Computers & Security (2005) **24**, 246–260

ELSEVIER

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 third section. The next two sections report on the methodological approach we followed during our research and provide a description of each case followed by a detailed analysis and conclusions. Next, our overall findings and conclusions derived from both cases are summarized and, in the last section, general remarks and indications for future research are presented.

IS security policies: formulation, implementation and adoption

The majority of studies on security policies published in the IS security literature adopt a technical perspective. The best part of the relevant research discusses small-scale formal security policies, rather than large-scale policies at the organisational level (Siponen, 2002). Different types of security policies can be categorised based on their focus on 'technical' or 'organisational' elements (Siponen, 2000b), or based on their specific topic as application policies, system specific policies, or organisational policies. IS security policies, however, include both the security objectives and the designated means and methods to achieve them; therefore they must combine technical and organisational guidelines addressing security requirements at the organisational level.

The *formulation* of a security policy is done at the planning stage, in most cases as part of a broader security plan that aims to provide adequate protection for the IS, through a set of security measures and practices (Peltier, 1999; Wood, 1999). The *implementation* of an IS security policy is the process during which the compiled security policy becomes 'translated' in guidelines, procedures and to-do lists that are put to practice by the IS users. The people who take up the responsibility of implementing the security policy usually belong to the IT department of the organisation. The outcome of the implementation process is a list of 'doable' actions to be performed by the members of the organisation, which aim to achieve the security goals stated in the *security policy*. This process can also have an organisational dimension, since it usually involves the creation or adaptation of organisational roles (e.g. Security Officer, IS auditor etc.) and their responsibilities. Thus, the implementation of a security policy entails the realization of the technical and organisational security measures that are prescribed in the policy. Once it has been implemented, the security policy must be communicated to the IS users and should be periodically reviewed and evaluated, particularly after any major change in the configuration or operational mode of the IS.

The *adoption* of the security policy by the users, which should follow a successful implementation process, requires that users shape their actions and behaviour, so as to accommodate the security guidelines. Researchers argue that for any programme affecting user behaviour to be effective, it should satisfy the requirements of behavioural theories (Siponen, 2000a). Information security guidelines are of prescriptive nature, constituting an imperative for IS users. However, users very often fail to apply them in the way they were intended (Siponen, 2000a) even though they are aware of them. Therefore, several researchers underline the need for further research on issues such as information security management, awareness, and information security policies (Siponen, 2000a; Björck, 2001). Moreover, Gritzalis (1997) argues that the security guidelines are context specific and that they can be effective within a given technological environment and operational mode.

Baskerville and Siponen (2002) explore the formulation of security policies in emergent organisations, placing emphasis on the fact that different organisations have different security needs, and thus different security requirements and objectives. Another issue that arises with regard to the application and use of a security policy is that, in order for users to apply the security guidelines, the latter need to be adequately justified. Justification provides the basis for the accommodation of the guidelines by the users. Fig. 1 depicts a high level process view of the processes involved in the application of an IS security policy in an organisation. The process of reviewing and evaluating the security policy serves as a feedback mechanism providing input for the reformulation of the policy.

Each process depicted in Fig. 1 uses certain input, includes a set of activities and results in certain outcomes. Figs. 2—4 present in detail the input, output and the activities of the processes depicted in Fig. 1. The process of security policy formulation, presented in Fig. 2, utilizes, among others, the results of a risk assessment and guidelines from security management standards and best practice as the input, for resulting to the compilation of the security policy document and a set of guidelines for the selection and application of security measures.

The process of the implementation of a security policy, that is depicted in Fig. 3, utilizes both the

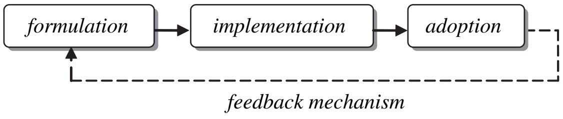

Figure 1 The security policy application process.

