8-6-2011

INFORMATION SECURITY BEHAVIOR: FACTORS AND RESEARCH DIRECTIONS

Sherly Abraham
University at Albany, abrahamsherly@gmail.com

INFORMATION SECURITY BEHAVIOR: FACTORS AND RESEARCH DIRECTIONS

Sherly Abraham
College of Computing & Information
University at Albany
abrahamsherly@gmail.com

ABSTRACT

This study presents an extensive literature review on information security behavior in the context of factors affecting security behavior of users in organizational environments. The study critically analyzes articles in the information security behavior and brings forward 18 themes for security practitioners and researchers to consider in implementing information security initiatives. The findings of this review can be used by researchers and practitioners as a roadmap to guide further research in information security behavior. Also, the various factors identified in this paper can be used to improve information security programs in organizations.

Keywords

Information security behavior; security policies, management and peer influences, deterrence efforts, self-efficacy, psychological ownership, organizational commitment

INTRODUCTION

Organizational environments present users with numerous choices in using personal computers that might support or deter information security best practices. The lack of awareness among users in regard to security policies and best practices have been identified by security scholars as a major cause of failure (Thoms and Solms 1998; Siponen 2000). Ironically, even though users might be aware of information security policies, they might not comply in various situations (Pahnila, Siponen, and Mahmood 2007; Workman et al. 2008). Therefore, an important facet in building successful security programs involves understanding the behaviors of users that lead to compliance with security policies (Proctor and Byrnes 2002).

In recent years, as the importance of end user security behavior has been recognized, information system researchers and practitioners have attempted to understand this phenomenon from various theoretical viewpoints. Although, this reveals the interdisciplinary nature of information security, it detracts in providing a holistic view of information security behavior. The information system literature has attempted to unpack end user security behavior from a micro perspective, focusing on individual factors such as attitudes, beliefs, and self efficacy. However, there is a need to critically analyze and synthesize this literature from both a micro and a macro perspective. This paper aims to narrow this gap by presenting a comprehensive literature that increases our understanding of the current state of research in information security behavior, and knits together the various fabrics that influence information security behavior of users in organizations.

This literature review addresses the following research question:

What factors influence information security behavior of users' in organizations?

The findings of this review can be used by researchers and practitioners as a roadmap to guide further research in information security behavior of people. Also, the various factors identified in this literature review can be used to improve information security programs in organizations.

Prior studies in the information security domain are broad in nature and provide a general overview of information security research streams (Sipponen and Oinas-Kukkonen 2007; Zafar and Clark 2009) or focus specifically on awareness approaches (Puhakainen 2006). However, these studies have not critically analyzed user behavior aspects such as the factors influencing end user security behavior, challenges in achieving compliance, and the security context used to understand information security behavior of people. Furthermore, there is a need for literature review studies in the information systems domain (Webster and Watson 2002; Levy and Ellis 2006).

The present study is organized as follows: In section two, the author elaborates on the method used to identify relevant literature. In section three, the author critically synthesizes the factors identified in the information system literature that shape information security behavior in organizations. The article concludes by discussing future research directions and limitations in studying end user security behavior in organizations.

IDENTIFYING RELEVANT LITERATURE

In order to understand the breadth of issues studied in regard to user behaviors in information security, the author adopted the approach proposed by Webster and Watson (2002) for identifying relevant literature. First, the author searched for relevant literature in the major information systems journals and then conducted an extensive literature search on end user security behavior in databases. Rather than rely solely on specific journals in a certain domain, the author expanded the search for literature to academic databases such as ACM Digital Library, EBSCO, Elsevier Science Direct, Emerald Library, IEEE/IEE and Springer Link with keyword searches such as: 'information security behavior'; 'information assurance behavior'; 'computer user security'; 'security behavior theories'; and 'human behavior information security'. To further capture research work not contained in these databases, Google Scholar searches with the specified keywords were utilized.

Second, the author reviewed the citations of the articles discovered in the first step for relevant literature. Literature was included if it focused on the end user security behavior. Articles that focused on information security but did not focus on user behavior such as studies of security risk planning, security laws, security investment and so on were not included. Finally, the author utilized Scopus (abstract and citation database) to identify articles that cited some of the key articles and included them if they focused on end user security behavior.

