usually from their colleagues and supervisors. However, mobile devices can be used anywhere: at home, in public places, as well as at work. Social influences that might affect users of mobile devices are by and large from social networks such as family members, friends, and so on.

Security training: In an organization, one would expect that there would be formal security policies, security education, and training regarding the use of the organization’s information system. However, only one-third of U.S. companies have mobile device usage policies [54]. And mobile users usually do not receive any security training. Their learning is therefore mainly based on informal lessons from friends, their own experience, or self- learning through public sources. Thus, arguably, social learning can be salient in the mobile environment, and represent a highly relevant unique characteristic of this setting.

Security responsibility: For management information systems, employees usually play a role as end-users. They may be required to comply with organizational security policies but usually they believe it is the organization or the technology department that is responsible for the organization’s IS security. Because of private ownership, mobile device users are mainly responsible for the security of their mobile devices, including the prevention of their loss or theft.

Responsibility for security breach consequences: For security breaches of management information systems, the organization involved bears any direct cost and consequences, and employees responsible for security may be sanctioned. For mobile devices, their users bear the full cost and consequences of device and any information loss.

Relevant theory for behavior study: Because of the above differences, existing security behavior studies of organizational information systems have often focused on employee compliance or violation of organizational security policy. Deterrence theory has been used to explain how the severity and certainty of sanctions may affect employee behavior and not the severity and certainty of the security threat because employees do not worry about the risk to the company but are more concerned about the risk of being punished. Formal training and the social norms of colleagues may also be taken into consideration [18]. Neutralization theory has also been used to explain employee security violation behavior because employees try to defend themselves and deny their responsibility for their company's security protection [66]. In the case of mobile device loss and theft, since most mobile devices are mainly used by individuals for personal purposes, there is no fixed security policy to follow. Even when some devices are given to employees by an organization for use in business, the organization's security policy is often rather vague or non-existent. Deterrence theory does not always apply in this case because mobile users are often not forced to follow some policy. Neither does neutralization theory work in this case because users need not find an excuse to defend their lack of attention to security. Since users are responsible for their own devices and bear the cost and consequences of device loss and information loss, if they want to protect themselves and avoid possible negative consequences, protection motivation theory [59] and avoidance theory [42] are arguably more appropriate to model their behavior. Since mobile users usually do not receive formal security training, they often learn by themselves or from their social networks, so the social learning perspective should also be more salient in the mobile device context than in others.

Given the prevalence of mobile device loss and theft, and the above-noted unique attributes of this situation, this study seeks to explain the factors that affect mobile user intentions to prevent and to cope with the threat of mobile device loss or theft. To this end, it uses the analysis lens of Protection Motivation Theory [PMT, 59] combined with the social learning aspect of Social Cognitive Theory [SCT, 8; 61]. PMT explains how people assess threats and coping strategies, and use these assessments for developing coping intentions. At the same time, social learning processes from SCT explain how people learn and adjust their appraisals, presumably also regarding device loss or theft, in response to events in their social environment. We argue that both of these processes (threat appraisal and learning to cope) are important for the development of coping intentions regarding the prevention of damage due to device loss or theft. This perspective is significantly different from previous employee security behavior research based on deterrence theory or neutralization theory, and it is arguably more appropriate in the examined context.

Based on PMT, it is first argued that mobile device loss or theft coping intentions are augmented by user assessments of the threat, their ability to employ countermeasures, and the effectiveness of the countermeasures. Next, it is argued that the abovementioned cognitive processes rely in part on available sources of information. This view is a tenet of social learning theory [SCT, 8; 61] according to which cognitions, such as threat and coping appraisals, are developed in part by social learning processes which take verbal and symbolic sources of information into account. Based on anecdotal evidence and informal discussion with peers, the sources of information in the case of device loss or theft can include past experience of the threat, as well as social pressures to use countermeasures, both of which can increase one's assessment that the threat is likely and viable (i.e., threat appraisal). In essence, users who have experienced loss or theft of their mobile devices may believe that this possibility is more realistic and painful, and hence develop stronger threat appraisals. Similarly, when one's important others (e.g., friends, employer) stipulate that these countermeasures should be utilized, it signals to that person that the risk of device loss or theft is

realistic. The last source of information an informal peers' input pointed to is existing knowledge regarding coping mechanisms (i.e., available countermeasures) which drive coping appraisals. The more people are familiar with possible countermeasures, the more effective they believe they are (response efficacy) and the more confident they feel in their ability to implement these countermeasures (self-efficacy).

A survey to initially assess and refine this model was undertaken with a pilot study involving a convenience sample of 115 mobile device users. The model was then tested and validated with SEM techniques applied to data collected from a cross-section of mobile device users (n=339). By doing so this study advanced not only our understanding of the security behaviors of mobile device users, but also of PMT in this context. Past applications of PMT to IS security behaviors have focused mostly on the cognitions that drive users to cope with security threats (coping and threat appraisals) in organizational information systems contexts. In this study, we expand such established frameworks [34] to include also the sources of information that shape the abovementioned cognitions in an understudied security context, namely mobile devices. It is important to identify these information sources, because many of them can be manipulated by organizations that are providing mobile devices to their employees. Moreover, by taking a social-learning perspective [61], this study also shows that social influence plays a broader role than previously assumed in determining IS security coping behaviors. Not only does it influence coping intentions directly [34], but also through the direct enhancement of threat appraisals, and the indirect enhancement of coping appraisals.

The rest of the 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 used, and the results. Finally the paper reviews the results in discussion and conclusion sections.

2. Conceptual Background

This study suggests that Protection Motivation Theory [PMT, 59] and Social Learning Theory [61] can be combined and used as a theoretical lens for explaining user intentions to employ measures for reducing or preventing damage from the loss or theft of mobile devices. Thus, in this section we provide background 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 smart phones, laptops and tablets, with them almost any place 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 loss or theft, which may result in a range of adverse outcomes. These include: (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 others to access such applications.

All of these adverse outcomes can cause a major inconvenience. For example, when a mobile device is lost or stolen the user may miss important calls, be unable to handle urgent work, or be incapable of accessing his or her device for communications of any kind. Replacement costs could be high as well, particularly for laptop computers, tablets, and smart phones. For convenience, people often store a variety of data in their mobile devices. Based on a survey by Kaspersky Labs in 2013 (Kaspersky 2013), 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%). 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 reputation, loss of competitive

position, and potential litigation [44]. If the device has remote access to other systems, such as banking services, social networks, or enterprise networks, the lost or stolen device may then be misused by unauthorized others. Unauthorized remote access to services could be a great threat to the user's banking account, personal contacts, and a company's information security. Mobile device loss and theft have thus become a serious security threat to individuals as well as organizations.

Given the magnitude of the adverse outcomes, many solutions for preventing or alleviating damage in such cases have been developed. Such countermeasures can be categorized into three groups using the Security Action Cycle [67]. First, some measures are targeted toward avoidance. Avoidance countermeasures refer to actions or tools that can reduce or eliminate the possibility of mobile device loss or theft, such as storing devices in safe areas, not carrying them around when not necessary, restricting the storage of sensitive information on devices through policies or technologies, and not enabling remote access to some 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 and mobile service providers can provide other countermeasures such as user authentication, device blocking, remote device wipe, etc., to prevent unauthorized use of devices when they are lost or stolen.

Third, remedy countermeasures refer to tools and activities that try to cope with the negative consequences of mobile device loss or theft and to compensate for any resulting damage. If a mobile device is lost or stolen, these remedies must be considered immediately. Checking lost and found services would be the first choice in attempting to get a device back. If data stored in the device are confidential, and may affect other people or businesses, notification of the affected party must be implemented immediately. Having important data backed up either online or offline and getting the

data restored is also a common remedy. Remote data wipe services and access blocking can also be useful in this regard. For instance, Kaspersky Lab (www.kaspersky.com) provides recovery services online with several functions including: the Lock & Locate function can block a missing device and identify its location using data received from the smartphone or tablet's GPS; Data Wipe completely deletes all data stored on the device; the Mugshot function can secretly take a photo of anyone using the missing device and send it to the police; the SIM Watch module allows the owner to block the mobile device or delete its memory even if the SIM card is replaced.

While behavioral countermeasures such as avoiding carrying the device are normally useful, they may not always be effective, at least in the areas of prevention and remedy. Thus, this study focuses on technical countermeasures such as remote device wipe, data encryption and password protection which have the potential to be effective in protecting one's device, data and remote access to applications. The problem is that though there are a variety of technical countermeasures that can be used to cope with mobile device loss and theft; many users are not aware of these tools or willing to use them. It is important to analyze the factors that may affect the adoption of technical solutions against device loss or theft. We suggest that Protection Motivation Theory and Social Learning Theory are appropriate lenses of analysis for explaining the driving forces behind such coping behaviors.

