MOBILE TECHNOLOGY USE IN ORGANIZATIONS: A CONCEPTUAL FRAMEWORK

Abstract

The purpose of this study was to develop a behavioral framework based on the Protection Motivation Theory to examine how employees' behavior can influence organizations' information security policies. The application of this framework will provide a link between the organization's information security policies and the employee perception towards these policies. The results of this study will provide mechanisms to improve overall security processes across the enterprises. Also this study represents future trends and provide useful direction for the IS community.

Keywords: protection motivation theory, security behavior, security policies

Introduction

Internet's growth has enabled a variety of applications and platforms, which encourage people's participation to use mobile devices. (Duggan, 2015; Duggan & Brenner, 2013). More and more companies adopt business solutions based on the use of mobile technologies (Abadi, Kabiry, & Forghani, 2013; Harris & Patten, 2014; Markelj & Bernik, 2012). Kim and Hwang (2012) stated that mobile devices have changed our way of doing business as well as our routine activities. But the major concern for information systems (IS) managers and IS professionals is the employees' security behaviors (Garba, Armarego, Murray, & Kenworthy, 2015).

Mobile and wireless communications have an amazing growth that resembles the rapid growth of the Internet in the mid-90s (Castells 2011; Rahman & Sharma 2012). Wireless communications provides a more effective form of mobility and performance which is not limited to the users in a confined space without affecting the work to be performed effectively (Yang, Ricciato, & Zhang, 2006). For this reason, many businesses and corporate environments make changes to incorporate wireless infrastructure according to the rise in demand of smartphones and tablets (Lee & Won 2012). Indeed, the flexibility of these types of devices exposes them to many different security vulnerabilities (Macía, Lanfranco, Venosa, & Sabolansky, 2015; Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013).

With the increased use and rising capabilities of mobile devices, there has been an increase in attacks and threats through these devices. Precisely, it is this accessibility that has become a very attractive target for malware creators (Fossi, et al. 2011). When accessing corporate data from personal devices, the risks of data leakage is especially accentuated. This leakage is due, not only for the loss of devices, but also by viruses and malware (Harris & Patten, 2014).

Many studies have emphasized the threats from outside the organization by proposing perimeter security strategies to keep threats outside the organization. But today, the threat is also present within the company in form of an unsafe directed behavior by the employees, intentional or unintentional (Bulgurcu, Cavusoglu, & Benbasat, 2010; Macía et al, 2015). Intentional unsafe directed behavior refers to deliberately disruptive, unethical, or illegal behavior enacted by individuals who possess substantial internal access to the organization's information assets (Stanton, Mastrangelo, Stam, & Jolton, 2004). On the other hand, unintentional unsafe behavior refers to inexpert individuals who misuse information resources such as forwarding spam emails, sharing password with colleagues or friends, using mobile devices carelessly outside the company among others (Bulgurcu et al. 2010; Stanton et al. 2004).

Purpose of the Study

The purpose of this study is to examine how employees' behavior can influence organizations' information security policies. We developed a behavioral framework based on the Protection Motivation Theory (PMT). This study will provide a link between the organization's information security policies and the employee perception towards these policies. The primary research question to be addressed in this study was: How does user's behavior of mobile technology affect organizational security? This question leads to the following research objectives:

- To determine if the employees know that their actions can make them more vulnerable to threats.
- To determine whether people who have suffered consequences of cyber threats and hazards, have changed their behavior to a more secure conduct.
- To determine which constructs of the Protection Motivation Theory affect or lead safe behavior, by the end user in the organization.

Literature Review

Several studies have examine the influence of users' behaviors, users' privacy, and security policies (Camacho, Ferrer, Rivera, & Ojeda, (2014); Hu, Dinev, Hart, & Cooke, 2012; Macía et al, 2015; Teh, Ahmed, & D'Arc, (2015). Organizations establish computer security policies to ensure the security of information resources. Many employees, and general users are unaware of the dangers they face using mobile devices (El-Maliki and Seigneur, 2013; Bajikar 2002). Alexandrou and Chen, (2014) reported that when using mobile devices in the healthcare industry, each individual perceives security risks differently and likewise their possible consequences. According to Alexandrou and Chen, the success of security management system appears to depend upon the effective behavior of the individuals involved in its use. Among the common security risks published are physical security, mobile malware, unauthorized access, and inadequate use (Hu, Dinev, Hart, & Cooke, 2012; Macía et al, 2015; Markelj & Bernick, 2012).

