5-15-2014

A Theory of Employee Compliance with Information Security

David Sikolia
dsikoli@ilstu.edu, dsikoli@ilstu.edu

Marlys Mason
Oklahoma State University, M.Mason@okstate.edu

David Biros
Oklahoma State University, david.biros@okstate.edu

Mark Weiser
Oklahoma State University, weiser@okstate.edu

A THEORY OF EMPLOYEE COMPLIANCE WITH INFORMATION SECURITY

David Sikolia
Illinois State University
dsikoli@ilstu.edu

Marlys Mason
Oklahoma State University
M.Mason@okstate.edu

David Biros
Oklahoma State University
David.Biros@okstate.edu

Mark Weiser
Oklahoma State University
weiser@okstate.edu

ABSTRACT

User non-compliance with information security policies in organizations due to negligence or ignorance is reported as a key data security problem for organizations. Research on employee violation of information security policies has focused on non-compliance due to poor training, low employee motivation, weak effective commitment, or individual oversight. However, the findings from some of the studies are contradictory. Furthermore, no parsimonious theory explains nor predicts employee compliance with information security policies. This study addresses this problem by building a theoretical model grounded in data using grounded theory methodology. The findings indicate organizations need to create a supportive organizational environment. These measures will impact individual employee's perception. Information technology plays a moderating role between organization practices and the individual cognitive factors. These cognitive factors will in turn have an effect on the individual employees' compliance with the information security policies.

Keywords

Information Security Policies, Compliance, Grounded Theory Methodology.

INTRODUCTION

Information security risks come from many fronts, both external and internal. Technical and non-technical measures have been implemented by organizations to mitigate these risks (Ifinedo 2012; Siponen et al. 2007). In this study, we focus on internal security risks, specifically the behavior of the trusted user or employee of an organization, perceived by some as the weakest link (Warkentin et al. 2009). We seek to understand the factors in an organization that lead to improved employee compliance with information security policies.

While studies on user compliance with information security policies are bountiful, unfortunately our understanding of this phenomena is no better that it was two decades ago. Comparison of the mixed findings is challenging and furthermore we don't have a satisfactory theoretical model to explain and predict this behavior. Evidence from some studies shows that counter-measures deter non-compliance with information security policies, but other studies indicate that such controls have little, if any effect (D'Arcy et al. 2009). Researchers doubt that deterrence based research adequately explains employee non-compliance with information security policies (Lee and Lee 2002). Other researchers have argued that employee non-compliance with information security policies is not best explained by fear of sanctions but rather by neutralization techniques. Neutralization techniques are justifications by which those who commit illegitimate acts temporarily neutralize certain values within themselves which would normally prohibit them from carrying out such acts, such as morality or the obligation to abide by the law (Siponen and Vance 2010b).

Information systems scholars don't have a clear understanding of this particular human behavior as evidenced by the numerous theories that have been applied in seeking to have a better explanation. A better understanding of the 'employee compliance with ISP' phenomenon is of paramount interest to both practitioners and researchers. We hope to contribute to this goal by carrying out a grounded theory study with the following research question:

How do organizational employees understand, interpret and comply with organizational information systems security policies?

Considering the consequences of data and computer systems breaches, we develop a framework for explaining user compliance with organizational security policies.

LITERATURE REVIEW

Research on employee violation of information security policies has focused on non-compliance due to poor training, low employee motivation, weak effective commitment, or individual oversight. Theoretical foundations applied to this phenomenon include deterrence, reasoned action, planned behavior, protection motivation, self-efficacy, individual adoption factors, organizational commitment and other individual cognitive factors(Birks et al. 2013). Three theoretical lenses have been applied most by information security researchers in the study of employee compliance with information security policies. These are deterrence theory, protection motivation theory, and rational choice theory. We discuss these below.

Deterrence Theory

According to deterrence theory, individuals weigh the costs and benefits before engaging in criminal behavior, and choose crime only if it pays. Thus if an individual comes to the conclusion that there is a high probability of being caught and the punishment is severe, then they will not engage in criminal behavior (Siponen et al. 2010; Straub Jr 1990). Based on deterrence theory, Herath and Rao argued that as punishment certainty and punishment severity increases, the level of unacceptable behavior decreases. Thus they proposed that the *severity of penalty* and *certainty of detection* will positively affect the *intention* to comply with organizational information security policies. Their empirical findings suggest that punishment severity has a significant impact on policy compliance but the direction of the relationship was opposite to what they hypothesized. *Detection certainty* was found to have a positive impact on *intention* to comply with information security policies as hypothesized (Herath et al. 2009a). In a separate study but using the same data, they report similar findings (Herath et al. 2009b). In his study, Straub found that *deterrent severity* had greater explanatory power compared to *deterrent certainty* (Straub Jr 1990). Siponen and others found that sanctions have a significant impact on actual compliance with information security policies. In their study, sanctions consisted of *detection probability, severity* and *celerity of legal sanctions* as well as *social pressure* from immediate supervisors, peers and information security staff (Siponen et al. 2007).