2.2. Protection Motivation Theory (PMT)

Protection Motivation Theory [59; 60] explains the formation of individual intentions to cope with a potential threat (protection motivation), and the consequent coping behaviors (coping mode). Such protective behaviors are argued to be driven by fear, which is aroused when a situation is deemed to be dangerous. In response to fear and in order to minimize it, people develop through protection motivation considerations a desire to take protective actions [59] . Fear appeals are multifaceted stimuli which are associated with the severity or seriousness of the noxious event,

perceived vulnerability to the threat, concern over the threat, and coping response efficacy. All of these elements are included in PMT.

PMT argues that one's motivation to protect him or herself stems from his or her assessments of the threat and the efficacy of potential responses. Threat appraisals involve a determination regarding the personal relevance of facts pertaining to the fear appeal of events. People assess a threat based on their own perceptions of the severity of the threat, and their own susceptibility to the threat. Therefore, threat appraisals encompass the individual's estimation of the probability of contracting the threat (perceived vulnerability) and the severity of the threat (perceived severity). For example, when taking a new medication a person may assess the likelihood of having side effects (susceptibility) and the consequences (severity) of such an event. The likelihood of an adaptive response (e.g., avoiding taking the new medication) is increased when perceptions of severity and vulnerability are high, while it is reduced when any rewards associated with executing the target behaviors (choosing to take the new medication) are expected.

Simultaneously to the threat evaluation, people also assess their available resources for coping with a situation. For this, people consider known adaptive recommendations and behaviors, and self-evaluate their ability to cope with, and avert the threat through such behaviors. These assessments pertain to the efficacy of the proposed response to the threat as well as one's self-efficacy regarding the protective actions required to mitigate the threat. The likelihood of an adaptive behavior is increased when high levels of the efficacy variables are present. In other words, perceptions of response efficacy and self-efficacy serve to increase the probability of an adaptive response. For example, the person in the above example may choose to avoid an alley if he or she believes that this countermeasure is efficacious against being robbed, and that he or she could find an alternative route. Therefore, the coping appraisal consists of the individual's expectancy that implementing the recommended behaviors can eliminate the threat (response efficacy) and the belief in one's ability to perform successfully the recommended behaviors (self-efficacy).

The abovementioned threats and coping appraisals, which are the basis for one's intended protection actions, are influenced by external sources of information, on which this study also focuses, because, arguably, these are key in mobile device use contexts in which formal policies and training are often nonexistent. The sources of information include verbal persuasion, observational learning, and prior experiences with similar threats. Thus, threat and coping appraisals mediate the effects of sources of information on intended coping behaviors [60]. In this study we focus on sources of information which may be relevant to the case of device loss or theft countermeasures.

Based on the same root of PMT, Technology Threat Avoidance Theory (TTAT) has been suggested by Liang and Xue (2009) to study IS user protection behaviors and applied to the situation of personal computer usage under the threat of spyware (Liang and Xiue, 2010), and Fear Appeal Theory (FAT) has been applied to explain how fear-inducing arguments may influence end-users taking or complying with recommended security measures such as anti-spyware (Johnston and Warkentin, 2010). These studies consider the context of personal computer usage, and used students as participants rather than organizational information system usage with employees as end users. In the context of mobile device use, PMT is possibly a viable lens of analysis for understanding why mobile users employ technical preventative measures for avoiding threats of device loss or theft, or minimizing the potential damage of such incidents. However, prior personal end-user security research did not consider the sources of information that may affect the threat appraisal and coping appraisal in the PMT model. In this study, the sources of information in the context of mobile device use are examined and fed into the cognitive mediating processes. It is suggested that social learning processes help individuals translate such knowledge signals and cues into threat and coping assessments. Hence, the next section provides a review of Social Learning Theory.

2.3. Social Learning Theory

Social learning processes have been studied by multiple researchers [6; 23; 61]. The common

thread in these theories is that learning from the social environment can inform one's cognitions which in turn can drive behavioral choices. Among these different versions, Bandura's [6; 8] social learning theory has been viewed as the most comprehensive and influential [27; 32; 63].

Bandura's theory explains human behavior in terms of a continuous reciprocal interaction among cognitive, behavioral, and environmental determinants. According to this theory human behavior is stimulated by external influences, by internal processing systems and regulatory codes, and by reinforcing response-feedback systems [6]. The theory states that people can control their behaviors by arranging environmental contingencies, establishing specific goals, and producing consequences for their actions. The role of self-reactive influences is emphasized in motivating and guiding one's behaviors. A self-system refers to cognitive structures that provide the referential standards for behavioral judgments, and a set of sub-functions for the perception, evaluation, and regulation of actions. There are three main sub-functions in the self-regulation of behaviors by self-produced incentives: self-observation, judgment process, and self-response. The first component relates to the selective observation of one's own behaviors in different performance dimensions. Then personal self-reactions are produced through several judgmental processes, which include referential comparison of perceived conduct to internal standards, valuation of the activities in which one is engaged, and cognitive appraisal of the determinants of one's behaviors. Finally, performance appraisals set the circumstances for self-produced consequences, where favorable appraisals activate positive self-reactions and unfavorable judgments lead to negative self-reactions [6; 8].

In the social learning component of Bandura's theory, learning is situated firmly in its social context, and is portrayed as a dynamic interplay between the person, the environment, and the behavior. The theory posits that humans can learn through observation without the need for imitation. Learning from the social environment could be either direct (e.g., by personal experience) or indirect (by observing others' behaviors and the consequences of those behaviors) [6]. This reciprocal interaction provides a comprehensive explanation of the factors that influence people's

learning [48]. This theory therefore posits that people do not merely react to external influences but actually select, organize, and transform stimuli that impinge on them.

Social learning theory has been successfully applied to the study of IS training [17; 35] and IS adoption [33; 74]. However, it has not been used so far to study end-user behavior toward information security. As we have mentioned that mobile users are very much influenced by their social environment through a self-learning process, it is our first attempt to combine social learning theory with protection motivation theory to investigate how signals and cues provided by one's environment cater to the formation of his or her threat and coping assessments.

3. Hypotheses Development

PMT and SLT were used jointly as the basis upon which the proposed research model (see Figure 1) was developed. The model posits that users' coping intentions are affected by appraisals of the threat and coping abilities, as well as by social influences. The threat appraisal is represented by perceived threat, and the coping appraisal includes self-efficacy and response-efficacy assessments. Moreover, these two cognitive processes are influenced by different sources of information, which include the user's knowledge, prior experience of the threat, and social influences. The concept of perceived cost which is an element in the coping appraisal assessment in the original PMT is not included in the current model for three reasons. First, response costs seem to be less important in coping appraisals across behaviors [50], and are hence excluded from many frameworks for explaining IS security compliance [64; 65]. Second, they may be less relevant in the context studied here, because many of the countermeasures are free of charge and require very little effort. Third, the perceived cost of implementing countermeasures against device loss or theft seems not to be theoretically related to the sources of information upon which this study focuses. The proposed research model is presented in Figure 1.

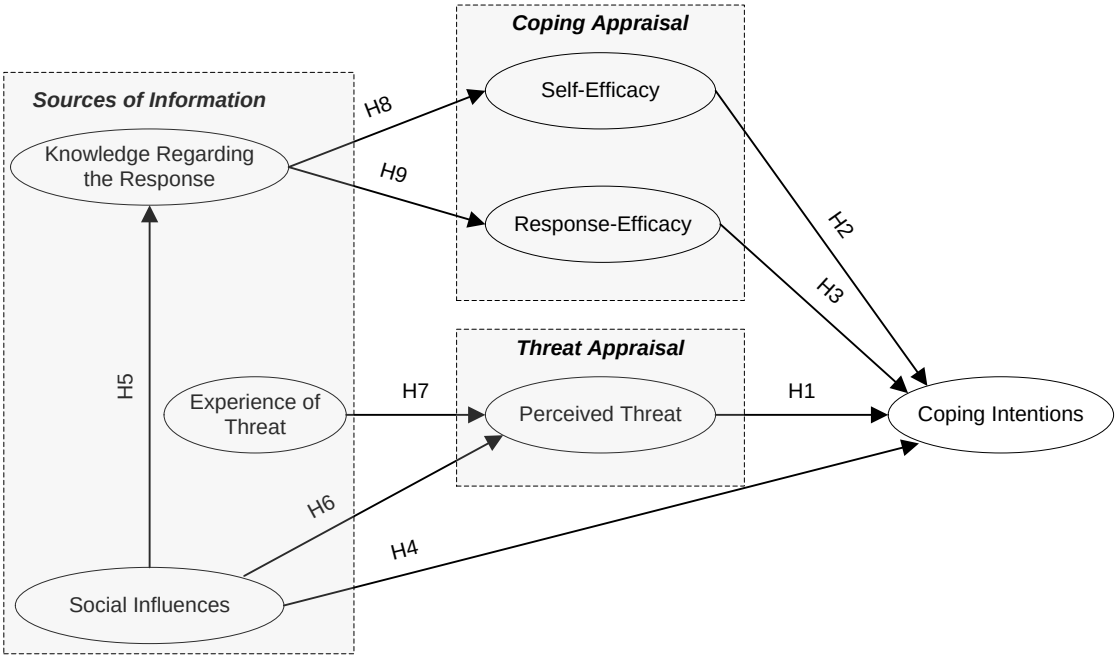

Figure 1: Research Model

3.1. Threat Appraisal Effects

A threat is an external stimulus that exists whether an individual perceives it or not [34]. The perception of threat refers to the anticipation of a psychological, physical, or sociological violation or harm to oneself or others, which may be induced vicariously [73]. People assess threats differently according to their experiences and their levels of threat vigilance [39]. Threat appraisal is often examined through two dimensions, namely perceived vulnerability and perceived severity. Perceived vulnerability refers to the conditional probability that the threatening event will occur, provided that no adaptive behavior is performed, or there is no modification of an existing behavioral disposition [40]. In this study, we define perceived vulnerability as a user's subjectively estimated probability that a loss or theft of his or her mobile device will occur. This is associated with the user's assessment of his/her probability of being exposed to such a threat. Some people may believe that they are more vulnerable to losing their mobile devices when they are naturally careless with keeping track of them. Other people may perceive lower vulnerability to mobile device loss, if they are always cautious and take good care of their devices. Similarly, people living in a community

where theft often occurs may feel more concerned about having their mobile devices stolen than people living in a safer community. Thereby, if a user perceives that a loss or theft may occur, with resulting damage or disturbance to their normal behaviors, they are more likely to be concerned. Conversely, if users do not believe that they are truly confronted by such threats, they are less likely to be concerned.

