Information Security Policy Research Agenda

Heather Fulford
The Robert Gordon University, UK

Neil Doherty
Loughborough University, UK

INTRODUCTION

For the past two decades, it has been argued that an 'information revolution' is taking place that is having a significant impact upon all aspects of organizational life (e.g., Porter & Millar, 1985; Drucker, 1988). If applied effectively as a strategic resource, investment in information can result in the realization of significant corporate benefits. Indeed it has been contended that "information is the firm's primary strategic asset" (Glazer, 1993), and elsewhere that it is the "lifeblood of the organization" (CBI, 1992) contributing directly, as it does, to the organization's operational performance and financial health. (Bowonder & Miyake, 1992; McPherson, 1996). However, information can only be recognized as a vital organizational resource if managers can readily gain access to it when required. Unfortunately, as a consequence of the high incidence of security breaches, many organizations are failing to consistently provide the information resources that their managers require (Angell, 1996; Gaston, 1996).

Information only retains the potential to deliver value if its confidentiality, integrity, and availability are protected (Menzies, 1993; Gaston, 1996). However, the increasing integration of information systems, both within and between organizations, when coupled with the growing value of corporate information resources, have made information security management a complex and challenging undertaking (Gerber, von Solms, & Overbeek, 2001). Indeed, it is estimated that "security breaches affect 90% of all businesses every year, and cost some $17 billion" (Austin & Darby, 2003). Moreover, Austin and Darby (2003) also suggest that protective measures can be very expensive, noting for example that "the average company can easily spend 5% to 10% of its IT budget on security."

One increasingly important mechanism for protecting corporate information, in an attempt to prevent security breaches rather than merely respond to them, is through the formulation, dissemination, and implementation of an information security policy (Hone & Eloff, 2002a). Indeed, the information security policy has been denoted as "one of the most important" information security controls (Hone & Eloff, 2002b), and elsewhere as the "start of security management" (Higgins, 1999) and the "sine qua non (indispensable condition) of effective security management" (von Solms & von Solms, 2004). The primary reason that the information security policy has become the "prerequisite" (David, 2002) or "foundation" (Lindup, 1995) of effective security management has been suggested by Higgins (1999), who notes that "without a policy, security practices will be developed without clear demarcation of objectives and responsibilities."

The overall aim of an information security policy then is to create the "ideal operating environment" for the management of information security (Barnard & von Solms, 1998). It does so by defining "the broad boundaries of information security" as well as the "rights and responsibilities of information resource users" (Hone & Eloff, 2002b). Specifically, a good information security policy should:

> *...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)

Furthermore, the information security policy should act as an important tool for demonstrating to employees, as well as to other stakeholders, management's commitment to, and recognition of, the importance of information security issues within the organization (Hone & Eloff, 2002b).

The increasing awareness of the importance of the information security policy, coupled with the advent

of national and international standards on policy formulation, dissemination, and implementation, have given rise to a growing body of literature on information security policies. The purpose of this article is to report on a thorough and focused review of the existing literature on the role of information security policies in information security management. A summary of the key themes in that literature are presented and discussed, demonstrating how the subject has been treated to date, and illustrating the issues and perspectives that have been addressed. In addition to reporting on what has been presented in the literature so far with regard to the role of policies in information security management, indications will be given of issues relating to information security policies that have not as yet been dealt with in any depth or detail in the existing literature. To conclude the article, these untreated issues will then be discussed and drawn together into a proposal for a future research agenda in this important area of information security management, and the implications for managers of the current literature coverage will be considered.

KEY THEMES IN THE LITERATURE ON INFORMATION SECURITY POLICIES

Gaston (1996) suggests that the information security policy can be defined as "broad guiding statements of goals to be achieved." Such a policy serves to "define and assign the responsibilities that various departments and individuals have in achieving policy goals." This definition is broadly in line with the British Standard on Information Security Management (BSI, 1999; now ISO 17799), which suggests that the information security policy document should "set out the organization's approach to managing information security." As such, information security policies typically include "general statements of goals, objectives, beliefs, ethics and responsibilities, often accompanied by the general means of achieving these things (such as procedures)" (Wood, 1995). These procedures or guidelines tend to be advisory, whereas "policies are mandatory," and consequently "special approval is needed where a worker wishes to take a different course of action" from that stipulated in the policy (Wood, 1995).

Theme I: The Structure and Format of Information Security Policies

While there is a high degree of consensus in the literature with regard to a broad definition for the information security policy, there is rather more debate as to whether there should be a single policy, or whether it should be subdivided into several distinct levels or types (Baskerville & Siponen, 2002). This debate represents a key theme in the literature on information security policy formulation. Examples of structures and formats discussed include Siponen's suggestion that security policies can be classified into two broad groups, namely "computer-oriented policies" or "people/organizational policies" (Siponen, 2000). By contrast, Sterne (1991) distinguishes between three levels of policy, namely the "institutional policy, the institutional information security policy and the technical information security policy." Lindup (1995) agrees that there is no single information security policy, but suggests instead that there are several distinct types, rather than levels, which include the "system security policy, product security policy, community security policy and corporate information security policy." Lindup (1995) further makes the claim that, while academics may continue the debate about ways of classifying or sub-dividing policies, in practice organizations tend to have a single "corporate policy."

Interesting though this theoretical debate may be, this area of information security management warrants in-depth empirical investigation in order to help inform the discussion and provide meaningful insights. Specific issues worthy of investigation in this respect include:

1. There is a need for studies of the range of policy structures and formats that exist, and indications of the levels of uptake in organizations of the various types, incorporating an examination of relationships between policy structure and organization type, size, industry sector, and so on.
2. There is scope for investigating the factors motivating an organization to adopt a particular policy structure and format.
3. A valuable contribution could be made by research exploring the efficacy of each type of policy structure in the overall framework of an organization's efforts to manage its information resources.