The search resulted in 84 relevant articles including journal articles, conference proceedings and books. The author organized the literature review analysis along the following key issues: research disciplines and theories, factors affecting information security behavior, organizational context, and security technology used to understand security behavior.

FACTORS AFFECTING SECURITY BEHAVIOR OF USERS

In order to systematically organize the factors affecting information security, the author utilized the conceptual model of information security behavior developed by Leach (2003) as shown in figure 1.

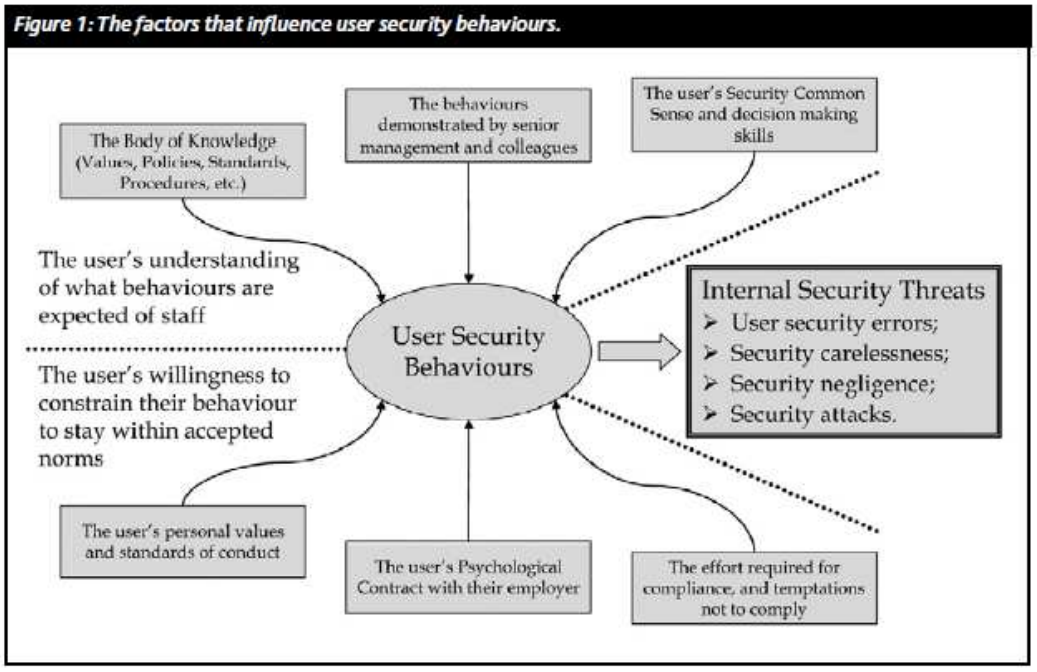

Figure 1. Factors affecting security behavior, adapted from (Leach 2003)

The Body of Knowledge- What Employees are Told

In this section, the author examines what employees are told and, as a result, come to know about security best practices in an organization. Employees are informed about information security through documents, emails, workshops, campaigns, and newsletters. The analysis of the IS literature regarding what employees are told can be categorized according to the following themes: security policies; communication practices of awareness efforts; and contents of awareness efforts.

Security Policies

It is important for organizations to have clear and well-defined security policies (Wood 1995; Baskerville and Siponen, 2002; Parker 1998). Although the need for formal policies is a well-established norm in IS literature, their impact on security behavior has not been promising. A number of studies show that formal codes of ethics have very little or no impact on information security behavior (Frank, Shamir, and Briggs 1991; Harrington 1996). This can be attributed to the dependency of formal policies on individual-level variables and attributes such as: attitudes, knowledge of users, and the communication practices used to relay polices to employees. For example, even though Frank et al. (1991) found no direct association between formal policies and security behavior of users, there were interaction effects between formal policies and user's level of knowledge associated with computers.