Perceived severity refers to the degree of physical harm, psychological harm, social threat, economic harm, and danger to oneself and others [40]. Applied to the current context, perceived severity is the extent to which an individual perceives that severe negative consequences would be caused by loss or theft of his or her mobile device. When users perceive a threat, they tend to adjust their behaviors in response to the extent of the damage the threat may cause [73]. The perceived severity of a threat will lead users to behave in a more cautious manner. Conversely, when users perceive that the severity of the threat has diminished, they will likely behave in a less cautious manner. In the event of loss or theft of mobile devices, we expect that at least some users will perceive these events to be a severe threat for themselves, and are hence more likely to consider protective actions.

Previous studies have occasionally found significant separate effects of perceived vulnerability and perceived severity on intentions to adopt protective behaviors in contexts such as the adoption by executives of anti-malware software [40], employee omission of information security measures [73], and user security behaviors in personal computer settings [43]. However, we contend that it is the joint effect of perceived vulnerability and perceived severity that affects threat perceptions. Threat often connotes risk [43]; and risk is typically calculated by multiplying the probability of occurrence with the cost of potential damage from the event [9; 10]. Thus we can define perceived threat as the multiplication of perceived vulnerability and perceived severity. This suggests that the perceived threat will disappear if either of the variables is zero. For example, when a user perceives that his or her mobile device has no chance of being lost or stolen, he or she will not feel threatened,

even if the loss or theft may result in serious damage. Similarly, people using cheap cell phones for phone calls only, may feel that the severity of loss or theft will be insignificant, since it would be easy and inexpensive to replace the devices.

In essence, users' coping intentions towards harms resulting from mobile device loss or theft depend on the joint effect of their perceptions of the likelihood of threat occurrence (perceived vulnerability) and its severity (perceived severity), rather than on their additive effect. Users are expected to develop stronger coping intentions when the perceived threat, as captured by the product of severity and vulnerability of device loss or theft, is high. A similar view, albeit operationalizing perceived threat as severity and vulnerability assessments has been supported in extant research [34; 40; 42; 43; 73].Thus:

H1. *The perceived threat of device loss or theft is positively associated with user intentions to cope with this threat through the employment of technical countermeasures.*

3.2. Coping Appraisal Effects

Coping appraisal involves assessments regarding how much control users have over the threat and what their adaptation options are, given the resources available to them [11]. In this assessment process users first need to determine whether the threat can be effectively prevented if particular safeguard measures are taken [42]. Coping appraisal therefore involves assessments of intrinsic and extrinsic factors available to users to prevent the occurrence of a threatened event, as well as perceptions of whether the threat is preventable [73]. Users, in essence, consider how confident they feel about taking the coping behaviors and how efficacious the coping behaviors are in preventing the threat. Hence, we propose that two constructs: self-efficacy and response efficacy, are assessed in the coping appraisal process.

Self-efficacy assessments influence behaviors through social cognitive theory (SCT)

mechanisms. This theory posits that when people perceive they have the capability to perform an act that benefits them, they will undertake substantial efforts to accomplish that act [6]. Self-efficacy relates to whether or not people feel they have the needed skills and resources to accomplish a goal. If people are highly confident in their ability to conduct a recommended and desirable action, they are more likely to take the action [6]. Applied to the current context, when users believe that they are capable of performing a needed coping behavior to prevent the loss or theft of mobile devices, they will be more motivated to take the coping action. For instance, if a user has high (/no) confidence in using data encryption to protect data on his or her smartphone, he or she may be motivated (/demotivated) to employ this measure. Such effects of self-efficacy on intentions to perform protective actions have been validated in various information security behavior contexts [31; 40; 43; 73]. Thus:

H2. Self-efficacy regarding using technical countermeasures against device loss or theft damages is positively associated with user intentions to cope with this threat through the employment of such countermeasures.

In addition to self-efficacy assessments, people also consider the effectiveness of coping actions as the basis for developing coping intentions [43; 73]. These considerations capture the response's efficacy, i.e., the extent to which a behavior, if executed, is believed to lead to specific outcomes [7]. In the context of IS security, this refers to subjective assessment regarding the ability of a safeguarding measure to avert a security threat [42]. Given available information about countermeasures for coping with security threats, users assess the effectiveness of the advocated adaptive behavior. For instance, some people set up a personal identification number (PIN) or a password to access their mobile devices, in part, because they believe such measures can effectively prevent unauthorized usage. However, other people do not use a PIN or password, because they think that a simple four digit PIN can be easily breached and thus cannot protect mobile devices effectively. Previous studies on IS security have consistently suggested that response efficacy can

predict intended coping behaviors [31; 40; 43; 73]. Replicating these studies we hypothesize:

H3. The perceived effectiveness of technical countermeasures against device loss or theft damage (Response efficacy) is positively associated with user intentions to cope with this threat through the employment of such countermeasures.

3.3. Sources of Information Effects

Mobile device users are often exposed to various behaviors, pressures and cues in their environment. For example, their friends or peers may convince them to employ security measures, or signal to them that such measures are needed by installing them and sharing this information. Users may also be exposed to news and professional materials regarding device loss threats and solutions, or they may have experienced device loss or theft which should help them learn about the severity and susceptibility of such events. Such incidents and actions can serve as sources of information which are used in the coping and threat appraisal processes. In this study we argue that such sources include knowledge regarding potential responses (technical security measures), prior experience of the threat (device loss or theft), and social influences.

Typically, individual users are affiliated with various social and professional groups. The behaviors of such social groups can help individual learn about and choose desirable and socially approved courses of action [57]. This happens through social learning processes as described by social learning theory [6]. According to SLT, people learn from the environmental sources through verbal persuasion and observational learning. Observational learning captures individuals' natural tendency to imitate what they observe others do [32]. Social influence is particularly important in the mobile context due to the ubiquitous and conspicuous nature of the devices. For example, while dining in a restaurant or attending football games, a person is very likely to be seen using a mobile device, which can easily become a topic of conversation with one's peers. Thus mobile device security problems will be subject to a lot more social influence as opposed to some other

technologies, such as using backup software to protect one's data, since the latter typically happens inside one's home and rarely surfaces during daily conversations. In the case of measures against device loss or theft, individuals may simply imitate what their peers do. For example, if one installs a remote data wipe application, others in his or her social circle may follow because they may assume that this is a desirable and socially acceptable behavior. Humans develop such imitation capabilities since infancy [14]. Similarly, people may be verbally convinced by peers to take recommended actions [30].

Arguably, such verbal and observational social influences operate also in the case of countermeasures against device loss or theft. When others in one's social and professional circles use such countermeasures or recommend their use, a person is socially-cued to employ such countermeasures. Similar social-cuing have been observed in multiple contexts [52; 62; 69], including in the cases of IT user threat avoidance [42] and adoption of anti-malware software [40]. Thus:

H4. Social influences regarding the use of technical countermeasures against device loss or theft damages are positively associated with user intentions to employ such countermeasures.

The social environment can also drive behaviors indirectly by providing information regarding an activity and driving learning regarding this activity. In essence, consistent with social learning theory [61], learning is assumed to be largely a social process which synthesizes direct and indirect information from peers, self-observation of the environment as well as other sources in the environment which may be directly or indirectly related to the acquired knowledge. First, by observing others' behaviors, one can gain knowledge regarding such behaviors [68]. Thus, when countermeasures against device loss or theft are employed by important others or one's work colleagues, he or she may increase knowledge regarding such tools through observation. Second, when important others recommend such countermeasures, or when a company provides such

countermeasures, a person may be prompted to learn about such countermeasures as a means to be able to decide whether, how, and to what extent he or she should use them. As such, social influences can facilitate knowledge acquisition [75]. This happens because individuals try to bridge the gap between their current levels of knowledge and the levels needed for executing the socially cued behavior. Indeed, when users lack knowledge and experience regarding IT threat avoidance, the social environment can provide them with information regarding malicious IT risk and possible safeguard measures [42]. Hence:

H5. Social influences regarding the use of technical countermeasures against device loss or theft damages are positively associated with user knowledge regarding such countermeasures.

