Spring 5-19-2016

Motivating Employees to Comply with Information Security Policies

David Sikolia
Illinois State University, david.sikolia@ilstu.edu

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

Motivating Employees to Comply with Information Security Policies

David Sikolia
Illinois State University
David.Sikolia@ilstu.edu

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

ABSTRACT

Employee noncompliance with Information Systems security policies is a serious computer security threat. Employees' extensive knowledge of information systems, their access credentials, and the trust accorded them by their employers make them a potential threat to computer security. The importance of this phenomenon has led to a number of studies on the "insider threat." However, research on employee compliance with IS security policies has focused mainly on the role of extrinsic motivation. Few studies have focused on the role of intrinsic motivation. This study fills this gap by building a theoretical model based on data using grounded theory methodology. Seed concepts from High Performance Work Systems (HPWS) were used to develop initial questions for structured interviews with employees from a variety of institutions. This theoretical model lays a framework for how organizations can intrinsically motivate their employees to comply with organizational information security policies.

Keywords: Information security, Grounded Theory Methodology, Intrinsic Motivation

INTRODUCTION

Information security threats come from many fronts, both external and internal, and organizations have implemented both technical and non-technical measures 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 employees of an organization. We seek to understand the organizational initiatives that lead to improved employee compliance with information security policies. Considering the consequences of data and computer systems breaches, we develop a framework for explaining how employees can be intrinsically motivated to comply with such security policies.

Motivational perspectives have been widely used to understand human behavior in relation to the use of information systems. For example, in their research, Davis et al. (1992) found both intrinsic and extrinsic motivational factors to be key drivers for the adoption of technology in organizations, giving perceived usefulness as an example of extrinsic motivation and enjoyment as an example of intrinsic motivation. Intrinsic motivation leads to behavior that is driven by internal rewards, while extrinsic motivation leads to behavior driven by external rewards. Intrinsic motivation refers to an individuals' engagement in a given behavior for no other reason other than the pleasure or satisfaction derived from it (Davies et al. 1992; Venkatesh 1999). Extrinsic motivation is behavior influenced by the value of outcomes that are distinct from the activity itself, for example promotions, pay raises, and improved job performance (Davies et al. 1992; Venkatesh 1999).

Most studies on the insider threat have focused on employee compliance or non-compliance with information security policies on the basis of extrinsic motivators (Guo et al. 2011). The extrinsic motivators in these studies include perceived certainty, severity, and celerity of punishment; subjective norms; cost-benefit analysis; perceived vulnerability; and sanction effects. These studies have examined this phenomenon using theoretical lenses that include deterrence theory (D'Arcy et al. 2009; Herath and Rao 2009; Hu et al. 2011; Siponen and Iivari 2006; Siponen and Vance 2010; Straub 1990), protection motivation theory (Herath and Rao 2009; Siponen and Iivari 2006), and rational choice theory (Bulgurcu et al. 2010; Li et al. 2010), among others.

A review of the literature reveals that extrinsic motivational factors show mixed or even contradictory results (D'Arcy and Herath 2011). As a research community, in seeking to understand why employees fail to comply with information security policies, we have not explicitly examined the role of intrinsic motivation. This is the gap we hope to fill by exploring the two research questions below.

RQ1: *Why do employees fail to comply with an organization's information security policies?*

RQ2: *How can organizations help their employees to be intrinsically motivated to comply with the organization's information security policies?*

The rest of the study is organized as follows. The next section describes the research methodology, followed by our findings, a discussion of the findings.

RESEARCH METHODOLOGY

This study applies a grounded theory methodology (GTM) because the goal is to generate a theoretical model with explanatory power (Birks and Mills 2011). We began by identifying ideational or seed constructs, which were used to develop initial interview questions. Data analysis proceeded from open coding (identifying categories, properties, and dimensions) through selective coding (clustering around categories), to theoretical coding (Urquhart 2012).

