Winter 12-13-2018

THE DYNAMICS OF INFORMATION SECURITY POLICY ADOPTION

Alper Yayla
Binghamton University

Sumantra Sarkar
Binghamton University

THE DYNAMICS OF INFORMATION SECURITY POLICY ADOPTION

Alper Yayla[1]
School of Management, Binghamton University
Binghamton, NY, USA

Sumantra Sarkar
School of Management, Binghamton University
Binghamton, NY, USA

ABSTRACT

We argue that most organizations fail to internalize information security policies (ISPs) and only ceremonially adopt them because the adoption decision is generally driven by external legitimization purposes rather than efficiency gains. Based on the data collected from semi-structured interviews of senior executives, our preliminary findings reveal that ISPs are not integrated to the existing organizational routines until there is an external jolt such as a security breach. However, given the sudden nature of these jolts, ISPs do not gain internal legitimacy. We propose that after the implementation and before the internalization of ISPs, organizations need to actively integrate ISPs into their existing routines, with the aim of internal legitimization in the eyes of the organizational members.

Keywords: Security policy, Policy adoption, Policy implementation, Diffusion, Legitimacy

INTRODUCTION

Information security has become an important concern in organizations given the recent highly publicized security breaches. While initially organizations considered information security as a technology problem, the increasing number of security breaches proved that this is mostly a people problem. Practitioners and academics agree that systems will continue to be

[1] Corresponding author. ayayla@binghamton.edu +1 607 777 2440

compromised if users do not adopt technological controls and policies, making humans the weakest link (Rudolph et al. 2002). Today, organizations rely on a variety of detective and preventive technologies to increase their security. However, as Higgins (1999) noted, "without a policy, security practices will be developed without clear demarcation of objectives and responsibilities, leading to increased weakness" (p.217).

Since compliance with information security policies (ISPs) is essential to protect organizational information assets, the majority of the ISP literature attempts to tackle this area. This research stream mostly focuses on factors at the individual level – why and why not individuals comply with a policy. We argue that ISP compliance at the individual level depends on the success of policy implementation at the organizational level. Thus, we aim to provide a more granular understanding of the dynamics of *implementation* and *internalization* of ISPs. Our main argument is that implementation is often not internalized by organizational members because ISPs are considered organizational controls and they are adopted for external legitimacy purposes rather than efficiency gains. We further argue that after implementation and before internalization, organizations need to integrate ISPs into their existing structure and routines. However, our preliminary results show that organizations fail to integrate ISPs until there is an external jolt such as a breach or new regulation that breaks their inertia and forces them to integrate ISPs. Our paper attempts to fill the gap highlighted by Cram et al.'s (2017) review that calls for attention to the link between policy implementation and policy legitimization.

LITERATURE REVIEW

Existing studies have identified several research streams that focus on various aspects of ISP design, implementation, and compliance (Cram et al. 2017). Among these research streams, compliance-oriented research has drawn special interest because this issue is directly related to

employees' behaviors and potential risk of a security breach (Cram et al. 2017). One cluster of research that focuses on deterrence and control theories has identified several factors which may affect employees' intention and behaviors to comply with current organizational policy such as use of sanctions by organizations (Bulgurcu et al. 2010), employees' perception of mandatoriness (Boss et al. 2009), and fear appeals (Boss et al. 2015). Another research stream examines employees' inherent traits, behavior features, and organizational contingencies to uncover compliance patterns. Main argument of this research stream is that organizations can successfully implement ISPs by motivating employees, raising awareness, and providing incentives (Hedström et al. 2011; Yayla and Lei 2018). However, the existence of policies does not guarantee that employees are aware of their content. In fact, employees are exposed to ISPs few times in their work, mostly during the hiring process. Moreover, ISPs tend to be mostly stand-alone policies initiated by IT departments with limited governing power.