Social learning theory postulates that human thought is influenced by observations. By observing the outcomes of others, an observer can acquire knowledge of predictable reinforcement contingencies and discern cues for the consequences [5]. In the context of device loss or theft, this learning can pertain to the countermeasures (as posited in H5), as well as to the threat itself. When social cues regarding the use of countermeasures against device loss or theft exist, they may signal to individuals that the threat is real and that they may be susceptible to severe consequences. Otherwise, their important others and work colleagues would not employ (indirect influence) or recommend employing (direct influence) such tools. In other words, direct (e.g., through persuasion) and indirect (e.g., through actions) social pressures will likely be applied only to threats that are deemed important by others; and the perceived risk of a threat can be manipulated through social pressures [5]. Thus, severity and susceptibility assessments of device loss or theft may be based in part on direct and indirect social pressures applied by others. Indeed, people utilize social cues from their environment for threat appraisals [6].. Hence:

H6. Social influences regarding the use of technical countermeasures against device loss or theft damages are positively associated with users' perceived threat of device loss or theft.

In general, people update their perceptions and situational assessments in response to events and direct experience with a behavior [8]. This view is also advanced by social learning theory according to which human thought is influenced by direct experience [38]. In the case of protection motivation, prior experiences with similar threats are intrapersonal sources of information, which can inform individuals' threat appraisals [60]. It is therefore common that the experience of an event, such as myocardial infarction can shape the appraisal of future cardiac risks [70], or the experience of terror attacks can shape terror threat appraisals [41]. Applied to the current context, it is likely that a user who has experienced mobile device loss or theft will have clearer perceptions of the vulnerability and severity of the threat of loss and theft. He or she will rationally see such events as more likely than others who have not experienced such a traumatic event, and potentially as more severe. Hence:

H7. User prior experience of device loss or theft threat is positively associated with perceived threat of device loss or theft.

Coping efficacy assessments can be influenced by individual differences [60]. User knowledge regarding security measures is one such individual difference variable; some users learn and know more than others about countermeasures against device loss and theft. According to social cognitive theory [8], people assess their efficacy by reflecting, in part, on what they know. For example, a person who is weak in math will likely develop weak self-efficacy for solving math problems. Thus, self-efficacy is both learned and modified via vicarious learning [12]. Users develop self-efficacy by determining what they should try to achieve and how much effort they put into their performance in a given situation, i.e., how or whether they put into action the knowledge they have [28]. Applied to the current context, when users have more knowledge regarding countermeasures against the threat, they will likely feel more confident in employing these countermeasures. For example, a user who knows how remote device wipe applications work is more likely to feel efficacious in using these countermeasures than a person who does not even know they exist. Therefore:

H8. User knowledge regarding technical countermeasures against device loss or theft is positively associated with self-efficacy to use such countermeasures.

Knowledge regarding countermeasures can also serve as the basis for assessing the efficacy of the countermeasures. This follows the logic of social cognitive theory [8] according to which beliefs regarding an object or behavior are updated in part based on knowledge regarding the object or behavior. This also follows the logic of PMT [60] according to which response efficacy assessments are developed based on various considerations, presumably including one's state of knowledge regarding the response. Hence, the efficacy of countermeasures should be assessed by considering, among other things, what a countermeasure can do. At one extreme, if no such knowledge exists, the efficacy of the countermeasure will be unclear and diminished. At the other extreme, if someone is familiar with the minute details of the countermeasure and its various functionalities and features, they will likely develop stronger efficacy beliefs regarding the countermeasure. For example, some encryption products include a "time bomb" capability that automatically erases data on the device upon a policy violation such as a number of failed login attempts. This countermeasure can effectively protect confidential data from unauthorized use if the mobile device is lost or stolen. However, without knowing what it is and how it works, users cannot anticipate the outcomes of taking this countermeasure. Therefore, user knowledge regarding a potential response can help them better assess the response's efficacy. Hence:

H9. User knowledge regarding technical countermeasures against device loss or theft is positively associated with response efficacy assessments.

4. Methods

This study included two phases. In the first, a pilot study was used for refining and validating the measurement scales that were based in part on existing scales which were adapted to the context of lost or stolen mobile devices. To this end, factor analysis techniques were applied to data collected

with an online survey from a convenience sample of 115 users of mobile devices prone to be lost or stolen (e.g., laptops and smart phones). In the second phase, data were collected from 339 U.S.-based mobile device users with an online survey administered by a commercial data collection firm[1]. These data were subjected to SEM analyses for validating the hypothesized research model.

4.1. Survey Instrument

The survey instrument captured the model's constructs as well as demographic and descriptive statistics. All measures were based on their theoretical meaning, specific aspects of mobile device loss or theft situations, and relevant literature. Whenever possible, initial scale items were taken from previously validated measures and reworded to relate to the studied context. Using specific mobile device loss or theft risks as identified in above section, several new multiple-item scales were also constructed. The survey items were presented to several academics and were refined based on their inputs. Because individuals may use multiple mobile devices they were asked to choose the mobile device which was the most important to them, and to reflect on this device when responding to the remainder of the survey.

Coping appraisal was measured by two constructs: self-efficacy and response efficacy. These were based on Lee and Larsen [40] and Workman et al. [73] and adapted to the context of this study. Threat appraisal was assessed with a perceived threat construct, which is consistent with the risk assessment literature and amalgamates vulnerability and severity aspects of mobile device loss or theft. The literature review indicated that the loss or theft of mobile devices represents three threats: loss of device, loss of data, and loss of services. Therefore, user threat (vulnerability and severity) perceptions should relate to these three dimensions; and the perceived threat can be conceptualized as the sum of products of the relevant threats' vulnerability and severity. This is consistent with the

[1] http://www.qualtrics.com. The firm was paid $5 per response, out of which respondents received an unknown portion for completing the survey. Respondents were all individuals who agreed to participate in such studies, and they represented a broad cross-section of the US population of mobile device users.

way perceptions and beliefs are operationalized in main theories of human behavior, such as the theory of reasoned action or planned behaviors (e.g., behavioral beliefs are often operationalized as the sum of products of likelihood of outcomes and their level of desirability) [1]. The specific threat items in this study were derived from the IS security literature [40; 42; 73] and adapted to the studied context.

Social influence was operationalized using a formative composite based on Johnston and Warkentin [34], and using the formative measurement specification technique outlined in Diamantopoulos et. al [20] . Experience of threat was operationalized as a binary-response question capturing whether individuals had experienced a loss or theft of their mobile device before (1) or not (0). Knowledge is a context-specific construct that cannot be easily generalized across domains [13]. It was therefore operationalized using items capturing knowledge regarding domain-specific responses, such as data encryption and device blocking. While the items are technology-specific, the underlying construct encapsulates the overall knowledge of individuals regarding countermeasures. In addition, it was assumed that knowledge about the response is inclusive of knowledge of the threat; and hence the latter was not measured separately. For example, it is unlikely that someone knows about anti-virus without knowing what viruses are and their risks. The coping intention scale was based on common behavioral intentions scales [19]. In addition to the model's constructs, the survey captured age, gender and mobile device type (mobile phone or laptop). The measures are listed in **Error! Reference source not found.**.

Table 2: Measurement Instrument

Constructs & Sources	Anchors	Items
Social Influence (formative)	[1=Strongly disagree, 5= Strongly agree]	– People who are important to me think I should implement protection measures for my mobile device. – My service provider has supported measures to protect my mobile device from being lost or stolen.
Knowledge Regarding	[1=I do not know it, 5=I	Please indicate the level of your knowledge regarding the following technologies or services:

the Response	know how it works]	– Data encryption – Device blocking – Remote device wipe – Device tracking
Experience of Threat	[0=never, 1= at least once]	– Did you lose your mobile device before?
Self-Efficacy	[1=Strongly disagree, 5= Strongly agree]	– I have the capability to use data encryption to stop others from getting my confidential data from my lost or stolen mobile device. – I have the capability to set up password to prevent unauthorized access to my services through my lost or stolen mobile device. – I have the capability to backup and to recover my data stored in my lost or stolen mobile device.
Response Efficacy	[1=Strongly disagree, 5= Strongly agree]	– Efforts to keep my mobile device safe would successfully protect my mobile device from loss and theft. – The available preventative measures (e.g. data encryption) would be useful to stop others from getting my confidential data from my lost or stolen mobile device. – The available preventative measures (e.g. password) would be useful to prevent unauthorized access to my services through my lost or stolen mobile device. – The available recovery measures (e.g. backup) would be useful to reduce the damage caused by the loss or theft of my mobile device.
Perceived Threat	[1=Strongly disagree, 5= Strongly agree] Operationalized as the sum of products of susceptibility and severity items regarding the device, data, and services.	***Susceptibility/ Vulnerability*** – There is a good possibility that my mobile device would be lost or stolen. – It is likely that the data stored in my lost or stolen mobile device will be lost. – It is likely that I will lose access to services through my lost or stolen mobile device. ***Severity*** – My lost or stolen mobile devices would cause significant financial loss. – Confidential information stored in my lost or stolen mobile devices could be exposed and thus my privacy would be invaded. – Unauthorized others could access my services through the lost or stolen mobile devices.
Coping Intentions	[1=Strongly disagree, 5= Strongly agree]	– I intend to take measures to stop others from getting my confidential data from my lost or stolen mobile devices. – I intend to take measures to prevent unauthorized access to my services through my lost or stolen mobile devices. – I intend to take backup measures to recover data stored in my lost or stolen mobile devices. – I intend to take measures to remedy the damages caused by my lost or stolen mobile devices.