Protection Motivation Theory

Protection motivation theory of fear appeals and attitude change postulates that there are three crucial components of fear appeal. These are magnitude of noxiousness of a depicted event, the probability of the events occurrence and the efficacy of a protective response (Rogers 1975). Based on protection motivation theory, Siponen and others proposed that *threat appraisal*, *self-efficacy, and response efficacy* affects employee's intention to comply with information security policies. Their research model explained 22 percent of the variance in the intention to comply with information systems security policies (Siponen et al. 2007). Herath and Rao proposed that *perceived severity of security breach and perceived probability of security breach* will positively influence *security breach concern level*. *Security breach concern level* and *response efficacy* will positively influence *security policy attitude*. *Response cost* will negatively influence *security policy attitude*. *Security policy attitude* will positively influence *security policy compliance intention (Herath et al. 2009a).*

Rational Choice Theory

Rational choice theory proposes that offenders weigh the costs and benefits of engaging in defiant behaviors before deciding to act (Li et al. 2010). Individuals are sensitive to the consequences of their behavior and make rational decisions based on a cost benefit analysis of intended behavior. The decision to act in an offending manner is a function of perceived costs and perceived benefits of the criminal behavior (Hu et al. 2011). Li and others proposed that a *cost-benefit analysis* and *personal norms* will impact internet use policy compliance *intention*. Cost benefit analysis consisted of *perceived risks* (*detection probability, sanction severity, subjective norms and security risks*) and *perceived benefits*. Their full research model explained 35 percent of the variance in internet use policy compliance intention (Li et al. 2010).

In summary, information systems researchers have borrowed multiple theories from multiple disciplines in an attempt to explain user compliance with information security policies.

GROUNDED THEORY METHODOLOGY

Information systems researchers use a variety of research methods to explore phenomena of interest. Some of the main high level research methodologies used include (1) Quantitative-positivist research developed from the natural sciences (Davies 1989; MacKenzie et al. 2011; Pedhazur et al. 1991; Straub et al. 2004; Straub 1989), (2) Design science research (Hevner et al. 2004; March et al. 1995; Nunamaker et al. 1991) and (3) qualitative research developed from the social sciences. Qualitative research includes case study research, action study research, ethnography and grounded theory (Myers 2009).

Grounded theory is appropriate for research if (1) little is known about the phenomenon of interest; (2) development of theory is the required outcome and (3) an inherent process is embedded in the phenomenon of interest and is more likely to be unearthed using grounded theory methods (Birks et al. 2011). Development of theory was the reason grounded theory methodology was found appropriate for this research endeavor.

