A Thematic Review of User Compliance with Information Security Policies Literature

David Sikolia
Ph.D. Candidate, Department of Management Science and Information Systems, Oklahoma State University, David.Sikolia@Okstate.edu

A THEMATIC REVIEW OF USER COMPLIANCE WITH INFORMATION SECURITY POLICIES LITERATURE

(Briefing Paper/Presentation)

David Sikolia
Ph.D. Candidate
Department of Management Science and Information Systems
Oklahoma State University
david.sikolia@okstate.edu

ABSTRACT

The adoption of computer and internet technology has greatly improved the way businesses operate. However the risk to the confidentiality, integrity and availability of organizational data and systems has greatly increased too. Information security is an ever present concern for all organizations. Financial estimates of the impact of security breaches to information and technology resources range from hundreds of billions to over one trillion dollars each year worldwide (D'Arcy et al., 2011b). Organizations have therefore developed a combination of technical, administrative, and physical controls to reduce this risk (D'Arcy et al., 2011a). Administrative measures include the development of information security policies, which are statements of the roles and responsibilities of the employee to safeguard the information technology resources of their organizations (Bulgurcu et al., 2010). Information security policy provisions include guidelines to employees on what they should do when interacting with information systems so as to secure the data and technology resources of their respective organizations.

Unfortunately, cases of employee intentional and non-intentional non-compliance with information security policies have been documented, with some security experts concluding employees are the weakest link in information security defenses (Aurigemma et al., 2012). Although popular media tends to headline the exploits of hackers or crackers, evidence suggests that a majority information security incidents occur as a result of trusted employees' actions (Hu et al., 2012; Karjalainen et al., 2011). Increasingly complex viruses, worms, Trojans, rootkits, and distributed botnet attacks are mounted by criminal gangs and sometimes foreign governments but the greatest threat of all is the insider threat, the trusted employee (Ifinedo, 2012; Warkentin et al., 2011). It has been claimed that over half of all information systems security breaches occur because employees do not comply with information security policies (Siponen et al., 2010b). Other reports indicate that 50% - 75% of security incidents originate form with the organization, perpetrated by the trusted employee (D'Arcy et al., 2009). However, it must be pointed out that not all violations are by malicious employees. Some violations might be accidental, others violations might be self-benefiting but without malicious intent. Nevertheless, regardless of the motivation, the end result is the same; rules are broken and possibly causing damage or security risk (Guo et al., 2011).

For over two decades, the information systems research community, starting with Straub (Straub, 1990) has published a sizable body of research on user compliance with information security policies. This body of research has been divided into three categories: (1) conceptual principles or studies without theoretical basis (2) theoretical models without empirical support; and (3) empirical support grounded upon theories (Pahnilaa et al., 2007). These theories were borrowed from reference disciplines such as criminology, economics and psychology.

Example theoretical lens used include general deterrence theory (D'Arcy et al., 2009; Herath et al., 2009b; Pahnilaa et al., 2007; Siponen et al., 2010b), protection motivation theory (Herath et al., 2009b; LaRose et al., 2008; Lee et al., 2009; Pahnilaa et al., 2007; Workman et al., 2008), theory of planned

behavior (Bulgurcu et al., 2010; Herath et al., 2009a), rational choice theory (Bulgurcu et al., 2010), social cognitive theory (Rhee et al., 2009), technology acceptance model (Cynthia et al., 2010; Yajiong et al., 2011), theory of reasoned action (Siponen et al., 2010b), innovation diffusion theory (Siponen et al., 2010a), neutralization theory (Siponen et al., 2010b) and justice theory (Yajiong et al., 2011) amongst others. Of these theoretical lenses, deterrence theory has been used most but the findings have been mixed (D'Arcy et al., 2011a).

The goal of this study is to build upon the body of knowledge on user compliance with information security policies over the last two decades by reviewing previous work and identifying themes or concepts that are antecedents for this behavior. A review of relevant literature is essential for any academic study (Webster et al, 2002), helping researchers identify any gaps that may exist in the body of knowledge. Literature reviews can be written by senior scholars who have published many papers in a given stream of research or by junior scholars who have completed a literature review prior to embarking on a research project such as a dissertation (Webster et al., 2002).