4.2. Pilot Study

A pilot study was conducted to validate the measurement instrument. Participants were faculty members and students of a North American university, as well as mobile users who were known to one of the researchers. All participants were presently using mobile devices. A total of 184 were approached (using email), and 115 completed the survey (response rate of 62.5%). The sample included 47.8% females. The average age was approximately 27. From these individuals, 56% considered their laptop/notebook to be their most important mobile device, and the rest considered their mobile/smart phone to be their most important mobile device.

The preliminary consistency and reliability of reflective multi-item scales was first established with Cronbach's alphas. Three scores were acceptable ($\alpha_{Knowledge} = 0.85$, $\alpha_{Response\ Efficacy} = 0.81$, and $\alpha_{Coping\ Intentions} = 0.84$), and one was slightly below the recommended threshold ($\alpha_{Self\ Efficacy} = 0.69$). However, the latter score could not be improved by removing items. Thus, for content validity purposes, it was decided to retain these items for further analysis. Next, exploratory factor analysis was performed on these scales with principle component analysis and Promax rotation. The four expected factors emerged; and all items had reasonable loadings (0.51 to 0.92) and substantially lower cross-loadings. Intra-construct correlations ranged from 0.05 to 0.34. These statistics provided preliminary evidence regarding convergent and discriminant validities.

To further establish scale validities, a Confirmatory Factor Analysis (CFA) model was applied to all the measures using the SEM facilities of AMOS 19. In this model all constructs were included except for the formative composite (the CFA model is unidentifiable with this construct). The model produced acceptable fit indices ($\chi^2(94) = 135.3$, CFI = 0.94, IFI = 0.94, RMSEA = 0.062 with p-close = 0.20, and SRMR = 0.071), acceptable intra-construct correlation (-0.04 to 0.49); and all loadings were significant ($p < 0.001$). This further supported discriminant and convergent validities, and allowed us to proceed to the full study.

4.3. Full Study

Data for the full study were collected using an online survey with the scales provided in **Error! Reference source not found.**2. The survey was administered by a commercial survey company to 400 respondents who met the inclusion criteria of US residence and usage of a laptop or mobile device. This approach was taken because it allowed reaching a broad cross-section of the population from different age and professional segments, making the sample possibly generalizable to a large segment of the population. This step yielded a sample of 339 usable records (85% response rate). Of this sample 48.4% were women. The average age was approximately 39, and the modal level of education was college or university degree. About 38.6% focused on their laptop/notebooks as their important devices in the survey, and the rest focused on their mobile/smart phones. Twenty six percent had already experienced loss or theft of a mobile device. The majority used the device for personal purposes (59.9%), and the rest used it for a combination of work and personal purposes (2.1% used it primarily for work, and 38% used it for both work and personal purposes). These data agree with the usage pattern we previously discussed for mobile devices, and the prevalence of mobile device loss or theft.

5. Analysis and Results

5.1. Preliminary Analyses

Three preliminary analyses were conducted before the hypothesized model was examined. First, descriptive statistics and reliability scores were calculated for the constructs. They are presented in **Error! Reference source not found.** together with intra-construct correlations. As one can see, all multi-item constructs have Cronbach's alpha scores above 0.7, Fornell and Larcker's [26] composite reliability scores above 0.7, Average Variance Extracted [30] (AVE) scores over 0.5, and the square root of AVE (on the diagonal) exceeds the corresponding intra-construct correlations. In addition, the correlations are not excessive and range from 0 to 0.66. It was therefore concluded that the scales

that were used are reliable and present sufficient convergent and discriminant validities.

It is interesting to see that in the sample older individuals perceived themselves to have less social influence, reported on lower levels of knowledge regarding potential responses (technologies that could help in coping with the threat), and fewer incidents of loss or theft of mobile devices. These correlations seem reasonable given that age and gender can influence various aspect of mobile device use [58]. At the same time, device type seems to be moderately associated with the outcome variable. Laptop or notebook users seem to have stronger coping intentions compared with those of cell/smart phone users. In addition, the type of primary use of the device (only personal vs. work and/or personal) seems to be associated with some of the model's constructs.

Table 3: Descriptive Statistics, Reliabilities, and Correlations†,††,†††

	Mean (Std. Div.)	Composite Reliability (Cronbach Alpha)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
(1) Social Influence	2.91 (0.97)	Formative	-									
(2) Knowledge re Response	2.52 (1.04)	0.87 (0.87)	0.40**	***0.79***								
(3) Experience of Threat	[yes = 26.0%]	Binary	0.14**	0.09	-							
(4) Self-Efficacy	3.77 (0.73)	0.85 (0.85)	0.33**	0.39**	-0.03	***0.82***						
(5) Response Efficacy	3.86 (0.70)	0.87 (0.86)	0.35**	0.23**	0.00	0.66**	***0.80***					
(6) Perceived Threat	27.06 (14.2)	Index Score	0.20**	0.08	0.17**	0.06	0.20**	-				
(7) Coping Intentions	3.54 (0.85)	0.91 (0.91)	0.53**	0.28**	0.03	0.53**	0.55**	0.26**	***0.84***			
(8) Age	38.87 (13.4)	Binary	-0.18**	-0.24**	-0.13*	-0.00	0.06	0.01	-0.03	-		
(9) Gender	[Male = 51.6%]	Single Indicator	-0.11*	-0.22**	0.01	-0.05	0.07	-0.00	0.01	0.08	-	
(10) Device Type	[Cell = 61.4%]	Binary	0.07	-0.02	-0.15**	0.05	0.03	-0.03	0.15**	0.11*	0.04	
(11) Major Use Type	[personal =59.9%]	Binary	0.32**	0.28**	0.10	0.16**	0.16**	0.06	0.19**	-0.10	-0.15**	0.09

† Square root of AVE is reported on the diagonal for multi-item scales

†† * $p<0.05$, ** $p<0.01$

††† For the gender variable males were coded as 1. Past experience of threat (i.e., losing a mobile device) was coded as 1. For the Device Type variable, laptops were coded as 1, and cell/smart phones as 0. For the major use type "personal" was coded as 0, and a combination of work and personal was coded as 1.

The second preliminary analysis focused on the assessment of Common Method Variance (CMV) risk. Because all assessment techniques have limitations, it is safer to use multiple techniques [53]. First, Harman's single factor test was performed. The test yielded a first component that captured only 31% of the variance. Next, the correlation matrix was assessed as per Pavlou and Gefen [51]. All correlations were below 0.9, and many were as small as zero. Lastly, a latent common method factor that draws equal variance from all observed indicators was included in a CFA model. The model fit the data well ($\chi^2(133) = 243.20$, CFI = 0.97, IFI = 0.97, RMSEA = 0.050 with p-close = 0.52, and SRMR = 0.046), but the loadings of this latent factor were not significant ($p < 0.30$). Moreover, contrasting this model with a CFA model with no latent method factor ($\chi^2(134) = 243.45$) produced a non-significant chi-square statistic ($\chi^2_{diff}(1) = 0.25$). This indicates that adding the method factor fails to significantly improve the chi-square statistic of the model; and that for parsimony reasons the model with no method factor is superior. All of these tests together point to the conclusion that CMV is unlikely to be an important source of variation in the data.

Lastly, while survey data were collected over a period of four days and presented a fairly high response rate, there may still be a risk of non-response bias. To mitigate this risk, we compared the earliest third of the responses collected with the latest third of the responses using Multivariate Analysis of Variance (MANOVA). The results (Pillai's Trace = 0.092, $F(25)=0.8$, $p<0.74$) indicated that there were no omnibus differences between early and late responses, and hence this mitigated risk of non-response bias.