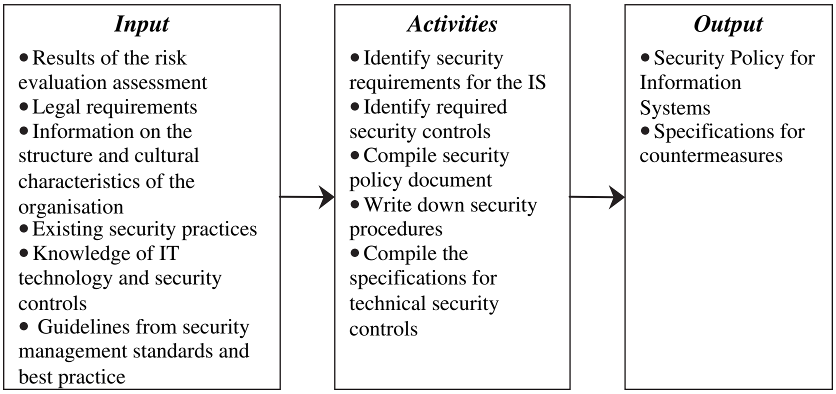
Input
• Results of the risk evaluation assessment
• Legal requirements
• Information on the structure and cultural characteristics of the organisation
• Existing security practices
• Knowledge of IT technology and security controls
• Guidelines from security management standards and best practice
Activities
• Identify security requirements for the IS
• Identify required security controls
• Compile security policy document
• Write down security procedures
• Compile the specifications for technical security controls
Output
• Security Policy for Information Systems
• Specifications for countermeasures

Figure 2 The process of security policy formulation.

security policy document and relevant knowledge and information on the social and cultural aspects of the organisation. Finally, the adoption of a security policy, as shown in Fig. 4, refers to established work practices enhanced with security procedures and the use of security controls, and results to an overall increase of the security awareness among IS users, that, in the long run, helps to develop a security culture in the organisation.

This paper aims to provide answers to the following questions: (a) how is a security policy formulated and implemented in a specific organisation? (b) which are the contextual factors that are associated with the successful adoption of a security policy? and (c) can the research framework proposed in this paper be used for providing useful answers to these questions? To accomplish this, we focus our analysis on the processes of formulating and implementing IS security policies within organisations, as well as on the elements that can play a critical role for their successful adoption.

Theoretical framework

The theoretical basis of our study evolved as a result of both our understanding gained through the collection and analysis of the field data and from studying the IS literature and looking for an appropriate theory. We were influenced by the stream of processual research; the theoretical framework applied for the analysis of the case studies mainly draws on the core tenets of the theory of contextualism (Pettigrew, 1987), and it is described in detail in the next sections.

The theory of contextualism and processual research

Security policies and guidelines are applied by people. Given the fact that human behaviour cannot be fully predicted, to study the application and use of security policies we need an approach that takes into consideration the diverse aspects of human action. For this reason, our research approach in this paper draws on the theory of *contextualism* (Pettigrew, 1987), using its key elements as a framework for analysing the formulation, implementation and adoption of a security policy in the cases of two organisations. In general, the theory of contextualism has been mainly used as an analytical instrument for exploring the relationship and interplay between the content of