Communication practices of security efforts

We know little about how security policies are communicated and how they affect user behavior in organizations. In an effort to review articles on corporate codes of ethics since 1994, Helin and Sandstrom (2007) showed that we still lack knowledge on how codes of ethics are communicated and transformed in an organization. Consistent with their findings, several other scholars have called for the need to further examine how codes of ethics are communicated and interpreted in organizations (Kabay 2002).

Contents of Awareness Efforts

A few studies have analyzed the effects of message framing on security behavior of users (Anderson and Agarwal 2010; Johnston and Warkentein 2010). Johnston and Warkentein (2010) showed that messages that aim to persuade users to comply with policies through the arousal of fear associated with the threat impacted security behavior of users (Johnston and Warkentein, 2010). Contrary to their discovery, Anderson and Agarwal (2010) in an experimental study with home computer users found positive messages that focus on benefits to be more effective than negative messages. This difference can be attributed to the autonomous freedom and choice in using computing resources from homes as opposed to organizational environments. Nevertheless, further research is necessary to draw strong connections on the influence of message framing on security behavior of users.

What they see in Practice in the Organization

In this section, the author examines factors affecting security behavior of users as determined by what employees see in practice around them in the organization. The analysis of the IS literature on what employees see in practice in organizations resulted in the following themes: management and peer influences, deterrence efforts or sanctions, rewards and the level employee participation in security efforts in the organization.

Management and Peer Influences

Management studies can be categorized according to whether they evaluate the competency of managers in security (Loch, Carr, and Warkentin 1992; Straub and Welke 1998; Yeh and Chang 2007) or try to understand perceptions of managers from employee perspectives (Puhakainen 2006; Pahanila 2007). The former has attracted much attention in IS research while the latter remains a less explored area.

The role of managers in spearheading information security is inevitable. Managers need to show employees that they themselves practice security. A recent action research intervention revealed that even though the organization's security policies required them to encrypt email messages, they were not doing so because they were not seeing it practiced in the organization by their peers or managers (Puhakainen 2006). Employees' perception of their managers' expectation to comply with security policies have shown to be empirically significant predictors of employee behaviors (Pahanila et al. 2007). Although managers might think their actions are propagating security behavior, we need to understand whether this aligns with employees' perception. We lack studies that empirically evaluate the effects of management uses of security practices on end user security behavior.

Also, there is strong evidence showing how peer behavior can affect security behavior of employees (Aytes and Connolly 2003; Herath and Rao 2009; Siponen et al. 2010). Peer interactions can result in knowledge transfer (Spears 2006); hence, peers can be a good resource for organizations to build a security culture by providing avenues for employees to socially interact and exchange information.

Deterrence Efforts or Sanctions

A number of studies have explained the effects of deterrence or sanctions from managers' perspectives (Straub 1990; Kankahalli et al., 2003), while other studies have explained the influence of deterrence on security behavior from users perspectives (D'Arcy, Hovav, Galleta 2009). Deterrence severity and certainty can result in reduced computer abuse (Straub 1990). While most studies reveal a positive relationship between deterrence efforts and users security behavior, there have been differences noted between the effects of perceived severity and perceived certainty on security behavior and computer abuse (Herath and Rao, 2009; D'Arcy, el al., 2009).

Rewards

Although a number of scholars conceptually state the need for rewards to encourage and remind employees to follow security best practices (Thomson and Solms 1998; Parker 1998), the few studies that empirically examined the influence of rewards on end user security behavior did not find consistently positive results (Leonard et al. 2004;

Stanton, Stam, Mastrangelo and Jolton 2005). However a recent study that associated rewards with perceived benefit of compliance found that even though rewards did not contribute significantly to comply with security policies it did have a significant impact on users' perceptions of the need to comply with security polices (Bulgurcu et al. 2010) suggesting that rewards can act as motivators for users' to practice security. In summary, even though rewards do not necessarily influence security behavior directly, they could be used as motivators to improve the security behavior of users'.

Employee Participation

Employee participation in the formulation and implementation of security initiatives can influence security behavior positively (Spurling, 1995). IS studies have also addressed user participation from the perspective of user involvement in awareness efforts (Albrechtsen and Hovden 2010) as well as user involvement in the implementation process of security efforts (Spears and Barki 2010).