Example literature review papers published in MIS quarterly over the last 30 years include management of information systems personnel (Bartol et al., 1982), knowledge management and knowledge management systems (Alavi et al., 2001), cognitive-affective model of organizational communication (Te'eni, 2001), the resource based view and information systems research (Wade et al., 2004), IT-dependent strategic initiatives and sustained competitive advantage (Piccoli et al., 2005), culture in information systems research (Leidner et al., 2006), Privacy in the digital age (Bélanger et al., 2011; Smith et al., 2011) and Absorptive capacity in information systems research (Roberts et al., 2012).

This study will help us understand the existing body of knowledge on user compliance with information security policies and any gaps that may exist. It will also help us place any future endeavors on this topic in the context of existing work (Levy et al., 2006). This will be accomplished through a systematic search of quality literature on this topic (Ellis et al., 2009), followed by a concept-centric review of the gathered material (Webster et al., 2002). The final outcome will be a model (Webster et al., 2002) to guide future research on user compliance with information security policies.

REFERENCES

Alavi, M., and Leidner, D. E. (2001). Review: knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, *25*(1), 107-136.

Aurigemma, S., and Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *45th Hawaii International Conference on Systems Sciences, IEEE Computer Society*, Hawaii, 3248-3257.

Bartol, K. M., and Martin, D. C. (1982). Managing information systems personnel: A Review of the literature and managerial implications. *MIS Quarterly*, *6*(4), 49-70.

Bélanger, F., and Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-A1036.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly 34*(3), 523-A527.

Cynthia, M. J., Richard, V. M., and Leila, H. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Journal of International Technology and Information Management*, *19*(2), 43-II.

D'Arcy, J., and Herath, T. (2011a). A review and analysis of deterrence theory in the IS literature: making sense of disparate findings. *European Journal of Information Systems*, *20*, 643-658.

D'Arcy, J., and Herath, T. (2011b). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

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

Ellis, T. J., and Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, *6*, 323 - 337.

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

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

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

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences Journal*, *43*(4), 615-659.

Ifinedo, P. (2012). Understanding information security systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. *Computers & Security*, *31*, 83-85.

Karjalainen, M., and Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) Security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518-555.

LaRose, R., Rifon, N. J., and Enbody, R. (2008). Promoting Personal responibility for internet safety. *Communications of the ACM*, *51*(3), 71-76.

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

Leidner, D. E., and Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *30*(2), 357-399.

Levy, Y., and Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, *9*, 181-212.

Pahnilaa, S., Siponena, M., and Mahmoodb, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE Computer Society*, Hawaii.

Piccoli, G., and Ives, B. (2005). IT-dependent strategic initiatives and sustained competitive advantage: a review and synthesis of the literature. *MIS Quarterly*, *29*(4), 747-776.

Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*, 816 - 826.

Roberts, N., Galluch, P. S., Dinger, M., and Grover, V. (2012). Absorptive capacity and information systems research: review, synthesis, and directions for future research. *MIS Quarterly*, *36*(2), 625-A626.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010a). Compliance with Information security policies: An Empirical investigation. *IEEE Computer*, 64 - 71.

Siponen, M., and Vance, A. (2020b). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-A412.

Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 980-A927.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Te'eni, D. (2001). Review: a cognitive-affective model of organizational communication for designing it. *MIS Quarterly*, *25*(2), 251-312.

Wade, M., and Hulland, J. (2004). The resource-based view and information systems research: review, extension, and suggestions for future research. *MIS Quarterly*, *28*(1), 107-142.

Warkentin, M., and Willison, R. (2011). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*, 101-105.

Webster, J., and Watson, R. T. (2002). Analyzing the past to prepare the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii-xxiii.

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

Yajiong, X., Huigang, L., and Liansheng, W. (2011). Punishment, justice, and compliance in mandatory IT Settings. *Information Systems Research*, *22(*2), 400-414.