Symantec, leader in security application and antiviruses' software, has identified more than one million apps infested with malware and 2.3 million were classified as problematics applications (Symantec Report, 2015). The damage made by mobile malware includes the theft of confidential data from a device, the eavesdropping of ongoing conversation by a third party, incurring extra charges through sending SMS, user tracking, and other injuries (Mohite

2014). Consequently, based on these threats, the organization chooses the appropriate security mechanisms in order to protect itself from these attacks. But, safety is not only determined by physical security mechanisms implemented in the infrastructure, but also on the behavior of the individual in relation to security (Ng et al. 2009).

Literature have identified elements that are considered safe or unsafe, intentional or unintentional behavior. The vulnerability elements play a leading role in these behaviors, which can lead to the severity of a threat. This can be countered with the efficacy and training provided by IT staff and will therefore achieve better safe behavior of end-users with managing mobile devices and IS of the organization. Vulnerability refers to be susceptible to any kind of threat (Posey, Roberts & Lowry, 2015). While severity refers to the degree of physical and psychological harm a threat can cause (Pahnila, Siponen, & Mahmood, 2013). Thus, efficacy is the ability to develop a desired result or effect according to the experience of others. Pahnila et al. (2007) described efficacy as an individual's ability or capabilities to perform the response actions.

According to Pahnila et al. (2007) severity refers to the consequences to individuals if a security threat occurs. One way to present the severity to employees is by articulating the severity of the threat that is, the degree of harm associated with a threat (Johnston and Warkentin 2010). The vulnerability, on many occasions, is constituted precisely by the employees. Macía et al. (2015) and Pahnila et al. (2007) exposed that if employees do not see that they are truly confronted by IS security threats, they will hardly comply with IS security policies which creates vulnerability. The organizations tend to be more apprehensive about vulnerability to external threats; research suggested that a significant proportion of security incidents originate from inside the organization (Macía et al., 2015; Stanton et al., 2005).

The effectiveness in an end-user can be measured according to how they react to a threat and how they use the given recommendations (Johnston and Warkentin 2010). Also, individuals with confidence in their abilities are more likely to initiate challenging behaviors than inexpert users (Ng et al. 2009; Pahnila et al. 2007; Bulgurcu et al. 2010). Safety training and orientation play a very important role when trying to change the behavior of people about security (Pahnila et al. 2007). Thus, organizations can incorporate a persuasive communication emphasizing in the factors related to the formation and sensitivity of security which can motivate the end users to evaluate and change their behavior (Bulgurcu et al. 2010).

Organizations typically develop and implement plans, policies, protocols, and procedures for guaranteeing the security of information resources, along with user training programs and governance structures to promote compliance with security policies and procedures (Johnston and Warkentin 2010). A security behavior is defined as user's predisposition and interest concerning practicing computer security (Johnston and Warkentin 2010). The security behavior of employees play an important role, and this calls for more research studying the factors that influence individual’s decision to practice computer security (Johnston and Warkentin).

Theoretical Framework and Conceptual Model

The Protection Motivation Theory (PMT) was originally developed by Rogers in 1975 in order to better understand fears and how people handle them. Rogers expanded the theory in 1983 to a more general theory of persuasive communication (Boer, 1996). PMT is a major theory that attempts to explain the perceptive process of behavioral change in terms of threat. The threat initiates two cognitive processes: threat appraisal and coping appraisal (Boer). The threat appraisal process evaluates the factors associated with the behavior that potentially creates danger including the severity of the danger and one’s vulnerability to it.

Boer (1996) exposed that threat appraisal is the estimation of the chance of contracting a disease (vulnerability) and estimates of the seriousness of a disease (severity).

Coping appraisal consists of response efficacy and self-efficacy (Boer, 1996). The coping appraisal process evaluates one's ability to cope with and prevent the threatened danger (response efficacy), balanced with the costs associated with protective behavior (Boer). Response efficacy is the individual's expectancy that carrying out recommendations can remove the threat. Self-efficacy is the belief to execute the recommend courses of action successfully. These two appraisal pathways: threat and coping, combine to form protective motivation and therefore the change in behavior (Boer, 1996).

Perceived Vulnerability (PV)

It refers to how an individual feels susceptible to a reported threat (Posey et al., 2015). This construct represents the part of threat where end-user can perceive threat of a developing hazard. This feeling can lead to fear in an individual and who reacts accordingly to this fear. In relation to threats and adversities, vulnerability is a concept that links the relationship that people have with their environment to social forces and the cultural values that sustain and contest them (Posey et al., 2015).

