End Users’ Contribution to Information Security Policy Effectiveness

Janine L. Spears

The Pennsylvania State University
Smeal College of Business
University Park

1. Introduction

An organizational information security policy is widely believed to be one of the most important mechanisms used for managing the implementation and effectiveness of information security (e.g., Doherty & Fulford 2005; Hone & Eloff 2002; Whitman 2004). Nonetheless, in a study conducted by Doherty and Fulford (2005), no statistical relationship was found between the adoption of information security policies and the number of incidences or degree of severity of security breaches. These authors suggest that policy ineffectiveness may be contributed to reasons such as lack of employee awareness of security policies, difficulties in enforcing security policies, and an organization’s failure to tailor its security policies to its own environment.

This paper outlines a model for examining end users’ effect on information security policy effectiveness. Although several factors may contribute to policy effectiveness (e.g., completeness, timeliness, etc.), the focus here is on users, because as Hone and Eloff (2002:14) suggested, “at the end of the day, the users will determine how effective the information security policy really is.” It is argued in this paper that an effective information security policy must be: 1) business-driven as opposed to technology-driven, 2) adhered to by organizational members (e.g., users), and 3) inspire a climate of voluntary employee behavior that positively affects the organization’s security goals. The paper also recommends user participation in information risk management as a means to increase information security policy effectiveness.

2. Information Security Policy Effectiveness

2.1. Information Security Policies Described

The information security policy conceptualized in this paper is an organizational policy that attempts to meet Whitman’s (2004:52) description of what a good information security policy should do: “outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations and provide a mechanism for updating the policy” (Whitman 2004:52). In other words, an information security policy outlines the security goals of
the company and organizational members’ responsibilities (Vroom & von Solms 2004). It is believed here that the security goals outlined in organizational policy should be business-driven, as opposed to technology-driven (Halliday et al. 1996; Kokolakis et al. 2000; Suh & Han 2003).

2.2. Information Security Policy Effectiveness

As illustrated in Figure 1, the effectiveness of a security policy depends on the degree to which: 1) the policy is business-driven, 2) the policy is known and understood (user cognition), and 3) it results in desirable organizational (i.e., user) behavior. A business-driven information security policy refers to one that takes a top-down approach by letting organizational goals and objectives drive technical security policies as opposed to a bottom-up approach where technology is the primary driver of security policies. User cognition refers to users’ awareness and comprehension of information security policies intended to guide their behavior. User behavior refers to the degree to which users: a) perform expected security behavior as indicated in information security policies (in-role behavior), and b) perform discretionary behavior that is not required but that positively affects an organization’s information security efforts (extra-role behavior).

![Information Security Policy Effectiveness Diagram]

Figure 1. Information Security Policy Effectiveness

2.2.1. User Behavior

Organizational behavior literature has distinguished between an employee’s in-role behavior and extra-role behavior (e.g., Van Dyne et al. 1995). The former is expected behavior that is required by employees, while the latter is discretionary (optional) behavior that an employee voluntarily performs which is not formally rewarded but benefits the organization.
In-role Behavior

Users’ in-role behavior is centered on the assumption that organizations expect employees to follow information security policies and procedures. Table 1 contains types of in-role behavior as described in Van Dyne, Cummings, and Park (1995) that have been adapted to information security. These authors indicate that although these dimensions are typically conceptualized as extra-role behaviors, they have often been operationalized in studies as being in-role behavior. The key characteristic distinguishing in-role from extra-role behavior is that the former is behavior that is formally expected of employees as prescribed in job descriptions, organizational rules and procedures, employee evaluation criteria, etc.

<table>
<thead>
<tr>
<th>In-role Behavior</th>
<th>Definition</th>
<th>Examples of Information Security Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courtesy</td>
<td>Keeping the boss and coworkers informed</td>
<td>I update my supervisor on policies and procedures for protecting data.</td>
</tr>
<tr>
<td>Functional Participation</td>
<td></td>
<td>I attend or read all required training on information security.</td>
</tr>
<tr>
<td>Obedience</td>
<td>Respect for rules and policies</td>
<td>I do my best to strictly follow organizational rules and policies.</td>
</tr>
<tr>
<td>Social Participation</td>
<td>Engaging in group meetings and activities</td>
<td>I do my best to attend all group meetings and activities related to safeguarding information and related policies.</td>
</tr>
</tbody>
</table>

Table 1. Users’ in-role behavior (adapted from Van Dyne et al. 1995) affecting information security policy effectiveness.

