Computers & Security (2005) 24, 246–260

Computers & Security

www.elsevier.com/locate/cose

Information systems security policies: a contextual perspective

Maria Karyda[a], Evangelos Kiountouzis[a,*], Spyros Kokolakis[b,1]

[a]*Department of Informatics, Athens University of Economics and Business, 76 Patission Street, Athens GR-10434, Greece*
[b]*Department of Information and Communication Systems Engineering, University of the Aegean, GR-83200 Karlovassi, Samos, Greece*

Received 6 April 2004; revised 16 August 2004; accepted 18 August 2004

KEYWORDS
Information systems;
Security policy implementation;
Security policy adoption;
Contextualism;
Security awareness

Abstract The protection of information systems is a major problem faced by organisations. The application of a security policy is considered essential for managing the security of information systems. Implementing a successful security policy in an organisation, however, is not a straightforward task and depends on many factors. This paper explores the processes of formulating, implementing and adopting a security policy in two different organisations. A theoretical framework based on the theory of contextualism is proposed and applied in the analysis of these cases. The contextual perspective employed in this paper illuminates the dynamic nature of the application of security policies and brings forth contextual factors that affect their successful adoption.

Introduction

Organisations nowadays depend largely on computer-based Information Systems (IS) for a vital part of their operation. IS comprise the *information* that is being stored, or in any way processed by an organisation, the *hardware* and *software* that constitutes the configuration of computer systems, a *social system* that is formed by the actions and relations among the IS users, as well as a set of *procedures* that guide the users' actions. Under this perspective, IS have not only a technical part, but also a social dimension. IS are of high significance to organisations across a wide range of economic sectors. In consequence, their proper function and unobstructed operation is a critical issue that has attracted the attention of both IS research and practice.

Information systems security management is a stream of management activities that aim to protect the IS and create a framework within which

* Corresponding author. Tel.: +30 210 8203555; fax: +30 210 8237369.

E-mail addresses: mka@aueb.gr (M. Karyda), eak@aueb.gr (E. Kiountouzis), sak@aegean.gr (S. Kokolakis).

[1] Tel.: +30 22730 82233; fax: +30 22730 82009.

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.08.011

the IS operates as expected by the organisation (Eloff and von Solms, 2000). IS security management aims to minimize risks that information systems face in their operation and includes a number of different phases: a *planning* phase, an *implementation* phase, during which security plans are put to action and an *assessment* or *audit* phase (Dhillon, 1997; Björck, 2001). Finally, tasks aiming to develop security *awareness* and provide security *training* and *education* are also included in the IS security management agenda (Trompeter and Eloff, 2001).

The application of an IS security policy is one of the major mechanisms employed by IS security management. An IS security policy includes the intentions and priorities with regard to the protection of the IS, usually referred to as security objectives, together with a general description of the means and methods to achieve these objectives. The formulation of a security policy is a multifaceted task of critical importance (Höne and Eloff, 2002a) and should combine technical and organisational measures that address security requirements for protecting not only the components of the IS, but also their overall functionality (Karyda et al., 2001).

Despite the fact that the formulation and use of a security policy is common practice and that organisations devote significant resources to security management activities, it is commonplace that too often the application of a security policy fails to accomplish its goals. The formulation of an effective security policy can be a very demanding and complicated activity. Although guidance for formulating a security policy is widely available (e.g. information security management standards, best practices etc.), there is strong scepticism from both IS security researchers and practitioners towards the use and effectiveness of security policies (Höne and Eloff, 2002b). A variety of reasons and explanations have been put forth for explaining the lack of effectiveness in the use of IS security policies, including that security controls often constitute a '*barrier to progress*' and that security policies are very likely to be circumvented by employees in their effort to perform efficiently their tasks (Wood, 2000). Other explanations that have been proposed acknowledge the fact that in order to be effective, an IS security policy should meet the particular security requirements and objectives that depend on the specific organisation and its environment. Whereas the security objectives for individual entities (such as servers, workstations, files and networks) may be similar across different organisations, nevertheless, there is no single security solution, nor a single security policy that can fit all organisations (Whitman et al., 2001).

Several surveys have been conducted to investigate security management issues. These surveys, however, have been mostly commercially oriented, using quantitative, primarily statistical methods, whereas hardly any academic studies based on qualitative analysis exist. Moreover, such surveys cover a broad range of IS security issues, rather than focusing specifically on the issues pertaining the application of IS security policies and their effectiveness.

This paper attempts to fill in this gap by studying the formulation, implementation and adoption of IS security policies in relation to the specific context within they take place. To accomplish this goal we have adopted a broader perspective on IS security policies than usually found in the literature, where most studies focus either on prescriptions for policy formulation (Peltier, 1999), or on the main obstacles that must be overcome during the implementation of the policy (Wood, 1999). More specifically, in this paper we examine the processes of the formulation, implementation and adoption of IS security policies in two cases: the case of a public sector social security organisation and the case of a non-governmental centre for the treatment of dependent individuals. The theoretical framework we propose and use for the analysis of the two case studies draws mainly from organisation theory and management science, and its focus is on understanding and exploring the dynamics and interplay of the processes related to the application of an IS security policy within a particular organisation. We use the theory of *contextualism*, in order to take into account the influence that the context has on security management processes, and to link these processes to their specific outcomes. The theory of contextualism, that has been largely applied in information systems studies to explore the issue of organisational change (Walsham and Waema, 1994), can provide IS security research with valuable insights. The conclusions we derive from studying two separate cases of organisations applying a security policy illuminate the dynamic relationship between the way security practices are put to use and their environment. Last, but not least, these conclusions can be an aid to practitioners that are either formulating or putting a security policy to action, since they bring forth some of the not so well accounted for aspects of security management.

The next section is an overview of the literature on IS security policies, underlining the need to explore the dynamics of the processes involved in the application of security policies within organisations. The theoretical framework used for the analysis of the case studies is presented in the