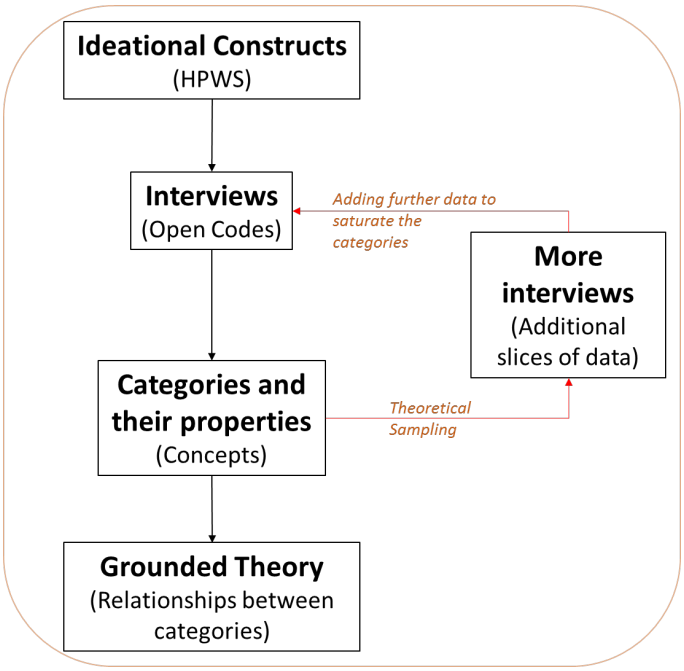

Figure 1. Research process

One characteristic of grounded theory is that there is no prior formulation of hypotheses or expectations to be confirmed by the data. The goal of grounded theory is not to verify or falsify existing theory. However, a researcher cannot approach a study with an empty head; rather he or she must be open minded (Urquhart et al. 2010). A priori specification of constructs can help guide the initial design of the data collection in grounded research, but these constructs are tentative and none is guaranteed a place in the final theory (Eisenhardt 1989).

The seed ideas for how organizations can help their employees be intrinsically motivated to comply with information security policies came from human resources literature. Specifically, we looked at the role of high performance work systems in motivating employees. High performance work systems (HPWS) are defined as "a set of unique but interconnected human resource practices designed to enhance employees' skills and effort" (Messersmith et al. 2011; Patel et al. 2013). The human resource (HR) literature does not include a specific set of HPWS practices but they traditionally included recruitment and selection, pay and compensation plans, information sharing, performance appraisal processes, and training. These HR practices have been linked to factors such as productivity, voluntary turnover, profitability, growth, innovation, and customer service (Messersmith et al. 2011; Patel et al. 2013).

HPWS are associated with higher levels of job satisfaction, commitment to the organization, and psychological empowerment by the employees. This positive attitude has been positively correlated with better organizational citizenship behavior (Messersmith et al. 2011; Patel et al. 2013). Such behavior may include compliance with organizational information security policies. The relationship between organizational HPWS and two individual-level employee attitudes, "job satisfaction" and "affective commitment" were found to be fully mediated by organizational-level concern for employees. HPWS have been found to facilitate a climate of concern for both employees and customers which resulted in employees' engaging in positive behaviors towards customers and fellow employees (Chuang and Liao 2010).

HPWS have been shown to affect employee motivation. Liao et al. (2009) found that two motivational constructs, psychological empowerment and perceived organizational support, have an impact on individual employee performance. Psychological empowerment, which refers to self-motivating mechanisms and consists of meaning, competency, and self-determination, reflects an individual's innate intrinsic task motivation (Liao et al. 2009).

We propose that these HPWS in an organization can lead to improved employee compliance with information systems security policies through psychological empowerment of the employees or the activation of their innate intrinsic motivation (Liao et al. 2009). Therefore, these HPWS practices provided the seed ideas or ideational concepts that informed our first set of interview questions.

Interviews

Data was collected through semi-structured interviews. The interview questions were adjusted during the interview based on the responses to initial questions as well as over the course of the data collection period. The initial interview questions were developed around concepts identified in the high performance work systems (Boxall and Macky 2009). The interviews were semi-structured and therefore new questions were asked whenever new ideas were presented by the interviewees. Additional questions were also asked to probe more deeply into the responses received or to clarify some issues. Thus, the interviews were tailored to the people and the context.