THEORETICAL FOUNDATIONS

There are two distinct motivations for practice adoption in organizations: efficiency gains and social legitimacy (Kennedy and Fiss 2009). Practices adopted for efficiency gains are driven by increases in economic performance, and practices adopted for social legitimacy are motivated with the desire to appear legitimate. Following Kostova and Roth (2002), we define practice as "an organization's routine use of knowledge for conducting a particular function that has evolved over time under the influence of the organization's history, people, interests, and actions" (p. 216). The level of institutionalization of the practice at the organization reflects the success of the adoption process. Institutionalization is conceptualized at two distinct levels: implementation and internalization (Kostova 1999). Implementation of a practice is the formation of ostensive routines at the organizational level. That is, the practice is an abstract concept and exists in

principle. Internalization of a practice is the formation of performative routines, which are routines practiced through certain actions by members of the organization. However, literature also shows that practices can be implemented yet not internalized in organizations. This is considered semi-institutionalization (Tolbert and Zucker 1996), ceremonial adoption (Kostova and Roth 2002), or symbolic adoption (Angst et al. 2017). Ceremonial adoption is likely to occur in the existence of strong external forces of legitimization and lack of internal motivation for adoption. Recent studies on practice adoption argue that there is a missing stage between implementation and internalization – an integration stage (Ahlvik and Bjorkman 2015; Bjorkman and Lervik 2007; Kennedy and Fiss 2009). In this stage, organizations integrate the new practice into their existing structure and routines (Kennedy and Fiss 2009). There have been many calls to fill the gap in the integration stage of practice adoption literature (Kennedy and Fiss 2009).

INFORMATION SECURITY POLICY ADOPTION

It is more likely that an adoption decision results in ceremonial adoption when the decision is driven by legitimization goal, rather than efficiency gain goal (Collings and Dick 2011). ISPs are rarely adopted for efficiency purposes, given their negative impact on performance. Organizations are more likely to adopt ISPs to conform to normative or regulative forces of their institutional environment. However, after organizations achieve external legitimization, they need to focus on internal legitimization – legitimization of the practice (i.e., ISP) in the eyes of the organizational members. Following Suchman (1995), we define legitimacy as "a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (p. 574). Basing their research on organizational control, Bijlsma-Frankema and

Costa (2010) argue that decrease in internal legitimization negatively affects the compliance behavior, highlighting the important role of internal legitimization in the adoption process.

RESEARCH METHODOLOGY

We use an exploratory case study approach and an inductive design to help build theory (Yin 2003). A case study approach will help us gain insights into the phenomenon by examining it in real-world settings.

Site Selection and Data Collection

We used theoretical sampling (Corbin and Strauss 2015) to select organizations with an IT department to support their business unit. Sample organizations varied from educational institutions to large electronics organization and banks. Our unit of analysis is an organization, comprising of business units and an IT department. Data was primarily collected through semi-structured interviews of senior executives of the organizations like chief information officers and chief information security officers. The focus of the interviews was to understand how ISPs were developed and maintained in the respective organizations of these executives. All interviews were recorded and transcribed. The interviews lasted for fifty minutes to one and a half hour. Six people have been interviewed so far with a target of 20 interviews spanning six organizations. Table 1 presents an excerpt of the interview questionnaire.

Table 1. Sample of interview questions

1. Please describe your role in your organization.
2. Please describe the IT security policies in your organization
3. Please describe your involvement in the design / development and implementation of the IT security policies in your organization
4. Please describe some challenges that you faced in implementation of the IT security policy
5. How did you overcome these challenges?

Data Analysis and Preliminary Findings

Data analysis were guided by principles laid by Klein and Myers (1999) and Walsham (2006) for interpretive studies. Seed concepts drawn from the literature on practice adoption, diffusion, and implementation were used to start our data analysis. The transcripts from the interviews were initially open coded, which was followed by axial and selective coding (Corbin and Strauss 2015). Key concepts, categories, and relationships were identified through this analysis process following the principle of abstraction and generalization. Text fragments from the interview transcripts ranging from phrases to sentences were tagged with codes along with justification for the selection of codes. New concepts emerging from data analysis were then related to the seed concepts. Finally, key themes were identified based on the codes that emerged, which were then synthesized into a framework presented in the next section. No attempts were made to statistically evaluate the strength of the concepts (Corbin and Strauss 2015), but the findings were used to develop a general explanation (Orlikowski 1993) through the use of analytic generalization (Yin 2013).

Analysis of the data led to interesting findings of the tension between integration and internal legitimacy of ISPs (Figure 1). Historically companies were in Cell 1 – ISPs are standalone and have low legitimacy. As security became a bigger concern in the past decade, companies moved to Cell 2. We found that most companies stay in Cell 2 and consider security as an important issue, yet do not integrate it into the routines of the organization. That is, for most companies ISPs are ceremonially adopted. Our interviews revealed that companies move from low integration to high integration only after an external jolt from a security breach, a change in a contractual obligation with a vendor/customer, or enforcement of a new regulation. However, because these jolts are external and sudden, companies tend to move from Cell 2 to

Cell 3. That is, ISPs are integrated, however, given their sudden enforcement, they are not aligned with existing routines. This is mostly reflected in terms of security taking over and becoming more important than daily operations and employees having hard time to conduct their daily work, leading to a decrease in the legitimacy of ISPs as they impede daily operations.