A recent intervention study (Albrechtsen and Hovden 2010) analyzed the effects of user participation in raising security awareness through an intervention study that involved 100 employees in 6 different workshops that encouraged workshops participants to talk and discuss their opinions on information security. The results demonstrated that user participation produced changes in information security awareness and behavior. Likewise, the effect of user participation in the security risk management process of Sarbanes-Oxley compliance have shown to add value to the organization by raising awareness of security risks and controls (Spears and Barki 2010).

User's Security Common Sense and Decision Making Skills

In this section, the author examines factors affecting security behavior of users in terms of the user's security knowledge. The analysis of the IS literature in this area resulted in two themes: user's knowledge and user's self- efficacy in conducting security procedures.

Users need to have the necessary knowledge to engage in security promoting actions (Thomson and Solms 1998; Aytes and Connolly 2003). The lack of knowledge among users with respect to security best practices can lead to security failures (Luker 1998; Stanton, Stam, Guzman, and Caldera 2003). Analogously, studies have attempted to understand the effects of user's general knowledge of computers in predicting security behavior. Although some studies show the importance of users' knowledge of computer usage to be significant (Frank et al. 1998), other studies did not find computer literacy to be important in predicting security behavior (Loch and Conger 1996); thus we cannot draw strong conclusions on the effects of users' knowledge of computers on their security behavior.

A considerable body of literature provides evidence on the role of self-efficacy in shaping security behavior (Dinev and Hu 2007; Ng et al. 2008; Workman et al. 2008; Rheea et al. 2009; Bulgurcu et al. 2010). Self efficacy is the belief that one has the abilities to perform the courses of actions required to administer potential tasks. While research has demonstrated the importance of self-efficacy in influencing users' security behavior, we know little about how users' can develop self efficacy towards security practices. We need to understand why some users attain more self-efficacy in security tasks compared to others, and how can we empower users so they can achieve an acceptable level of self-efficacy to promote security behavior. There is a need for IS studies to move from studying self efficacy as being a determinant of security behavior towards developing methods to improve self- efficacy in security.

Users Personal Values and Standard of Conduct

In this section, the author examines factors affecting security behavior of users based on the user's personal values, beliefs and standard of conduct. The analysis of the literature on user's personal values and standards of conduct revealed themes such as attitudes and beliefs.

A number of studies recognized the effects of users' attitudes in shaping security behavior (Thomson and Solms 1998) and some have further examined the antecedents of attitudes (Loch and Cogner 1996; Leonard et al. 2004; Bulgurcu et al. 2010). While one school of thought contends that attitudes impact security awareness (Leonard

et al. 2004; Bulgurcu et al. 2010); the other school of thought asserts that influencing personal values and belief systems of users might not be feasible in organizations, especially in the short term (Leach 2003). Additionally, gender and age have been shown to have varying influences on security behavior of people (Loch and Cogner 1996; Gattiker and Kelley 1999; Leonard et al. 2004).

Clearly, organizations need to employ an ongoing multipronged approach that aims to tap in to the attitudes, values, and beliefs of users so changes can occur in the long term as well as focus on short-term efforts that raise basic awareness of users. Also, organizations could benefit by understanding the demographic characteristics of their employees and catering awareness efforts based on these characteristics.

Users Sense of Obligation

The next macro facet affecting security behavior consists of the unwritten reciprocal agreement existing between the employee and employer to act in each other interests. The author's analysis of the literature on the user's sense of obligation revealed themes such as: psychological ownership, organizational commitment, trust and procedural justice.

The concept of psychological ownership (connection that people feel towards objects and concepts) has been utilized in studying home computer security behavior (Anderson and Agarwal 2010). The study shows that perceptions of psychological ownership held by users influence security behaviors towards their personal computers at home. In view of the fact that people can draw territorial connections to their organizations (Brown, Lawrence, and Robinson 2005), understanding the effects of psychological ownership on employee security behavior can be beneficial to organizations.