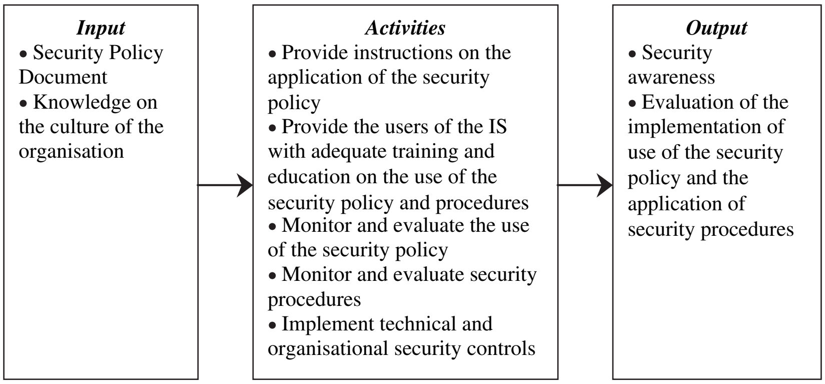
Input
• Security Policy Document
• Knowledge on the culture of the organisation
Activities
• Provide instructions on the application of the security policy
• Provide the users of the IS with adequate training and education on the use of the security policy and procedures
• Monitor and evaluate the use of the security policy
• Monitor and evaluate security procedures
• Implement technical and organisational security controls
Output
• Security awareness
• Evaluation of the implementation of use of the security policy and the application of security procedures

Figure 3 The process of security policy implementation.

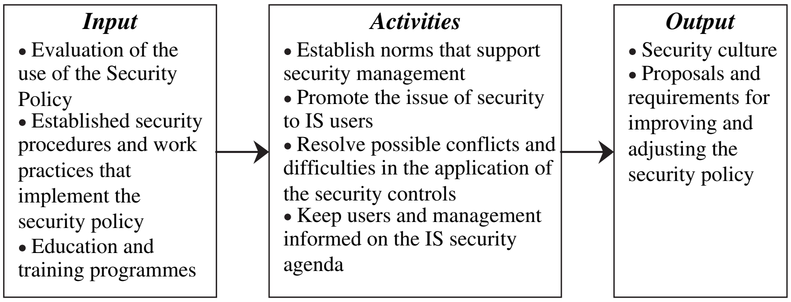
Input
• Evaluation of the use of the Security Policy
• Established security procedures and work practices that implement the security policy
• Education and training programmes
Activities
• Establish norms that support security management
• Promote the issue of security to IS users
• Resolve possible conflicts and difficulties in the application of the security controls
• Keep users and management informed on the IS security agenda
Output
• Security culture
• Proposals and requirements for improving and adjusting the security policy

Figure 4 The process of security policy adoption.

strategic change, the context of change and the process of managing change (Pettigrew and Whipp, 1993) in organisation studies.

The theory of contextualism has an underlying processual perspective, where a process can be described as '*a sequence of individual and collective events, actions and activities unfolding over time in context*' (Pettigrew, 1997). Social processes are considered embedded in the contexts that produce and are produced by them, therefore they cannot be studied outside this context. Processes can span different levels of analysis and there can also be multiple processes at the same level of analysis.

Levels of analysis

In the two cases presented in this paper, we have studied the processes of formulating, implementing and adopting a security policy in each organisation at three different levels: at the *organisational* level, at the level of the *work system* and at the level of *information technology*.

Information systems are used throughout most organisational activities; therefore we use the concept of *work system* to refer to a set of different elements that operate in conjunction with one another: business processes, services, customers, employees, information, technology. A work system is a system in which human participants and/or technological elements realize business processes using information, technology and other resources to produce services and/or products for internal or external customers. The people who participate in a work system, called *participants* or *actors*, are the users of the information system and *their actions realize the security policy*. Typically, organisations contain multiple work systems and operate through them (Alter, 1999). Understanding a work system entails also understanding its environment that includes managerial, organisational, legal, regulatory, and competitive factors. These factors, that comprise the context of a work system, have been the focus of our analysis at the organisational level. At the technical level we have explored the technical infrastructure with regard to the information systems used in each organisation. Particularly, the object of the analysis at this level has been the technical security controls that are applied for the implementation of the security policy. Table 1 summarizes the description of the three different levels of analysis used in the two case studies.