Perceived Severity

Refer to the degree of physical harm, psychological harm, social threats, economic harm, dangers to others rather than oneself, and even threats to other species (Sun et al. 2013; Lee and Larsen 2009). This construct represents the part of threat that the end-user can feel the reality latent danger. Perceived severity has been greatly used in the clinic or health area describing how a person, once suffered a severe disease tend to change his habit or behavior towards the cause of the disease (Boer, 1996; Ng et al., 2009).

Response Efficacy

Refers to the belief that the adaptive response will work in averting an undesirable threat concerns (Lee and Larsen 2009). Boer (1996) stated that by handling appraisal, evaluates the mechanisms that are relevant for the evaluation of the coping responses. These components are an individual's expectancy in carrying out the recommendations that can remove threats and the belief in one's ability to perform a recommended courses of action successfully. This construct aims to measure whether hints provided by other help to have or improve safe behavior.

Security Training

Security computer training was found to significantly improve an individual's computer self-efficacy. According to Herath and Rao (2009) security literature has placed a strong emphasis on the availability of resources, including training, the online availability of policies and other mechanisms of promoting and enabling policy compliance. The persuasive communications, by the IT personal, are an effective method for modifying human attitudes, intentions, and behaviors secure. Johnston and Warkentin (2010) recommended the use of persuasion in security management, specifically citing emotions as a leverage point from which persuasive messages can affect attitudes and motivation in a positive manner.

Security Behavior

IT personal and administrators are responsible to set up and provide security, users are responsible for practicing security countermeasures. Thus, for effective security, users have to make a conscious decision to comply with the organization's security policies and adopt security behavior (Ng et al. 2009).

The results of this study will provide mechanisms to improve overall security processes across the enterprises. Also this study represents future trends and provide useful direction for the IS community. The findings provide a basis for further research and a guide for curriculum evaluations. Now this study discusses the proposed model and hypotheses. From Protection Motivation Theory, this study will use the constructs perceived severity and perceived vulnerability to measure the effects of threat appraisal. Perceived response efficacy will measure coping appraisal. Security training is the moderating construct in the research framework. The moderating constructs is used to measure the balance of costs involved in promoting safety.

The proposed model in Figure 1 serves to understand how employees' behavior can influence organizations' information security policies.

Figure 1. Model User Secure Behavior (USB)

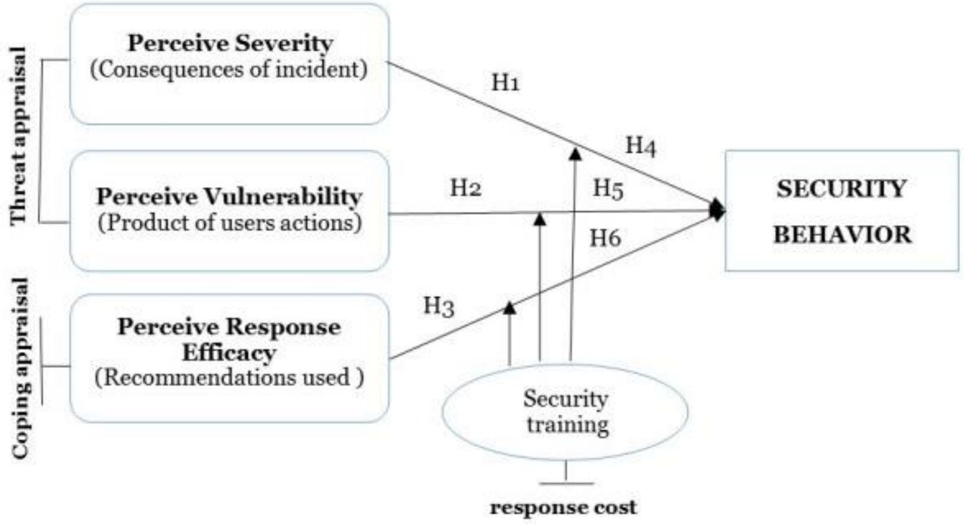

Figure 1. Model User Secure Behavior (USB). Developed by authors

Hypotheses Development

PMT identified the perceived threat severity as the first primary component of a fear appeal that contributes to an addressee's reaction, in other words, the ability to influence the intensity of a response to this threat (Johnston & Warkentin, 2010). When the person perceives an imminent threat or danger he or she tends to look for the mechanisms of action or defense, known as countermeasure. This threat serves as a trigger that activates defense mechanisms which lead to a safe behavior.