In the same vein, organizational commitment contributes to the degree of alliance between the employer and employee in terms of employee satisfaction and psychological attachment with the organization. People with high organizational commitment are less likely to engage in activities that put the organization at risk (Stanton et al. 2003). A key component in boosting the organizational commitment of employees is trust (Lee et al. 2004). Employees need to feel they are trusted by their employers (Luker 1990) and perceive a sense of fairness also known as procedural justice (Workman et al. 2008) in administration. A misfit in these areas could result in the employees holding resentment towards the organization that would cause them to punish the organization, neglect security policies, or hurt the reputation of the organization.

The Difficulty in Complying

Finally, the author examines the influence of the degree to which organizations make it easy for their employees to adhere to security standards and procedures. The analysis of the literature on the difficulty of complying revealed two themes: ease of use and effectiveness of security technologies.

Although the information systems literature, in general, shows that perceived ease of use is an important determinant of technology usage (Davis 1989), and managers think that perceived ease of use might be a factor in security behavior (Cannoy and Salam 2010), IS security studies in particular, have consistently shown perceived ease of use to be a non-significant determinant of security behavior (Dinev and Hu 2007; Lee and Kozar 2008). For example, perceived ease of use in the context of anti-spyware technologies have show no significant results (Dinev and Hu 2007; Younghwa and Kozar 2008). This finding was also consistent in the context of email-related security behavior of end users' (Ng et al. 2008). This can be explained by the specificity of the security technology (Dinev and Hu 2007) and the simplicity and user friendliness in installing security technologies such as spyware (Younghwa and Kozar 2008).

The table below (Table 1) summarizes the literature review based on the major factors identified in the Leach (2003) model grouped by the themes identified in the literature review. A few of the key articles from the literature review are listed in the table. Some of the key findings from the literature review are summarized in the table. The literature review discussion identified in the table is based on the entire literature review conducted and not specific to the research articles identified in the table.

Factors Affecting Information Security Behavior identified in Literature	**Research Articles**	**Literature Review Discussion**
The Body of Knowledge 1. Security Policies 2. Communication Practices 3. Content of Awareness Efforts	Anderson & Agarwal, 2010 Frank et al. 1991 Helin & Sandstrom 2007 Johnston & Warkentin, 2010	**Organizations cannot solely rely on existence of formal code of ethics **IS literature scant on communicative practices of security policies **Further research needed in examining the effects of contents and framing of policies
What they see in Practice in the Organization 1. Management Influences 2. Peer Influences 3. Detterance Efforts 4. Rewards 5. Employee Participation	Albrechtsen, & Hovden 2010 Aytes & Connolly, 2003 Herath & Rao, 2009 Kankanhalli, 2003 Spears & Barki, 2010 Stanton et al. 2005 Straub & Welke,1998	**Managers need to show employees they practice security **Studies show that employees look to their peers in building security practices **Broad acceptance for deterrence theories and efforts ** Studies have shown positive results of user participation and security behavior ** Empirical studies show that rewards do not directly influence security behavior
User's Security Common Sense and Decesion Making Skills 1. User's Knowledge 2. Self-Efficacy	Aytes & Connolly 2003 Dinev & Hu 2007 Loch & Conger, 1996 Ng et al. 2009 Rheea et al. 2009 Workman et al. 2008	**Self efficacy shown to be an important predictor of security behavior; **Lack of studies in understanding why some users develop more self-efficacy than others and how to develop self-efficacy among users towards security actions

Factors Affecting Information Security behavior (CONT)	**Research Articles**	**Literature Review Discussion**
The User's Personal Values and standard of conduct 1. Attitudes 2. Beliefs	Bulgurcu et al. 2010 Gattiker & Kelley, 1999 Leonard et al. 2004 Loch & Cogner 1996	**Attitudes have shown to have a strong influence on security behavior
The user's psychological contract with employer 1. Psychological ownership 2. Organizational commitment 3. Trust 4. Procedural justice	Anderson & Agarwal, 2010 Luker 1990 Stanton et al. 2003 Workman et al. 2008	**Employees perception of sense of fairness in the organization influences security behavior **Providing advance notice of monitoring employee activities can assist in demystifying the negative effects of loss of trust in monitoring employee activities **Strong connection between organizational commitment and security behavior
Effort required for compliance and temptation not to comply 1. Ease of use 2. Effectiveness of security technology	Cannoy & Salam 2010; Dinev & Hu 2007; Herath & Rao 2009	**IS security studies consistently show perceived ease of use to be insignificant in predicting security behavior in the context of anti-spyware technologies **Further research needed in other security contexts