Extra-role Behavior

Extra-role behavior is important because organizations cannot specify every desirable act an employee can or should perform in order to positively contribute to organizational objectives. As a result, organizations rely on employees to go beyond what is explicitly outlined in information security policies and procedures. Table 2 contains types of extra-role behavior as described in Van Dyne, Cummings, and Park (1995).
<table>
<thead>
<tr>
<th>Extra-role Behavior</th>
<th>Definition</th>
<th>Examples of Information Security Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advocacy</td>
<td>Innovation and proactively synergizing others</td>
<td>I proactively promote safe computing practices to my coworkers.</td>
</tr>
<tr>
<td>Courtesy</td>
<td>Keeping the boss and coworkers informed</td>
<td>I voluntarily update my coworkers on policies and procedures for protecting data.</td>
</tr>
<tr>
<td>Functional participation</td>
<td>Work-oriented effort and self-development</td>
<td>I go beyond what is required to learn about safe computing.</td>
</tr>
<tr>
<td>Task revision</td>
<td>Taking action to correct a faulty task or misdirected work role</td>
<td>I voluntarily took action to correct a control that was deficient or ineffective.</td>
</tr>
<tr>
<td>Principled dissent</td>
<td>A protest and/or effort to change the organizational status quo because of a conscientious objection to current policy or practice; requires violation of some impersonal system of value such as justice or honesty</td>
<td>I initiated a new or revised policy to limit system access or improve separation of duties in order to better secure information.</td>
</tr>
<tr>
<td>Voice</td>
<td>any attempt at all to change, rather than to escape from dissatisfying work conditions</td>
<td>I have spoken up about inefficient security controls that are not being followed.</td>
</tr>
<tr>
<td>Whistle-blowing</td>
<td>organizational members displacing illegal, immoral, or illegitimate practices under the control of their employers, to parties who may be able to effect action</td>
<td>I have reported breaches to information security committed by an internal employee to an appropriate authority.</td>
</tr>
</tbody>
</table>

Table 2. Users’ extra-role behavior affecting information security policy effectiveness (adapted from Van Dyne et al. 1995).

2.2.2. User Cognition

Although organizations may have established security policies, organizational members are often unaware that they exist (Dhillon 2004). For an information security policy to be effective, employees must be aware of the policy and understand the goals and responsibilities outlined in the policy. Table 3 contains dimensions of user cognition and examples that may be used to measure information security policy effectiveness.
--- | --- | ---
Policy Awareness | I am aware of the organization’s information security policy. I am aware of what to do in the event of an information security breach. | Adapted from Chan et al. 2005
Policy Comprehension | I understand the organization’s information security policy. I understand expected employee behavior to protect information. | Adapted from Chan et al. 2005
Understanding of Risk | I would likely be able to identify a breach to information security in my work environment if it occurred. | Adapted from Chan et al. 2005

Table 3. User cognition dimensions affecting information security policy effectiveness.

### 3. User Participation as a Strategy to Improve Information Security Policy Effectiveness

Effective management of information security risks requires participation from business users in the risk management process (Spears 2005). In addition to their knowledge of business objectives and processes that can aid in designing effective business-driven controls, business users need to be aware of how to manage information security risk. User participation in the risk management process refers to users analyzing information risk within their business processes, and designing and implementing security policies and procedures.

When users who perform or manage business processes participate in information risk management, information security policy effectiveness is likely to increase because (Spears 2007): 1) users can provide critical business information resulting in business-driven security policies, 2) through participation, users develop an intimate knowledge of information risk and organizational security policies, and 3) users are likely to develop a sense of ownership for the security policies and procedures resulting from their participation in the risk management process. These effects directly translate to information security policy effectiveness as reflected by: a) business-driven security policies, b) users’ awareness and understanding of information security policies and procedures, c) users’ adherence to security policies as required (in-role behavior), and d) users’ voluntary performance of desirable behavior that is not formally rewarded, but that is beneficial to information security objectives (extra-role behavior).

### 4. Conclusion

This paper has described dimensions of information security policy effectiveness. It is believed that an information security policy must be business-driven; it must outline expected behavior via formal rules; and employees must be cognizant of the policy.
The information security policy effectiveness concept described in this paper is congruent with Dhillon and Moore’s (2001) classification of formal and informal interventions respectively. Dhillon and Moores (2001) classified information security interventions into three categories: technical (deals with restricting access), formal (deals with establishing rules and ensuring compliance with laws and procedures), and informal (deals with educational awareness within organizations). In other words, in addition to technical interventions (controls), information security policies specify formal expected role behavior and must be disseminated via informal interventions that increase user awareness and understanding of such policies.

References

Suh, B., and Han, I. "The IS risk analysis based on a business model," Information & Management (41:2), 2003 2003, pp pp. 149-158.