Security risks arise from multiple sources and environments especially with the introduction of mobile technology in the enterprise (Warkentin and Willison 2009). Vulnerability refers to the inability to withstand the effects of a hostile environment.

Organizations concern is to try to reduce vulnerability looking for safe behavior in specific information systems. For this reason companies are creating a security policies and guidance as to what can be perceived as a threat to both the company and the end-users.

Efficacy is the capacity to produce an effect. It indicates the ability for beneficial change of a given intervention. Response efficacy refers to a person's beliefs as to whether the recommended action step will actually avoid the threat. According to Johnston and Warkentin (2010), if managerial security communications appeal to users' perceptions of threat, susceptibility and perception of response efficacy; then the desired result should be security behavior enhanced. PMT identified response efficacy as the main determinant of coping appraisal (Milne and Orbell 2000).

IT security training can provide persuasive messages that can be incorporated into interdepartmental communications (Johnston and Warkentin 2010). Through this, it is possible to recreate an event of chance at which any end-user has been involved and the consequences he faced. The training will provide a better perception of severity of the threat and its respective real consequences.

Organizations have been implementing security training and awareness programs to educate users. An effective awareness program should influence a user's attitude and behavior to be more security-conscious (Ng et al. 2009). The training is the best mechanism that can bring knowledge of threat to end-users. According to Ng et al. (2009) the importance of efficacy indicates the need for security training so that users are equipped with the confidence in their skills to practice the appropriate security behavior. Greater emphasis on training and motivating employees to act securely will generate great payoff for the organizations that pursue a better security behavior (Warkentin and Willison 2009). The above discussion leads to the following hypothesis:

H_1:   Perceived severity of security incidents is positively related to security behavior.

H_2: Perceived vulnerability of how others communications threat is positively related to adopt security behavior.

H_3: Response efficacy will have a positive effect on end user intentions to adopt recommended individual security behavior.

H_4: Security training impact the perception of severity.

H_5: Security training impact the perception of vulnerability.

H_6: Security training will have a positive effect on response efficacy

Methodology

The purpose of this study is to examine how employees' behavior can influence organizations' information security policies. This is a non- experimental study with a transversal research design in which there is no intentional manipulation of the variables (Hernández, Fernández, & Baptista, 2014). This study will use a quantitative approach using the survey method to collect the data. The questionnaire will be distributed by email and through personal contacts. To calculate the sample size it will be used a level of confidence of 95% and a margin error of 5%.

The questionnaire was designed based on the literature. The questionnaire will ask respondents their perceptions on the latent variables: perceived severity, perceived vulnerability, response efficacy, and security training. Several researchers have provided the exogenous factors to measure the latent variables. Accordingly, to gain respondents answers a 5-point Likert scale will be used in which 1 represents strongly disagree to 5 represents strongly agree. All the latent variables or unobservable variables will be related with the measures identified. The questionnaire also will gather demographic data about the respondents and their industries, such as: type of industry, job title, management level, and years of experience in job, age of firm, number of workers employed, gender, and educational background. The target population will consist of employees that use their mobile devices to perform functions or tasks related to their work. The questionnaire was revised by IS professionals. A pilot study will be conducted to test the reliability of the instrument.

Data Analysis

Results will be summarized using descriptive statistics, reliability analysis, and multivariate analysis to test the relationships using SPSS. Factor analysis will be used to describe each component, measure the total variance explained by each variable, and the adequacy of the sample. Factor analysis is a technique used to determine how well the variables related to each other and how its form sets or factors (Salkind, 2004; Valentín, 2014). Multivariate analysis using structural equation model of Partial Least Squares will be used to analyze unobservable variables or constructs. (Hair, Hult, Ringle, & Sarstedt, 2016).

CONCLUSIONS AND RECOMMENDATIONS

The results of our research will offer a useful model to examine how employees' behavior can influence organizations' information security policies. There are many dangers and threats related to the incorporation of mobile technologies in enterprises. These threats can compromise the confidentiality, integrity, and availability of IS. However, although organizations are aware of the threats that may arise when using mobile devices, they have incorporated this technology in order to take full advantage of accessibility that allow breaking the barriers of time and geographical space. The results of this study will reduce the gap in our understanding of users' behavior in the context of mobile devices in the work environment. The results will also serve as a vehicle to improve security policies in the organizations and help to develop employees' awareness of security policies.