Key elements in contextual research

The core concepts in contextualism are the *context*, the *content* and the *process* of organisational

Table 1 Levels of analysis

Levels of analysis	Description
Organisational level	• Structure, management style, norms and culture of the organisation. • Role and support provided by management. • Relationships both within the organisation, as well as relationship with external organisations, bodies etc.
Work system level	• It refers to IS users, business processes and their products or services, customers of the services or products, the technology and the information that is used.
Information technology level	• Specifications and configuration of the technical components of the IS. • Software and hardware used for the implementation of the security controls.

change and they are considered to be interrelated. The main objective of contextual research is to trace their dynamic interlinking over time, providing explanations on how the content of change has been shaped by the processes within the specific context where they take place.

Processes that unfold in an organisation are shaped by the outer and the inner context. The *outer context* includes factors that are found in the economic, political, social, competitive and sectoral environment in which the organisation is located, whereas the *inner context* includes structural, political and cultural elements within the organisation. Both the outer and inner context in conjunction shape the features of the processes. The context shapes the outcome of the processes through the activities and behaviour of the actors. *Human agency* is also a basic element in contextualism, since actions drive the processes, but the processes cannot be fully explained by reference only to individual or collective agency. Actions are embedded in the context, which limits their information, insight and influence, thus the context is shaping the actions and actions shape the context. Another critical point is the element of *time*. The theory of contextualism interprets organisational phenomena by linking the processes under study to their outcomes; therefore understanding the sequence and flow of events over time is a crucial requirement.

The aim of contextual research is to discover the mechanisms that shape the patterns in the processes under study, and to provide holistic explanations on organisational features, by linking these processes with the content of change as it is shaped within the context. A core requirement of contextual analysis is to understand the emergent, situational and holistic features of the processes under study in their context.

Pettigrew's categorisation of *content*, *context* and *process* has been used as a framework for reviewing issues pertaining the evaluation of information systems (Symons, 1991) and the formation of information systems security policies (Karyda et al., 2003). In this paper, contextualism provides a meta-framework (Pettigrew and Whipp, 1993), for exploring the way security policies are formulated, implemented and adopted within organisations. Contextualism was chosen as a basis for developing the theoretical framework in our research, because it can help us explore the way security policies are formulated, implemented and adopted by providing us with an analytical device for exploring the dynamic interlinking among *the content of security policy, the processes of IS security policy formulation, implementation and adoption* and the different *levels of organisational context*. The application of security policies in organisations entails changes that occur at the different organisational levels and these changes are shaped by the processes involved in this endeavour. Therefore, contextual analysis is a useful tool for studying the application of security policies in organisations.

Perspectives on the application of IS security policies: power and culture

The application of the theory of contextualism in research requires that an underlying theory of human behaviour is adopted, for explaining the way processes unfold in their context (Pettigrew, 1987). In this paper, we have adopted a twofold perspective on the actions and relations among the IS users: on the one hand we examine the *power* relations between the users, and on the other hand, we study the *culture* of each organisation, aiming to explore the way the processes of formulation and implementation of the security policy have evolved in each case.

Therefore, we have explored the use and exercise of *power* by the members of each of the organisations we have studied with regard to the formulation and the implementation of the security policy. This approach constitutes the adoption of a '*political perspective*' that is increasingly used in the organisation and management literature, where many researchers have embraced the idea that organisations can be considered as '*political arenas*' (Mintzberg, 1985). Although many definitions of power have been proposed, in this paper we use the term with its general and inclusive meaning of *the ability of an actor to affect an outcome, or more simply, to get things done*. Under this view, we have interpreted the actions performed by the IS users who were associated with the application of the security policy, on the basis of their ability to exercise their influence or authority, to use and allocate resources and make decisions. Despite the fact that the issue of organisational power relations is usually considered in a negative way, implying behind-the-scenes manipulation and manoeuvring, we have adopted a neutral view, considering power as an inherently necessary mechanism for the function of the organisation (Ammeter et al., 2002).