Table1. Summary of factors affecting information security behavior

DISCUSSION AND FUTURE DIRECTIONS

This literature review has summarized the factors identified in the information systems literature to explain information security behavior of people in organizations. A large number of the studies have focused on explaining how to prevent deviant acts in organization and how to motivate users to perform security actions. A few studies have also focused on explaining why users fail to follow security policies and the challenges of achieving compliance. Although these approaches have contributed immensely in explaining security user behavior, they have relied heavily on perceptions of users, and perceptions might not necessarily reflect actual behavior (Kraemer, Kruger and Kearney 2006). While some studies have analyzed user logs to monitor actual behavior (Workman et al. 2008), the majority of user security behavior studies have relied on users perceptions to explain security behavior. The inability to observe in real time, the behavior of users is a major limitation to studies that explained security behavior of people based on users perceptions of security.

The author examined 52 studies that employed empirical methodologies to shed light on security behavior. Although there was a range of types of organizations studied including health care (Cannoy and Salam 2010), higher education (Rhee et al. 2009) and manufacturing (Herath and Rao, 2010) organizations, there were a high concentration of articles studying end user security behavior in higher educational environments. Even though higher education environments are good outlets to find users from varying backgrounds, the security policies tend to focus on an open network access policy as opposed to other restricted environments found in call centers, health care industries, and so on. Therefore, it would add value to the body of knowledge regarding security behavior to conduct further empirical investigations in restricted environments such as government agencies, call centers, and health care organizations to capture differences in security behavior of users.

Also, while we see that a few studies have attempted to narrow the security context to email usage (Loch and Cogner 1996) and Spyware security practices (Johnston and Warkentin 2010), the majority of studies examined the general security compliance attitudes and/or behaviors of users. This approach may be too broad to clearly understand security behavior of users given the range of security policies governing organizational computing use. Organizational security policies vary from email and webpage usage policies to physical security policies. People could develop varying security behaviors to the different policies. For example, an employee who pays careful attention when opening email messages might not necessarily value locking doors. Consequently, the author brings forward the need for studies that analyze specific behaviors towards specific policies.

In addition to the contents of policies, the communication practices used to relay policies can influence how users comprehend the policies. Organizations utilize several communication practices ranging from face-to- face to electronic methods to train employees on security best practices. Similarly, security policies are relayed to employees in the forms of emails, webpages, or newsletters. However, we know little about the effects of these communication practices and media choices on the information security behavior of users. There is evidence in the organization science literature showing how face- to- face and online communication methods could vary in terms of trust, clarity, reliability and relationship among users (Griffith and Northcraft 1994; Walther 1995; Fiol and O'Connor 2005). Theories such as task- technology fit postulate that technology is more likely to be perceived as beneficial to the user if the capabilities of the technology match the tasks the user must perform. Accordingly, the application of theories such as task-technology fit would help in deciphering this facet of organizational security. Security behavior studies would also benefit by focusing on the influence of security procedures and processes on users' behavior by drawing on organizational development and communication theories.

Another factor that has recently gained momentum but requires further research is the influence of organizational commitment of the employee on security behavior. It is crucial for organizations to ensure employees have strong organizational ties, especially among employees who handle highly sensitive information. While the few studies that have explained the effects of this phenomenon have pointed to positive relationships between organizational commitment and security behavior of users, we lack evidence regarding the influence of trust on security behavior. The issue of trust would be significant in organizations that monitor employee electronic activities. The challenge for organizations lies in influencing employees to perceive they are trusted and simultaneously monitor employee computing activities.

