Legitimization of Information Security Policies in Organizations

TREO Talk Paper

Alper Yayla
Binghamton University - SUNY
ayayla@binghamton.edu

Sumantra Sarkar
Binghamton University - SUNY
ssarkar@binghamton.edu

Abstract

Given the recent highly publicized security breaches, information security has become an important concern in organizations. While initially organizations considered information security as a technology problem, the increasing number of security breaches proved that this is mostly a people problem. Existing studies in the literature have identified several research streams that focus on various aspects of information security policy (ISP) design, implementation, and compliance. Among these research streams, compliance-oriented research – why and why not individuals comply with a policy – has drawn special interest.

We argue that ISP compliance at the individual level depends on the success of policy implementation at the organizational level. 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.

Currently, we are using an exploratory case study approach and an inductive design to help build theory. We are using theoretical sampling to select organizations for our study. Data collection is primarily done through semi-structured interviews of senior executives of the organization. The focus of the interviews is to understand how ISPs were developed and maintained in these organizations. At the current stage of our data collection, we have sample organizations varying from educational institutions to large electronics organization and banks.

Analysis of the data collected so far 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 internal 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

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.