References

Abadi, H. R. D., Kabiry, N., & Forghani, M. H. (2013). Factors affecting Isfahanian mobile banking adoption based on the technology acceptance model. *International Journal of Academic Research in Business and Social Sciences, 3*(5), 611.

Alexandrou, A., & Chen, L. C. (2014). The security risk perception model for the adoption of mobile devices in the healthcare industry. Proquest

Bajikar, S. (2002). Trusted platform module (TPM) based security on notebook pcs-white paper. *Mobile Platforms Group, Intel Corporation*.

Boer, H. & Seydel, E.R. (1996). Protection motivation theory. In: Conner, M. & Norman, P. (Eds), Predicting Health Behaviour: Research and Practice with Social Cognition Models (pp. 95/120). Buckingham: Open University Press.

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

Camacho-Martínez, A., Ferrer-Moreno, E., Rivera, I., & Ojeda, A. (2014, November). Social networks in the era of mobile devices: The simulation of privacy. *International Journal of Research in Computer Application & Management*, *4*(11), 1-4.

Castells, M. 2011. The rise of the network society: The information age: Economy, society, and culture, 1. Wiley

Consumer Statistics. (2010). Global Data Backup Survey Results, 2010. Retrieved from: http://www.consumerstatistics

Duggan, M. (2015). *Mobile messaging and social media 2015*. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/

Duggan, M., & Brenner, J. (2013). *The demographics of social media users, 14*. Washington, DC: Pew Research Center's Internet & American Life Project.

El Maliki, T., & Seigneur, J. M. (2013). Security adaptation based on autonomic and trust systems for ubiquitous mobile network and green IT. *In UBICOMM 2013*: The Seventh International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (pp. 152-158).

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T. & Wood, P. (2011). *Symantec Internet Security Threat Report Trends for 2010, 16*(20).

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in Bring Your Own Device environments. *Journal of Information Privacy and Security, 11*(1), 38-54.

Harris, M., & Patten, K. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125.

Hair, Jr., J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM), (2nd)*. Sage Publications.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2014). *Metodología de la investigación,* (6th ed.). Mc Graw Hill. México.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organization culture. *Decision Sciences Journal*, *43*(4).

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, *34*(3).

Kim, D. J., & Hwang, Y. (2012). A study of mobile internet user's service quality perceptions from a user's utilitarian and hedonic value tendency perspectives. *Information Systems Frontiers, 14*(2), 409-421.

Lee, D., & Won, D. (2012). A Study on Security Management Service System for Wireless Network Environment. *Applied Mathematics & Information Sciences, 6*, 209-220.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Macía, N., Lanfranco, E. F., Venosa, P., & Sabolansky, A. J. (2015). Uso de dispositivos móviles y BYOD: Su impacto en la seguridad. In XVII Workshop de Investigadores en Ciencias de la Computación (Salta, 2015).

Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, *6*(1), 97-104.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.

Mohite, S. (2014). A Survey on mobile malware: War without end. *International Journal of Computer Science and Business Informatics*, *9*(1).

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information Security Behavior: Towards Multi-Stage Models.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *In System Sciences*. HICSS 2007. 40th Annual Hawaii International Conference on (pp. 156b-156b). IEEE.

Posey, C., Roberts, T., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems, Forthcoming.

Rahman, A., & Sharma, K. (2012). Fourth generation of mobile communication network: evolution, prospects, objectives, challenges and security. *International Journal of Research in IT & Management*, *2*(2).

Stanton, J. M., Mastrangelo, P., Stam, K. R., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. *In AMCIS* (p. 175).

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *Journal of Electronic Commerce Research*, *14*(2), 183-200.

Symantec Report (2015). *Internet Security Threat Report 2015, 20*. Retrieved http://www.symantec.com/security_response/publications/

Valentin, A. (2014). Factores que influyen en la adopción de las tecnologías de código abierto en las instituciones de educación superior. ProQuest Dissertations & Theses Global. (1564230224). Retrieved from http://search.proquest.com/docview/

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101.

Yang, H., Ricciato, F., Lu, S., & Zhang, L. (2006). Securing a wireless world. *Proceedings of the IEEE*, 94(2), 442-454.

Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013). Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior. In Social Computing (SocialCom), 2013 International Conference on (pp. 411-416). IEEE.

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology*. New York: Guilford Press.

Salkind, N. J. (2004). An introduction to theories of human development. Sage Publications.