High Integration	3	4
Low Integration	1	2
	Low Legitimacy	**High Legitimacy**

Figure 1. Integration vs. legitimacy of ISPs in organizations

DISCUSSION

In summary, our main argument is that ISPs needs to be integrated into the organization before they can be successfully internalized. When ISPs are integrated, employees do not consider security as a separate issue but part of daily operations (Puhakainen and Siponen 2010). Tthe integration process should focus on the internal legitimization to achieve fully institutionalized ISPs. Currently, we are in the process of conducting more interviews. We expect that the findings of our study will provide more granular understanding to the ISP development, implementation, and legitimization process in organizations.

REFERENCES

Angst, C.A., Block, E.S., D'Arcy, J., and Kelly, K. 2017. "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), 894-916.

Ahlvik, C., and Bjorkman, I. 2015. "Towards Explaining Subsidiary Implementation, Integration, and Internalization of MNC Headquarters HRM Practices," *International Business Review* (24), pp. 497–505.

Bijlsma-Frankema, K. M., and Costa, A. C. 2010. "Consequences and Antecedents of Managerial and Employee Legitimacy Interpretations of Control: A Natural, Open System Approach," in *Organizational Control*, S. B. Sitkin, L. B. Cardinal, and K. M. Bijlsma-Frankema (eds.), Cambridge, UK: Cambridge University Press, pp. 396–433.

Bjorkman, I., and Lervik, J. E. 2007. "Transferring HR Practices within Multinational Corporations," *Human Resources Management Journal* (17:4), pp. 320–335.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. a, and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151–164.

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. 523–548.

Collings, D. G., and Dick, P. 2011. "The Relationship between Ceremonial Adoption of Popular Management Practices and the Motivation for Practice Adoption and Diffusion in an American," *The International J. of Human Resource Management* (22:18), pp. 3849–3866.

Corbin, J. M., and A. L. Strauss 2015. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Newbury Park, CA, Sage.

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), Palgrave Macmillan UK, pp. 605–641.

Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. 2011. "Value Conflicts for Information Security Management," *Journal of Strategic Information Systems* (20:4), pp. 373–384.

Higgins, H. N. 1999. "Corporate System Security: Towards an Integrated Management Approach," *Information Management & Computer Security* (7:5), pp. 217–222.

Kennedy, M. T., and Fiss, P. C. 2009. "Institutionalization, Framing, and Diffusion: The Logic of TQM Adoption and Implementation Decisions among U.S. Hospitals," *The Academy of Management Annals* (52:5), pp. 897–918.

Klein, H. K. and M. D. Myers (1999). "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), 67-94.

Kostova, T. 1999. "Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective.," *Academy of Management Review* (24:2), pp. 308–324.

Kostova, T., and Roth, K. 2002. *Adoption of an Organizational Practice By Subsidiaries of Multinational Corporations : Institutional and Relational Effects*, (45:1), pp. 215–233.

Orlikowski, W. J. 1993. "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems," *MIS Quarterly* (17:3), 309-340.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778.

Rudolph, K., Warshawsky, G., and Numkin, L. 2002. "Security Awareness," in *Computer Security Handbook* (4th ed.), S. B. and M. E. Kabay (ed.), New York: John Wiley.

Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *The Academy of Management Review* (20:3), pp. 571–610.

Tolbert, P. S., and Zucker, L. G. 1996. "The Institutionalization of Institutional Theory," *Handbook of Organization Studies*, pp. 175–190.

Walsham, G. 2006. "Doing Interpretive Research." *European Journal of Information Systems* (15:3), 320-330.

Yayla, A., and Lei, Y. 2018. "Information Security Policies and Value Con Flict in Multinational Companies," *Information and Computer Security* (26:2), pp. 1–17.

Yin, R. K. 2003. Case Study Research: Design and Methods. Thousand Oaks, CA, Sage.

Yin, R. K. 2013. "Validity and Generalization in future Case Study Evaluations," *Evaluation* (19:3), 321-332.