A related but distinct, factor is the influence of user participation in security initiatives in organizations on security behavior. Contrary to the belief that users are a threat to security, this ideology portrays users as a valuable resource in building quality security efforts. As discussed earlier in this literature review, studies have collectively pointed to benefits of user participation in security implementation activities and security training activities. However, studies have failed to explain some of the challenges that come with employee participation in security efforts. Although studies have shown user participation in awareness efforts to be promising, its feasibility in larger organizations is questionable due to resource constraints. In addition, information security entails protecting areas in an organization that might need to remain hidden from employees, further complicating issues associated with user participation in security initiatives. Accordingly, participative activities in security initiatives might need to be segmented based on the role of employees in the organization and the type of security efforts.

Finally, information security is a complex phenomenon and its repercussions extend beyond individuals to groups and teams in organizations. While numerous studies have addressed end user security behavior, we lack studies that examine security group behavior. Individuals can act differently in group environments (Kabay 2002),

especially when groups are responsible for ensuring security. We identify the need for studies that examine the dynamics of security behavior in group and team settings in organizations.

CONCLUSION

Information security behavior of users is an evolving research stream and plays a major role in shaping the information security state of an organization. The role of users in the effectiveness of information security programs is inevitable and warrants continued research as new threats and exploits continue to be discovered every day. The study provides a comprehensive overview of the factors affecting information security behavior of users' in organizations. Finally the review discusses challenges in studying security behavior of users' and brings forward future research directions.

REFERENCES

Albrechtsen, E. & Hovden, J. (2010). "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security* 29(4) pp 432-445

Anderson, C. & Agarwal, R. (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3) pp 613-643

Aytes, K., & Connolly T,. (2003). " A research Model for Investigating Human Behavior Related to Computer Security," *Proceedings of the Ninth Americas Conference on Information Systems*: 2027-2031

Baskerville, R. & Siponen, M.T. (2002): An Information Security Meta-policy for Emergent Organizations. *Journal of Logistics Information Management*, special issue on Information Security, Vol. 5-6, pp. 337-346.

Brown, G., Lawrence, T., & Robinson, S. (2005). "Territoriality in Organizations," *Academy of Management Review* 30(3) pp 577-594

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). "Information Security Policy Complaince: An Empirical Study of Rationality-Based Beleifs and Information Security Awareness," *MIS Quartely* (34:3), pp 523-548

Cannoy, S. , & Salam., A. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*. 53(3), 126-131.

D'Arcy, J. , Hovav, A., & Galletta, D. (2009). ""User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. A Detterance Approach,"" *Information Systems Research* (20:1), pp 79-98

Davis, F. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* 13(3) pp 319-340

Dinev, T. & Q, Hu. (2007). "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protecting Information Technologies," *Journal of the Association for Information Systems* (8) 7, pp. 386-408

Fiol, C,M. & O'Connor, E. "Identification in Face-to-Face, Hybrid, and Pure Virtual Teams: Untangling the Contradictions," *Organization Science* (16:1), pp 19-32

Frank, J., Shamir, B., Briggs, W. (1991). "Security-related behavior of PC users' in Organizations," *Information & Management* (21:3), pp127-135

Gattiker, U., & Kelley, U. (1999). "Morality and Computers: Attitudes and Differences in Judgments," *Information Systems Research* 10 (3) 233-254

Griffith, T., & Northcraft, G. (1994). "Distinguishing Between the Forest and the Trees: Media, Features, and Methodology in Electronic Communication Research," *Organization Science* (5:2), pp 272-285

Harrington,S. (1996). ""The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions,"" *MISQ Quarterly* (20:3), pp 257-278.

Helin, S. and J. Sandström (2007). "An inquiry into the study of corporate codes of ethics." *Journal of Business*

Ethics 75(3): 253-271.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness . *Decision Support Systems*, 47(2), 154-165.

Johnston, A., & Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kabay ME (2002) Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) *Computer Security Handbook*, 4th edition. John Wiley & Sons, Inc., USA, 32.1-32.16.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. & Wei, K.-K., (2003). An integrative study of information systems security effectiveness, *International Journal of Information Management*, v23, pp. 139-154.

Kraemer,Kruger, H., & Kearney, W. (2006). ""A prototype for assessing information security awareness, *Computers & Security* 25 (4) pp 289-296

Leach, J. (2003). Improving User Security Behavior. *Computers & Security*. 22(8).