We conducted more than 20 interviews, 17 face to face and recorded on an audio device and three by telephone with notes taken during the interview. The interviewees came from a large mid-western University, a small technology firm with 150 employees, a large oil company and an aircraft parts manufacturer. On average, each interview lasted a little more than 30 minutes. In total there were 670 minutes of interview audio. The interviews were then transcribed, resulting in more than 200 single spaced pages in a Word document.

Data analysis

The interviews were coded in the following order: open coding, selective coding, and theoretical coding (Urquhart 2012). A memo summarizing the core message from each interview was also written at this stage. Open coding was performed multiple times on each of these transcripts. The next step was selective coding.

From the open codes identified in each interview, we selected core codes that explain compliance with information security policies. The memos summarizing each interview transcript were used to search for themes that appeared in more than one interview. These themes were aggregated into categories or super-categories. At this point, we used NVivo software to help us manage and organize the textual data.

From our analysis of the data, the following framework emerged for improving employee compliance with information security policies in organizations (Figure 2).

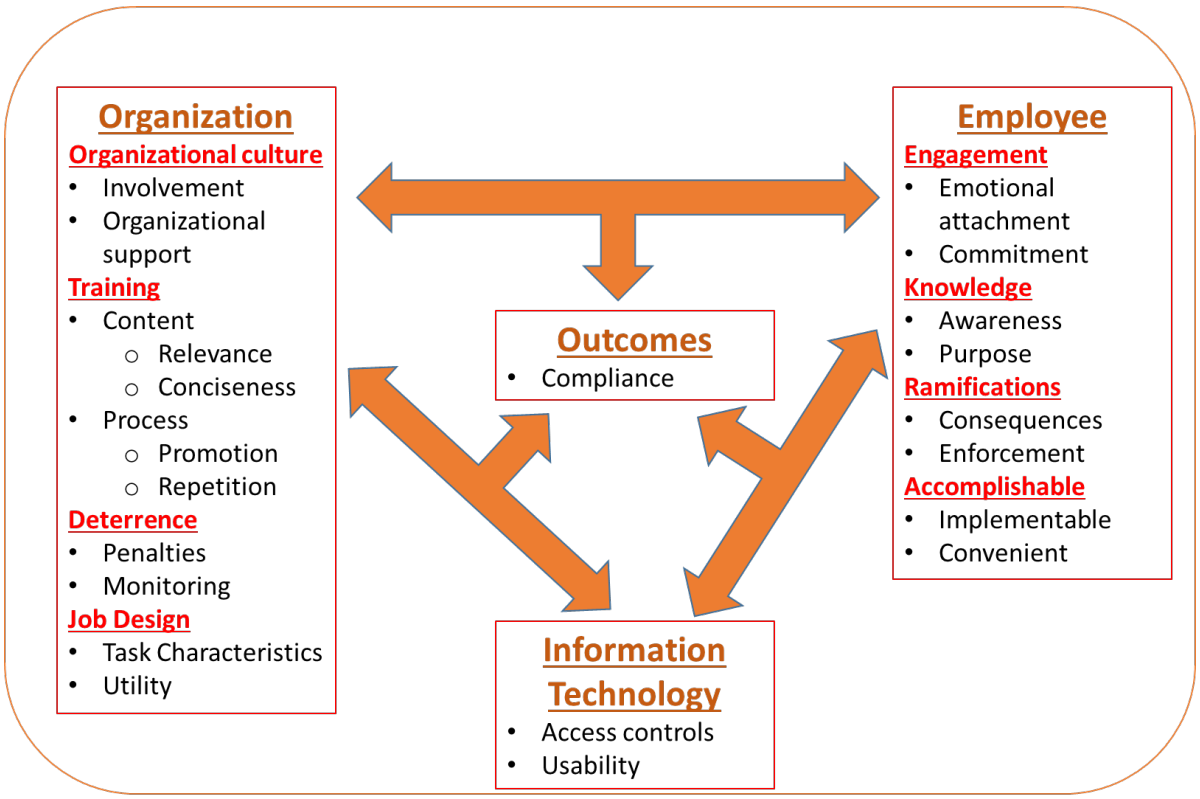

Figure 2: Framework for improving employee compliance with information security policies

The concepts, formed from selectively coding and categorizing the open coding labels, are clustered into four main categories: organization, information technology, employee, and outcomes. The framework represents a cycle with each of the categories impacting all the other categories.