5.2. Model Estimation

After establishing reasonable validity, the proposed model was estimated with the SEM facilities of AMOS 19, using the two-step approach [3] . First, a CFA model was fitted to the data. The model produced acceptable fit indices ($\chi^2(134) = 243.45$, CFI = 0.97, IFI = 0.97, RMSEA = 0.049 with p-close = 0.54, and SRMR = 0.046), which indicated that the measurement model is

likely valid. Thus, it was concluded that it was possible to proceed to the estimation of the structural model. Next, a structural model that included four control variables: age, gender, device type and use type was fitted to the data. The model had adequate fit indices ($\chi^2(206) = 414.6$, CFI = 0.94, IFI = 0.94, RMSEA = 0.055 with p-close = 0.15, and SRMR = 0.085). While all hypothesized paths were significant at $p < 0.05$, the control variables had no significant effect on the endogenous constructs. It is noteworthy to mention that use type had a marginal effect on social influence (-.05, $p<0.07$) and on coping self-efficacy (.09, $p<0.08$) indicating that when the devices were used primarily for personal purposes people felt marginally stronger social influence, and had marginally lower coping self-efficacy compared with others. Nevertheless, even these effects were small and not significant at $p<0.05$. For parsimony reasons they were removed, and the model as depicted in Figure 2 was re-estimated. The fit indices were good χ^2 (142) = 285.7, CFI=0.96, IFI=0.96, RMSEA=0.055 with p-close =0.19, and SRMR = 0.079); and all hypothesized effects were significant.

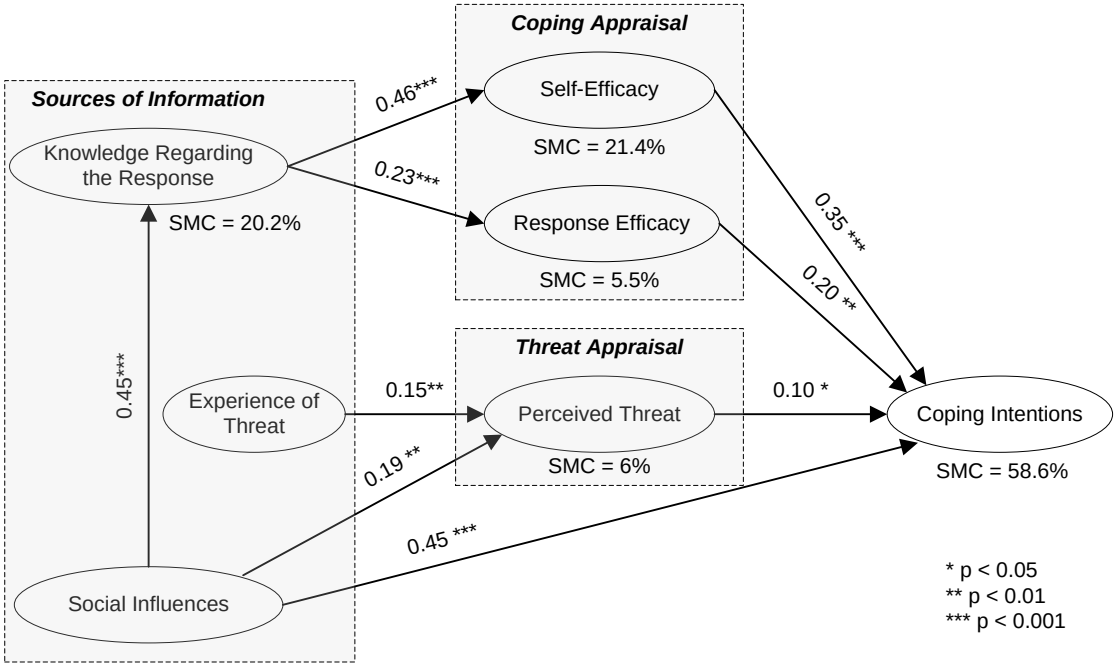

Figure 2: Structural Model

As can be seen, social influence has a broad influence on coping intentions. Not only did it

influence coping intentions directly, as demonstrated in past research [34], but also through the information signals it provides to mobile device users. The signals increase perceived threat to users, and push them to gain knowledge regarding potential technical solutions for the threat. This knowledge in turn increases their coping appraisals as captured by self-, and response-efficacy. Past experience of the threat is also an important source of information, and it drives individuals to perceive the threat to be more likely and more severe. Overall, the model explains close to 59% of the variation in coping intentions.

6. Discussion

Why do mobile device users intend to use technical countermeasures against device loss or theft? The findings indicate that this has to do with protection considerations which are partly informed by social learning processes. As per PMT [60], users of mobile devices simultaneously appraise the severity and susceptibility of the threat of device loss or theft (threat appraisal). They also develop assessments regarding potential technical countermeasures against the harms of device loss or theft (coping appraisal). These threat and coping appraisals serve as the basis upon which intentions to employ such countermeasures (coping intentions) are developed. Specifically, when users perceive the threat of device loss or theft to be strong, or when they strongly believe in their ability to use the countermeasures as well as in the efficacy of such countermeasures to reduce harm, they develop stronger coping intentions (i.e., intentions to employ countermeasures against device loss or theft).

As per the social learning aspect of social cognitive theory [6] the development of threat and coping appraisals is done in part through social cuing and vicarious learning. When important others and organizations support or encourage the use of countermeasures against device loss or theft, it signals to users that the threat of device loss or theft is serious and imminent. It also provides them with information regarding potential countermeasures and drives them to seek knowledge regarding

such solutions. Moreover, in line with other applications of PMT [40; 42], social influences also directly increase intentions to employ countermeasures against device loss or theft.

Consistent with social cognitive theory [8] and protection motivation theory [60], knowledge regarding countermeasures against device loss or theft is an important source of information for efficacy assessments. It increases self- and response- efficacy beliefs. That is, when users are well aware of all the features and inner workings of such solutions, they feel more efficacious in using them and believe that the solutions are better able to reduce the harms of device loss or theft. Lastly, learning through experience [46] also applies to cases of device loss or theft. Users who have experienced such an event perceive the threat to be more severe than others who did not, presumably because they perceive themselves to be more susceptible to device loss or theft, and are well aware of the potential harms of such events.

Altogether, the findings indicate that PMT and social learning processes can be intertwined and influence user intentions to employ countermeasures against device loss or theft. The implications of this view for research and practice are discussed below.

6.1. Implications for Research

We analyzed a special security issue in the mobile device use context and built a user behavior model that combines both self-protection and social learning perspectives. Because mobile devices can be used anywhere and their use is fairly visible; and mobile device loss or theft can be quite prevalent, learning in this contexts relies on multiple sources of information which perhaps may be less relevant in other contexts, including explicit and implicit social influences and personal experience of the threat. By combining the PMT and social learning theory as a means to address unique features of the mobile environment this study makes important strides toward better understanding user security behaviors in the mobile device use context.

First, this study extends the view of PMT employed by past research by adding the social learning perspective. Prior studies have mostly illuminated the importance of threat and coping assessments in the coping behavior development process, e.g., Johnston and Warkentin [34]; and have done so in organizational systems context. This study extends the well-established view that coping and threat appraisals influence coping behaviors, by delving into key social and learning antecedents of such appraisals in the mobile device use context. To do so, it examined key information sources that can shape the development of coping and threat assessments through social and vicarious learning, in an understudied context with a unique set of information sources. That is, while prior research has mostly focused on the cognitive meditational processes (i.e., coping and threat appraisals) as antecedents of coping intentions in organizational systems contexts, this study extends this view such that it includes sources of information as predictors of the cognitive mediation processes in mobile device use settings which are prevalent, yet different and understudied. This perspective, which posits that coping and threat appraisals are mediational mechanisms, is consistent with the PMT model [60]. Hence the findings imply that more research should be done on such information sources, especially in mobile device use contexts, because they have the potential to be the basis upon which important threat and coping assessments are developed. These informational sources can sometimes be manipulated directly by companies and service providers, as opposed to threat assessment. Findings regarding informational sources can therefore also have practical implications.

Second, the findings of this study illuminate the relevance of social learning processes, as well as the applicability of social learning theories to the case of mobile device security behaviors. The findings suggest that mobile device users learn from their environments through observation, imitation, and social cuing, as prescribed by the social learning aspects of the social cognitive theory [8]. While such effects of social cues and pressures on one's threat and coping appraisals have been demonstrated in other contexts [e.g., 50], this study is among the first ones to articulate and

empirically support such broad effects in the case of mobile device security behavior, which is unique in many respects, as per the introduction. It is worth noting that social cues have been shown to influence self-efficacy assessments in the case of privacy policy compliance [72]. Nevertheless, we have argued and demonstrated that social cues and environmental stimuli can also influence threat appraisals. Thus, social cues and other environmental stimuli have a broader influence on protection-motivation processes than previously assumed.

Arguably, the informational sources used in our model, while especially relevant and salient in the mobile device context, may be relevant to other contexts as well. That is, the boundary conditions for the theory which we set in this study to include mobile devices use settings, can be possibly extended to other IS use situations. For example, past incidents of computer virus infection; or pressures from peers or organizations regarding the use of virus defense software may signal to users that such threats are more imminent and influence their threat appraisals. Similarly, knowledge regarding virus protection applications or privacy regulation mechanisms may drive user assessments of their abilities to use tools or comply with such policies. Ultimately, this study can serve as a platform for extending our understanding of user security-related behaviors using a broad PMT view which includes the information sources on which threat and coping appraisals are partially based.