Lee, Y. & Kozar, K. (2008) "An empirical investigation of anti-spyware software adoption: A multitheoretical perspective, *Information and Management*, 45(2) pp 109-119

Leonard, L.N.K., Cronan, T.P., Kreie, J. (2004), ""What are influences of ethical behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics?"", *Information & Management*, Vol. 42 No.1, pp.143-58.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support ofinformation systems research. *Informing Science Journal*, 9, 181-212. Retrieved from http://inform.nu/Articles/Vol9/V9p181-212Levy99.pdf

Loch, K.D., Carr, H.H. and Warkentin, M.E., 1992. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly* 16 2, pp. 173–186

Loch, K.D., Conger, S. (1996), "Evaluating ethical decision making and computer use", *Communications of the ACM,* Vol. 39 No.7, pp.74-83.

Luker, N. W. (1990) "Do You Trust Your Employees?" *Security Management* (34:9), pp. 127-130

Thomson. M.E, and Von Solms, R. (1998) Information security awareness: educating your users effectively, *Information Management & Computer Security*, Vol. 6 (4), pp.167 – 173

Ng, B.Y., Kankanhalli, A., Xu, Y.C. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No.4, pp.815-25

Pahnila, S., Siponen, M., Mahmood, A. (2007). *Proceedings of the 40th Hawaii International Conference on System Science*s. IEEE Computer Society Press, Big Island: Hawaii

Parker, D. B., (1998), Fighting Computer Crime - A New Framework for Protecting Information. *Wiley Computer Publishing*. USA.

Proctor PE & Byrnes FC (2002) The Secured Enterprise: Protecting Your Information Assets. *Prentice Hall*, Upper Saddle River, USA.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness. *Unpublished doctoral dissertation*, University of Oulu, Oulu, Finland.

Rheea, H. , Kim, C., Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior . *Computers & Security*, 28(8)

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, *MIS Quarterly* (34:3), pp 487-502.

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database*, 38 (1).

Siponen, M., "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management & Computer Security,* 8,1, 2000, 31–41

Spears, J. & Barki, H. (2010). User Participation in Information Systems Security Risk Management, *MIS Quarterly* (34:3), pp 503-522

Spears, J. (2006). "The effects of user participation in identifying information security risk in business processes, *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research* pg 351-352

Spurling P (1995), Promoting security awareness and commitment. *Information Management & Computer Security* 3(2): 20-26.

Stanton, J. M., Stam, K. R., Guzman, I., & Caldera, C. (2003, October). Examining the linkage between organizational commitment and information security. *Proceedings of the IEEE Systems, Man, and Cybernetics Conference*, Washington, DC

Stanton, M.J , Stam, R K, Mastrangelo, P and Jolton, J. (2005), Analysis of End User Security Behavior. *Computers & Security*. 24, pp 124-133

Straub, D. W., Jr. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255-276

Straub, D.W., and Welke, R.J. (1998), "Coping with systems risks: security planning models for management decision making", *Management Information Systems Quarterly*, 22 (4), 441-469

Walther, J. (1995). "Relational Aspects of Computer-mediated Communication: Experimental Observations over Time," *Organization Science* (6:2), pp186-203

Webster, J., and Watson, R. (2002). " Analyzing the Past to Prepare for the Future: Writing A Literature Review, " *MIS Quarterly* (26:2), pp

Wood, C.C. (1995), Writing InfoSec policies, *Computer and Security*, Vol. 14 No. 8, pp. 667-74.

Workman, M., Bommer, W.H., Straub, D. (2008), Security lapses and the omission of information security measures: an empirical test of the threat control model, *Journal of Computers in Human Behavior*, Vol. 24 No.6, pp.2799-816.

Yeh, Q., & Chang, A., (2007). Threats and countermeasures for information system security: A cross-industry study, *Information & Management* 44(5) pp 480-491

Zafar, H., & Clark, J. (2009). Current State of Information Security Research in IS. *Communications of the Association for Information Systems*, 24 (34).