DISCUSSION

The primary goal of this study was to understand how organizations can intrinsically motivate their employees to comply with information security policies. Although our data analysis shows that employees need both intrinsic and extrinsic motivation to improve their compliance, the discussion here is limited to intrinsic motivation. The first research question was:

> RQ1: *Why do employees fail to comply with an organization's information security policies?*

Our study found two intrinsic motivations, employee engagement and employee perception that a task can be accomplished. Engagement has two components, emotional attachment and commitment. Employees who demonstrate engagement comply with the information security policies with a passion and understand how important their behavior is to the organization. They feel a strong emotional bond to the organization and demonstrate a willingness to encourage fellow employees to comply with the information security policies.

Accomplishable refers to a policy that is realizable, achievable, doable, or manageable. The information security policies make sense to the employees and they have the ability to actually comply with them. The information security policies are well defined so that the employees can act on them. Therefor employees fail to comply for lack of engagement and if given tasks that are difficult to implement.

The second research question was:

> RQ2: *How can organizations help their employees to be intrinsically motivated to comply with the organization's information security policies?*

These two sources of intrinsic motivation are influenced by two organizational practices, organizational culture and job design respectively.

Organizational culture emerged as a determinant of employee compliance with information security policies. Two dimensions were identified in the organizational environment: employee involvement and organizational support. Employee involvement refers to employees' feeling they are part of the team that makes decisions impacting them. The opposite of this is a feeling of living under the law, and a dislike for rules that are inhibiting and excessively restrictive. Organizational support refers to the perception by employees that the organization has in place structures to help them succeed in their job. This support ranges from compensation, the work environment, and in-house technical support to the relationship with management.

Job design, the putting together of tasks or elements to form a job, includes what tasks are done, when and how the tasks are done, how many tasks are done, and in what order the tasks are done, factors which affect the work and the organization of the content and tasks. It is easier to comply with IT policies if they are built into the work process. For example, if employees are required to destroy social security numbers as part of their work, building this process into an IT policy would almost guarantee compliance. Job design clarifies what tasks are done and when and how they are done. For example, the interaction between a nurse, a patient, and the information technology (computer hardware and software applications) should be clearly stated step by step. Job design encompasses task characteristics and the usefulness of the procedures and limitations imposed by the information systems. In this context, "procedure" refers to who, what, where, when, and why a job is done in a given way; other words and phrases for this concept include protocol, accounting rules, and departmental login processes. "Usefulness" refers to convenient, enabling, and unobtrusive information security policies. For example, being required to change one's password too often is seen as inconvenient and policies that are too restrictive slow down the pace at which a job is done. Sometimes employees perceive information security policies as a barrier to accomplishing their day-to-day business.

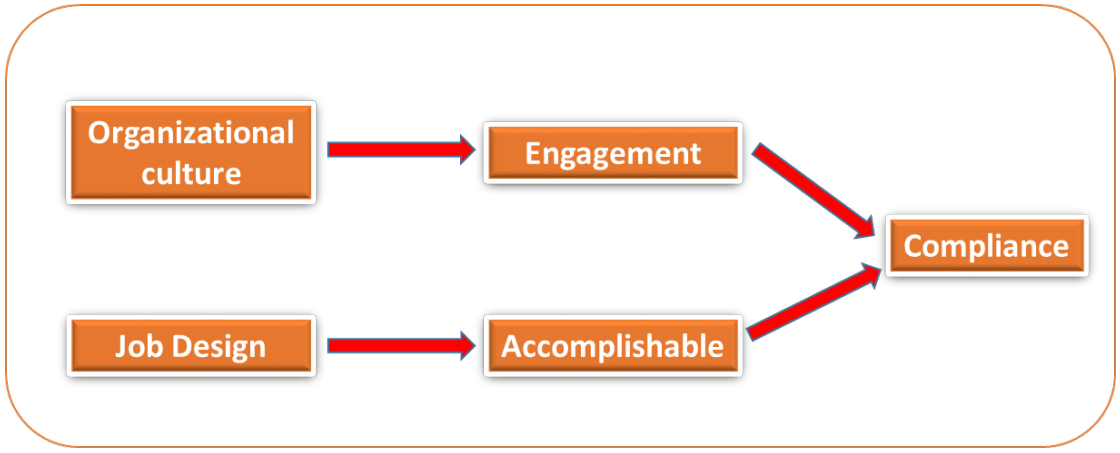

Figure 3: Model for intrinsically motivating employees

Effect of organizational culture on employee engagement

Therefore, organizations can help their employees comply with IS policies through creation of a positive work environment and designing policies that can be implemented comfortably.