Third, our results support and extend current findings regarding protection-motivation in IS contexts. This study extends the generalizability of the protection-motivation framework to a relatively unexplored, yet important context, i.e., coping with mobile device loss or theft harms. This extension is important, because existing studies often focus on organizational information systems, where the organizations want their employees to protect organizational interests. In such IS contexts, security policies are developed by organizations, and employees are educated and encouraged (through rewards and punishments) to follow these policies. Differing from such studies, the current research applied PMT in a personal mobile usage context, where individual users are personally

responsible for protecting their mobile devices from the threat of loss or theft, without necessarily having policy pressure from the workplace. Hence the findings imply that PMT is also suitable for explaining IS-related personal goal-oriented protective behaviors. Given the prevalence of individual device use, both for personal and work settings ([e.g., the Bring-Your-Own-device trend, see 49; 76]), such protective behaviors regarding one's own device are research-worthy.

Lastly, this study has shown that it is feasible to treat threat appraisals as the product of threat severity and susceptibility. This view is consistent with the operationalization of risk [9; 10], which often includes a product of the event likelihood and the severity of the outcome. Considering threat appraisals as risk assessments opens the door for expanding the body of work on protection motivation in the IS context, by relying on the vast literature on risk [2; 22; 47]. We thus call for future research to add risk analysis aspects, drivers, and outcomes to protection-motivation models.

6.2. Implications for Practice

The findings point to several important implications for mobile service providers, and organizations that provide their employees with mobile devices, mobile device owners, as well as BYOD-enabled organization. The results of this study showed that threat and coping appraisals are important determinants of intentions to employ protective countermeasures against the threat of device loss or theft; and that these assessment are influenced in part by knowledge regarding the response, past experience of the threat, and social influences. Interestingly, many of these antecedents can be modified and manipulated through actions of mobile service providers, organizations that provide their employees with mobile devices, and mobile device owners.

Firstly, this study illustrated the importance of self-protection of personal-IS users. Nowadays more and more technologies such as smart phones and tablets have become consumer products that are used for both personal and working purposes. Social learning therefore should be encouraged by organizations to make self-protection more proactive. However, given the dual-use of many of these

devices (e.g., they can store work documents as well as personal pictures), the responsibility for improving users' coping abilities shifts also to the end-users, who should be motivated to protect their personal assets, learn about loss and theft risks, and act upon their threat appraisals.

Secondly, BYOD enabled organizations (through their IT departments) and mobile service providers should give users access to countermeasures against device loss or theft. This would serve a triple purpose. As per our model it can increase coping intentions directly, increase user threat assessments through social cuing, and increase their knowledge regarding, and awareness of, the countermeasures. Social cues can be amplified by letting users know how many of their friends or co-workers use such countermeasures. This can be done on company portals or by emailing users such information. Presumably such social pressures have the capacity to drive conformity [23], and ultimately the abovementioned triple effect.

Thirdly, it is not enough to provide or give access to such countermeasures. Multiple stakeholders need to increase user knowledge regarding such tools in order to increase user coping appraisals. Organizations can increase user knowledge regarding coping mechanisms by providing mandatory training, or by providing users with incentives (e.g., more remote access privileges, higher pay) if they go through the required training. Organizations can also increase employees' knowledge regarding device loss and theft countermeasures by offering online discussion forums and wikis devoted to such issues, and encouraging participation [71]. Mobile service providers can employ similar means – provide online training to users, or discuss such issues in forums and wikis such that mobile device user knowledge regarding countermeasures against device loss or theft is increased. Users can also actively seek for knowledge in forums, websites and countermeasure applications vendor materials. These actions should help them advance their levels of knowledge, and consequently their self- and response-efficacy assessments.

Lastly, companies can simulate device loss or theft in training sessions and show users what

they might go through in real cases of device loss or theft. Similarly, they can ask users who have experienced device loss or theft to share their presumably painful experiences with others. While none of these steps amounts to actual device loss or theft, they can achieve similar objectives – increase user fear of this event, and impact user beliefs regarding the susceptibility and severity of such an event.

6.3. Limitations

Several limitations of this study should be noted. First, we used a dataset collected at one point in time. Such cross-sectional data may not reflect cognitive changes in the social learning process and support the causality implied by our model. Moreover, because there is often a gap between intentions and actual behaviors, it would be better had we been able to capture consequent coping behaviors. In addition, our model focused on a limited set of information sources. SLT is general and does not point to specific information sources. We hence used informal discussions with peers as well as an application of the SLT logic to the mobile context to elicit this set. Future research can perhaps engage in deeper qualitative analyses and detect a broader set of information sources which can be used for threat and coping appraisals.

Second, because our model was developed around the unique attributes of mobile technologies, the generalizability of our findings may be limited. Moreover, it is possible that the results may be different in other cultures [25], or when applied to other coping behaviors in different IS use contexts. Furthermore, the measures we used were tailored to the current context (mobile devices), and deviated from existing measures which focused mostly on organizational systems. Thus, even though they were validated in the pilot study, caution should be exercised when comparing our results to those presented in past research. In addition, the experience of threat was measured in a binary fashion. Future research can extend this view and examine the effects of the severity and recency of the threat experience.

Lastly, the sample in this study may be somewhat heterogeneous as it taps into different types of devices and uses. On the one hand, this allowed for seeing the forest; i.e., the big picture. On the other, it prevented us from seeing the trees, i.e., the specifics of each situation. While we controlled for these effects and ruled them out, it is still possible that a larger sample will reveal that user behaviors differ by the device they employ and their primary uses of the device. Furthermore, while our model relies on the unique attributes of mobile devices (e.g., that it is relatively easy to lose them and that they are used among other things for personal purposes), it did not capture such attributes and integrated them with the captured concepts. We hence call for future research to enrich our model and include mobile-environments-specific factors.

7. Conclusion

This study sought to explain why people intend to use technical countermeasures against mobile device loss or theft harms. It used a combined protection-motivation and social-learning lens of analysis to explain this phenomenon. The findings indicated that user intentions to employ such countermeasures are influenced by their assessments of the threat, beliefs regarding their ability to employ the countermeasures, and assessments regarding the effectiveness of the countermeasures. These appraisals were informed through social and vicarious learning processes, in part, by available sources of information – social influence, knowledge regarding the countermeasures, and past experience of the threat. Ultimately, this study depicts threat and coping appraisals as mediational mechanisms which are informed by various internal and external sources of information. By demonstrating the viability of such informational sources in forming threat and coping appraisals, this study paves the way for further expansions of the protection-motivation framework and points to several theoretical and practical implications. Future research is encouraged to further expand this view in order to help organizations fight the dangerous epidemic of mobile device loss or theft.

References

[1] I. Ajzen and M. Fishbein *Understanding attitudes and predicting social behavior*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1980.

[2] D.R. Anderson and M.J. Staufacker "The impact of worksite-based health risk appraisal on health-related outcomes: A review of the literature," *American Journal of Health Promotion* (10:6), 1996, pp. 499-508.

[3] J.C. Anderson and D.W. Gerbing "Structural Equation Modeling in practice: A review and recommendent two-step approach," *Psychological Bulletin* (103:3), 1988, pp. 411-423.

[4] S. Arieanna "Unprotected mobile devices at risk with growing mobile theft epidemic," 2013.

[5] A. Bandura "Social-learning theory of identificatory processes," In *Handbook of Socialization Theory and Research*, D. Goslin (Ed.), Rand McNally, 1969, pp. 213-262.

[6] A. Bandura "Self-efficacy: toward a unifying theory of behavior change," *Psychological Review* (84:2), 1977, pp. 191-215.

[7] A. Bandura "Self-efficacy mechanism in human agency," *American Psychologist* (37:2), 1982, pp. 122-147.

[8] A. Bandura *Foundations of Thought and Action: A Social Cognitive Theory*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1986.

[9] R. Baskerville "Risk analysis: An interpretive feasibility tool in justifying information systems security," *European Journal of Information Systems* (1:2), 1991, pp. 121-130.

[10] R. Baskerville "Information systems security design methods: Implications for information systems development," *ACM Computing Surveys* (25:4), 1993, pp. 375-414.

[11] A. Beaudry and A. Pinsonneault "Understanding user responses to information technology: A coping model of user adaptation," *MIS Quarterly* (29:3), 2005, pp. 493-524.

[12] N.E. Betz and G. Hackett "The relationship of career-related self-efficacy expectations to perceived career options in college women and men," *Journal of Counseling Psychology* (28:5), 1981, pp. 399-410.

[13] N. Bontis "Assessing knowledge assets: a review of the models used to measure intellectual capital," *International Journal of Management Reviews* (3:1), 2001, pp. 41-60.

[14] A. Brugger, L.A. Lariviere, D.L. Mumme and E.W. Bushnell "Doing the right thing: Infants' selection of actions to imitate from observed event sequences," *Child Development* (78:3), 2007, pp. 806-824.

[15] B. Bulgurcu, H. Cavusoglu and I. Benbasat "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), 2010, pp. 523-548.

[16] Cisco "Cisco 2013 Annual Security Report," 2013.