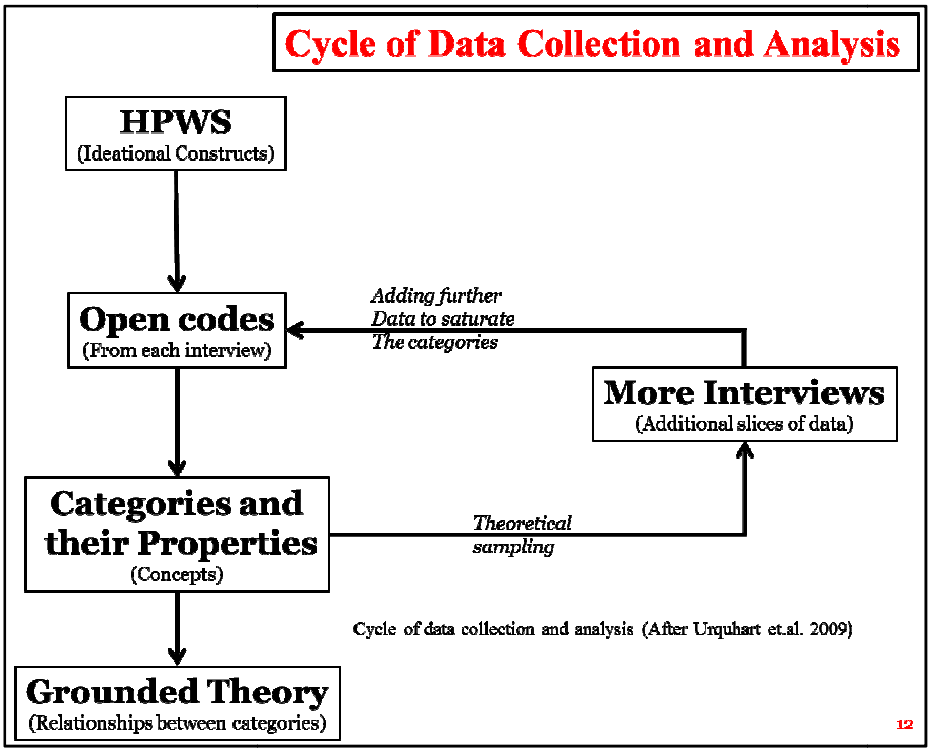

Figure 1. Cycle of Data Collection and Analysis

As depicted in figure 1 above, the process began by identifying ideational or seed constructs, which were used to develop the initial interview questions. The initial interview questions were developed around concepts identified in the High Performance Work Systems (HPWS) (Boxall et al. 2009). Data analysis proceeds from open coding (identifying categories, properties and dimensions) through selective coding (clustering around categories), to theoretical coding (Urquhart 2012).

FINDINGS

The framework for improving employee compliance with information security policies in organizations is depicted in figure 6. The concepts, formed from selectively coding and categorizing the open coding labels, are clustered into four main categories: organization, information technology, employee, and outcomes.

Organization concepts consist of organizational environment, training, deterrence and job design. Employee concepts consist of engagement, knowledge, ramifications and accomplishable. Information technology concepts are access controls and user friendliness. Outcomes consist of compliance with information security policies as well as engagement in the process. The framework represents a cycle with each of the categories impacting all the other categories.

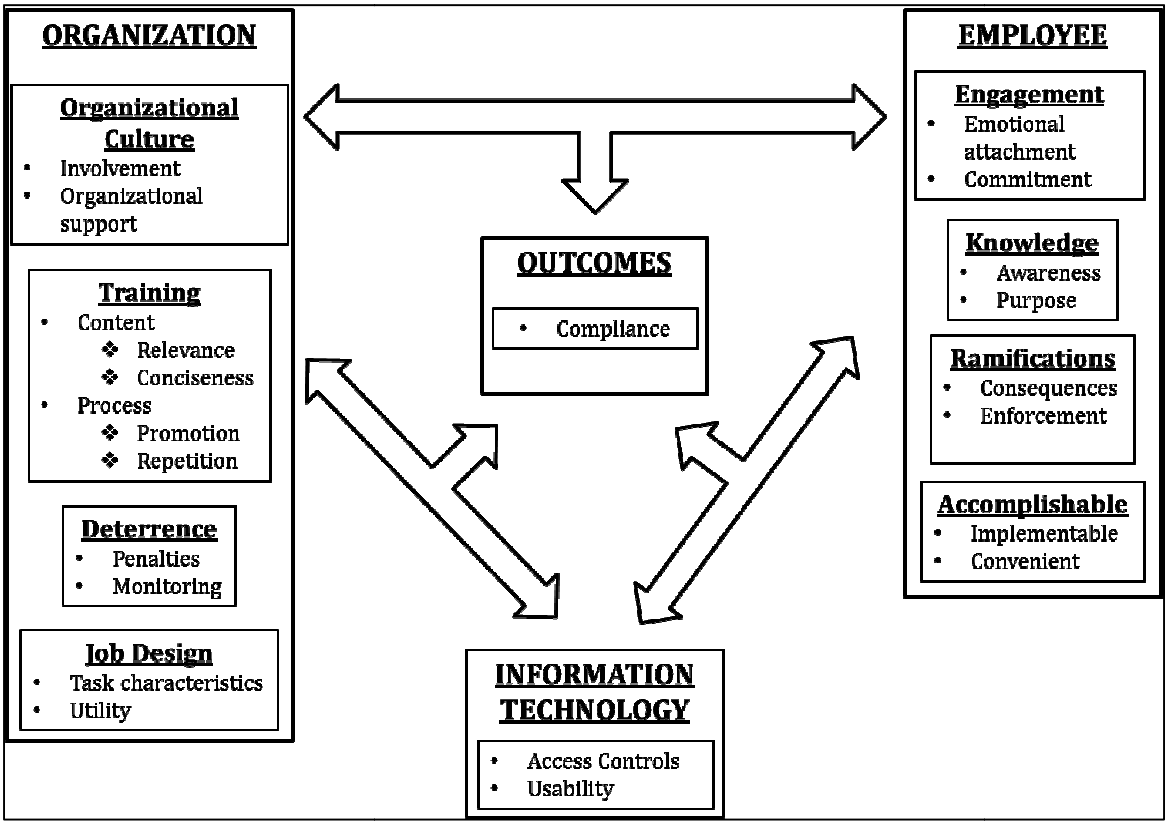

Figure 2. Framework for improving employee compliance with information security policies

CONCLUSION

The goal of this study was to have a better understanding of employee compliance with information security policies. This was the expected outcome of research question for this study:

How do organizational employees understand, interpret and comply with organizational information systems security policies?