REFERENCES

(Sykes and Matza 1957)Birks, M., and Mills, J. 2011. Grounded Theory: A Practical Guide. Thousand Oaks, California: Sage.

Boxall, P., and Macky, K. 2009. "Research and Theory on High-Performance Work Systems: Progressing the High Involvement Stream," *Human Resource Management Journal* (19:1), pp. 3 - 23.

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), pp. 523-A527.

Chuang, C.-H., and Liao, H. 2010. "Strategic Human Resource Management in Service Context: Taking Care of Business by Taking Care of Employees and Customers," *Personnel Psychology* (63:1), pp. 153 - 196.

D'Arcy, J., and Herath, T. 2011. "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), pp. 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), pp. 79-98.

Davies, F. D., Bagozzi, R. B., and Warshaw, P. R. 1992. "Extrinsic and Intrinsic Motivation to Use Computes in the Workplace," *Journal of Applied Psychology* (22:14), pp. 1111 - 1132.

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of Management Review* (14:4), pp. 532 - 550.

Goffee, R., and Jones, G. 1996. "What Hold the Modern Company Together?," *Harvard Business Review* (76:6), pp. 133 - 148.

Goodhue, D. L., and Thompson, R. L. 1995. "Task-Technology Fit and Individual Performance," *MIS Quarterly* (19:2), pp. 213 - 236.

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), pp. 203-236.

Hackman, J. R., and Oldham, G. R. 1976. "Motivation through the Design of Work," *Organizational Behaviour and Human Performance* (16), pp. 250 - 279.

Harper, G. R., and Utley, D. R. 2001. "Organizational Culture and Successful Information Technology Implementation," *Engineering Management Journal* (13:2), pp. 11 - 15.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hoffman, N., and Klepper, R. 2000. "Assimilating New Technologies: The Role of Organizational Culture," *Information Systems Management* (17:3), pp. 36 - 42.

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 Security Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and Protection Motivation Theory," *Computers & Security* (31), pp. 83 - 85.

Lawler, E. E., and Hall, D. T. 1970. "Relationship of Job Characteristics to Job Invlovement, Satisfaction and Intrinsic Motivation," *Journal of Applied Psychology* (54:4), pp. 305 - 312.

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), pp. 357 - 399.

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), pp. 635-645.

Liao, H., Toya, K., Lepak, D. P., and Hong, Y. 2009. "Do They See Eye to Eye? Management and Employee Perspectives of High-Perfomance Work Systems and Influence Processes on Service Quality," *Journal of Applied Psychology* (94:2), pp. 371 - 391.

Messersmith, J. G., Patel, P. C., and Lepak, D. P. 2011. "Unlocking the Black Box: Exploring the Link between High-Performance Work Systems and Performance," *Journal of Applied Psychology* (96:6), pp. 1105 - 1118.

Minor, W. W. 1981. "Techniques of Neutralization: A Reconceptualization and Empirical Examination," *Journal of Research in Crime and Delinquency* (18:2), pp. 295-318.

Patel, P. C., Messersmith, J. G., and Lepak, D. P. 2013. "Walking the Tightrope: An Assessment of the Relationship between High-Performance Work Systems and Organizational Ambidexterity," *Academy of Management Journal* (56:5), pp. 1420 - 1442.

Siponen, M., and Iivari, J. 2006. "Six Design Theories for Is Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:7), pp. 445-472.

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

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

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

Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review* (22:6), pp. 664-670.

Urquhart, C., Lehmann, H., and Myers, M. D. 2010. "Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20), pp. 357 - 381.

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

Venkatesh, V. 1999. "Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation," *MIS Quarterly* (23:2), pp. 239 - 260.