[17] D.R. Compeau and C.A. Higgins "Application of social cognitive theory to training for computer skills," *Information systems research* (6:2), 1995, pp. 118-143.

[18] J. D'Arcy, A. Hovav and D. Galletta "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1), 2009, pp. 79-98.

[19] F.D. Davis "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* (13:3), 1989, pp. 319-340.

[20] A. Diamantopoulos, P. Riefler and K.P. Roth "Advancing formative measurement models," *Journal of Business Research* (61:12), 2008, pp. 1203-1218.

[21] Dimensional Research "The impact of mobile devices on information security: A survey of IT professionals," 2012.

[22] B.T. Doerr and E.B. Hutchins "Health risk appraisal: process, problems, and prospects for nursing practice and research," *Nursing research* (30:5), 1981, pp. 299-306.

[23] J. Dollard and N.E. Miller *Personality and Psychotherapy: An Analysis in Terms of Learning, Thinking, and Culture*, McGraw-Hill, New York, 1950.

[24] N. Epley and T. Gilovich "Just going along: Nonconscious priming and conformity to social pressure," *Journal of Experimental Social Psychology* (35:6), 1999, pp. 578-589.

[25] D.P. Ford, C.E. Connelly and D.B. Meister "Information systems research and Hofstede's culture's consequences: An uneasy and incomplete partnership," *Ieee Transactions on Engineering Management* (50:1), 2003, pp. 8-25.

[26] C. Fornell and D. Larcker "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18), 1981, pp. 39-50.

[27] S.K. Gibson "Social learning (cognitive) theory and implications for human resource development," *Advances in Developing Human Resources* (6:2), 2004, pp. 193-210.

[28] J.E. Grusec "Social learning theory and developmental psychology: The legacies of Robert Sears and Albert Bandura," *Developmental Psychology* (28:5), 1992, pp. 776-786.

[29] K.H. Guo, Y. Yuan, N.P. Archer and C.E. Connelly "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems* (28:2), 2011, pp. 203-236.

[30] B.C. Hardgrave, F.D. Davis and C.K. Riemenschneider "Investigating determinants of software developers' intentions to follow methodologies," *Journal of Management Information Systems* (20:1), 2003, pp. 123-151.

[31] T. Herath and H.R. Rao "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), 2009, pp. 106-125.

[32] B.R. Hergenhahn and M.H. Olson *An Introduction to Theories of Learning (5th ed.)*, Prentice-Hall, Upper Saddle River, NJ, 1997.

[33] W. Hong, J.Y. Thong, L.C. Chasalow and G. Dhillon "User acceptance of agile information systems: A model and empirical test," *Journal of Management Information Systems* (28:1), 2011, pp. 235-272.

[34] A.C. Johnston and M. Warkentin "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), 2010, pp. 549-566.

[35] M. Karjalainen and M. Siponen "Toward a new meta-theory for designing information systems (IS) security training approaches," *Journal of the Association for Information Systems* (12:8), 2011, pp. 518–555.

[36] Kaspersky Lab "Security in a multi-device world: the customer's point of view," 2013.

[37] Kensington "Cost of stolen or lost laptops, tablets & smartphones," 2011.

[38] G.P. Latham and L.M. Saari "Application of social-learning theory to training supervisors through behavioral modeling," *Journal of Applied Psychology* (64:3), 1979, pp. 239-246.

[39] R.S. Lazarus *Emotion and Adaptation*, Oxford University Press, New York, 1991.

[40] Y. Lee and K.R. Larsen "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," *European Journal of Information Systems* (18:2), 2009, pp. 177-187.

[41] L.J. Lengua, A.C. Long and A.N. Meltzoff "Pre-attack stress-load, appraisals, and coping in children's responses to the 9/11 terrorist attacks," *Journal of Child Psychology and Psychiatry* (47:12), 2006, pp. 1219-1227.

[42] H.G. Liang and Y.J. Xue "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly* (33:1), 2009, pp. 71-90.

[43] H.G. Liang and Y.J. Xue "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems* (11:7), 2010, pp. 394-413.

[44] A. Loo "Security threats of smart phones and bluetooth," *Communications of the ACM* (52:3), 2009, pp. 150-152.

[45] Lookout.com "Five key business insights for mobile security in a BYOD world," 2013.

[46] R.A. Mar and K. Oatley "The Function of Fiction is the Abstraction and Simulation of Social Experience," *Perspectives on Psychological Science* (3:3), 2008, pp. 173-192.

[47] R.D. Marshall, R.A. Bryant, L. Amsel, E.J. Suh, J.M. Cook and Y. Neria "The psychology of ongoing threat - Relative risk appraisal, the September 11 attacks, and terrorism-related fears," *American Psychologist* (62:4), 2007, pp. 304-316.

[48] S.B. Merriam and R.S. Caffarella *Learning in Adulthood (2nd ed.)*, Jossey-Bass, San Francisco, 1999.

[49] K.W. Miller, J. Voas and G.F. Hurlburt "BYOD: Security and Privacy Considerations," *It Professional* (14:5), 2012, pp. 53-55.

[50] S. Milne, P. Sheeran and S. Orbell "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology* (30:1), 2000, pp. 106-143.

[51] P.A. Pavlou and D. Gefen "Building effective online marketplaces with institution-based trust," *Information Systems Research* (15:1), 2004, pp. 37-59.

[52] C.L. Pickett, W.L. Gardner and M. Knowles "Getting a cue: The need to belong and enhanced sensitivity to social cues," *Personality and Social Psychology Bulletin* (30:9), 2004, pp. 1095-1107.

[53] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee and N.P. Podsakoff "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), 2003, pp. 879-903.

[54] Ponemon Institute "Global study on mobility risks," 2012.

[55] R. Power "Mobility and security: Dazzling opportunities, profound challenges, Carnegie Mellon CyLab," 2011.

[56] F.Y. Rashid "Mobile device data losses pose rising security risk: Survey," *eWeek*, 2011.

[57] R.R. Reno, R.B. Cialdini and C.A. Kallgren "The transsituational influence of social norms," *Journal of Personality and Social Psychology* (64:1), 1993, pp. 104-112.

[58] R.E. Rice and J.E. Katz "Comparing internet and mobile phone usage: digital divides of usage, adoption, and dropouts," *Telecommunications Policy* (27:8-9), 2003, pp. 597-623.

[59] R.W. Rogers "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology* (91:1), 1975, pp. 93-114.

[60] R.W. Rogers "Cognitive and physiological process in fear appeals and attitude change: a revised theory of protection motivation," In *Social Psychophysiology: A Source Book*, R. Petty (Ed.), Guilford Press, New York, 1983, pp. 153-176.

[61] J.B. Rotter *Social learning and clinical psychology*, Prentice-Hall, NY, NY, 1954.

[62] D.N. Ruble and C.Y. Nakamura "Task orientation versus social orientation in young children and their attention to relevant social cues," *Child development* (43:2), 1972, pp. 471-80.

[63] H.P. Sims and P. Lorenzi *The New Leadership Paradigm: Social Learning and Cognition in Organizations*, Sage, Newbury Park, CA, 1992.

[64] M. Siponen, M.A. Mahmood and S. Pahnila "Are Employees Putting Your Company At Risk By Not Following Information Security Policies?," *Communications of the Acm* (52:12), 2009, pp. 145-147.

[65] M. Siponen, S. Pahnila and M.A. Mahmood "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), 2010, pp. 64-71.

[66] M. Siponen and A. Vance "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), 2010, pp. 487-502.

[67] D.W. Straub and R.J. Welke "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

[68] G. Szulanski "Exploring internal stickiness: Impediments to the transfer of best practice within the firm," *Strategic Management Journal* (17), 1996, pp. 27-43.

[69] L. Trotter, M. Wakefield and R. Borland "Socially cued smoking in bars, nightclubs, and gaming venues: a case for introducing smoke-free policies," *Tobacco Control* (11:4), 2002, pp. 300-304.

[70] C. Vögele, O. Christ and H. Spaderna "Cardiac threat appraisal and depression after first Myocardial Infarction," *Frontiers in Psychology* (3), 2012, pp. 1-7.

[71] C. Wagner "Supporting knowledge management in organizations with conversational technologies: Discussion forums, weblogs, and wikis," *Journal of Database Management* (16:2), 2005, pp. I-VIII.

[72] M. Warkentin, A.C. Johnston and J. Shropshire "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:3), 2011, pp. 267-284.

[73] M. Workman, W.H. Bommer and D. Straub "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24:6), 2008, pp. 2799-2816.

[74] H.D. Yang, J.M. Yun and C. Rowley "Social influence on knowledge worker's adoption of innovative information technology," *Journal of Computer Information Systems* (50:1), 2009, pp. 25-36.

[75] H. Yli-Renko, E. Autio and H.J. Sapienza "Social capital, knowledge acquisition, and knowledge exploitation in young technology-based firms," *Strategic Management Journal* (22:6-7), 2001, pp. 587-613.

[76] H. Yun, W.J. Kettinger and C.C. Lee "A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance," *International Journal of Electronic Commerce* (16:4), 2012, pp. 121-151.