Using a qualitative research method, grounded theory methodology, a model to explain this phenomenon was developed. The model shows how an organization can influence its employees to comply with their information security policies. Through creation of the right kind of organizational culture, training, deterrence and job design, the organization can influence employee engagement, knowledge, and perception of ramifications and accomplish ability which in turn will have an effect on compliance with the information security policies. In the next section we discuss the implications of these findings for research and practice.

Contributions to research

Senior scholars in management information systems have called for a 'good theory'(Watson 2001) in information systems and the development of our 'own' theory(Weber 2003). Over the years, the information systems discipline has borrowed a variety of theoretical lenses to explain phenomena in information systems research(Watson 2001). Heeding this call, this dissertation research developed an information systems theory explain user compliance with information security policies. In our study, a theory of explaining is presented with a diagram and words. Even though a very high level of generality is suggested, statements of relationships including causal explanations are given.

Implications for Practice

This research suggests that organizations can improve employee compliance with information security policies through creation of an enabling organizational culture, appropriate training, specifying deterrence measures and the design of work. The organizations should spell out clearly the consequences of non-compliance and how this behavior is determined. The utility and task characteristics of their daily work should be aligned with the information security policies. Furthermore, information technology can be used as a catalyst for ensuring compliance by use of access controls and usability of the technology.

Limitations of the study and future research

There is one main limitation to this study. Although a number of steps were taken to improve the trustworthiness of the study, the credibility could have been improved through triangulation of data. Instead of relying on data collected through semi-structured interviews only, use of data from organizational documents would have raised the trustworthiness of the findings. Getting real organizations and employees to participate in research is a challenge, which explains the use of students in survey samples because it is more convenient. The lack of document data was not for lack of trying but rather reluctance on management in many organizations to open up internal communications to people from outside.

There are four major directions we see future follow-up research taking. The improvement of the theory presented in this study by including document data in further analysis; development of a measurement model; stratification of compliance along management levels; and determining the role of national culture in employee compliance with information security policies.

To conclude, the purpose of this study was to have a better understanding of the cognitive factors that influence employee compliance with information security policies. Towards this goal, we have presented a theoretical framework that hopefully makes a contribution towards our collective understanding of this phenomenon.

REFERENCES

Birks, D. F., Fernandez, W., Levina, N., and Nasirin, S. 2013. "Grounded theory method in information systems research: its nature, diversity and opportunities," *European Journal of Information Systems* (22:1), pp 1 - 8.

Birks, M., and Mills, J. 2011. *Grounded Theory: A practical guide*, (Sage: Thousand Oaks, California.

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

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

Herath, T., and Rao, H. R. 2009b. "Encouraging Information Security Behaviours in Organizations: Role of Penalities, Pressures and Persceived Effectiveness," *Decision Support Systems* (47), pp 154 - 165.

Hevner, A. R., March, S. T., Jinsoo, P., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp 75-105.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp 54 - 60.

Ifinedo, P. 2012. "Understanding information systems security policy complaince: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security* (31), pp 83 - 95.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems* (48:4) Mar, pp 635-645.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in MIS and Behavioural Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp 293 - 334.

March, S. T., and Smith, G. F. 1995. "Design and natural science research on information technology," *Decision Support Systems* (15), pp 251 - 266.

Myers, M. D. 2009. *Qualitative Research in Business & Management*, (Sage Publications: London.

Nunamaker, J. F., Chen, M., and Purdin, T. D. M. 1991. "Systems Development in Information Systems Research," *Journal of Management Information Systems* (7:3), pp 89 - 106.

Pedhazur, E. J., and Schmelkin, L. P. 1991. *Measurement, Design and Analysis: An Integrated Approach*, (Lawrence Erlbaum Associates: Hillsdale, New Jersey.

Rogers, R. W. 1975. "A PROTECTION MOTIVATION THEORY OF FEAR APPEALS AND ATTITUDE CHANGE," *Journal of Psychology* (91:1), p 93.

Siponen, M., Pahnila, S., and Mahmood, A. (eds.) *Employee's Adherence to Information Security Policies: An Empirical Study*. Springer, Boston, 2007.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violiations," *MIS Quarterly* (34:3), pp 487-A412.

Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of AIS* (13:24), pp 380 - 427.

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), pp 147 - 169.

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

Urquhart, K. 2012. *Grounded Theory for Qualitative Research: A Practical Guide*, (

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18), pp 101 - 105.

Watson, R. 2001. "Research in Information Systems: What We Haven't Learned," *MIS Quarterly* (25:4), pp vii - viii.

Weber, R. 2003. "Still Desperately Seeking the IT Artifact," *MIS Quarterly* (27:2), pp 183-183.