Besides the issue of power relations, we have also explored the *cultural* dimension of the application of a security policy. The concept of culture, brought in the IS field from anthropology, has been used in a variety of ways in the IS literature and with many different meanings. In this paper, we use the term culture to refer to the '*shared* *meaning among an organised group of individuals*' (Walsham and Waema, 1994). The context in which a security policy is formulated and eventually is put to practice, and particularly the inner context, is characterised by certain rules, norms and interpretation schemes that guide the actions and the relationships between the policy users. The implementation and use of a security policy entails the introduction of new rules and interpretation schemas that can be in accordance or in conflict with the pre-existing ones, therefore altering the way people perceive things and thus creating new norms and patterns of practice. However, it is often the case that the security rules and guidelines, are viewed in a negative way by the users, who may reject them or refuse to use them, thereby preserving pre-existing norms and rules.

Framework for analysis

A theoretical framework is an organised set of ideas and concepts and it is used for organising a thought process about a particular object or situation. Within a theoretical framework different topics for consideration are identified, along with an indication of their interrelation. To study the processes involved in the formulation, implementation and adoption of IS security policies, we have developed a theoretical framework that is based on the theory of contextualism, as described in the previous sections. The framework also adopts a power and a cultural perspective. We apply the theoretical framework in the analysis of the application of a security policy in two different cases: the case of a state-governed institute for social security and the case of an independent organisation for the treatment of individuals with problems of drug addiction. The theoretical framework we have developed spans three different levels of analysis, the *organisation* level, the *work system* level and the *information technology* level that have been presented in Table 1. We apply this framework in the two cases to explore the dynamics of the processes of the formulation, implementation and adoption of the IS security policy, as has been depicted in Fig. 1. Our aim for this analysis is to provide explanations to the research questions that have triggered this research, that is to find out how a security policy is formulated and implemented in a specific organisation and which factors affect its successful adoption. Table 2 presents in detail the dimensions of the theoretical framework for analysis that has been applied.

Research strategy and design

Within the IS security literature, a variety of research approaches, including surveys and case studies (Björck, 2001), have been employed for exploring issues pertaining security management.

Table 2 Dimensions of the contextual framework

Dimensions	Description
Content	Organisational level: • Changes to the organisational structure and roles. • Changes to the norms and attitudes. Work system level: • New work practices developed. • Existing work practices adapted for compliance. Information technology level: • Changes to hardware, software and related technological infrastructure used. • Introduction of new technological components.
Context	Outer context: • Economic, legal, political, social, competitive and sectoral factors that are found in the environment of the organisation. Inner context: • Managerial, structural, political, social and cultural elements within the organisation.
Process	Cultural perspective: • The formulation and implementation of a security policy draw on the existing culture, norms and rules and have the potential to affect them, therefore these processes can have an impact on the social context. Power perspective: • Power relations are involved in the formulation and implementation of a security policy, altering or reinforcing the context in which they take place.

The research approach we have adopted to the application and use of IS security policies is primarily explorative and descriptive in nature, aiming to provide us with an understanding of the dynamics of the application of security policies, and to give us an insight into the contextual factors that affect their successful adoption.

The underlying epistemology of our approach lies in the interpretive paradigm (Dhillon, 1997); we assume that the implementation and use of an IS security policy in an organisation should be examined against the frame of reference of the individuals associated with these processes, and against the overall social context within which they occur. Under this perspective, decisions affecting the formulation and implementation of a security policy are made by individuals, depending on their prior experience and knowledge, as well as their personal goals and priorities. Likewise, security policies are used by people, who have to interpret the directions and guidelines included in the policy and act accordingly.

Our goal throughout this research has been to explore and reveal the contextual factors that are critical for security management, through shaping the processes involved in IS security management and their outcome. The selection of our research method has been guided by the nature of our research object and by the type of the research questions that have triggered this research, as is widely suggested in the literature (Jarvinen, 2000; Eisenhardt, 1989; Yin, 1994). Therefore, we have studied the processes of security policy formulation, application and adoption within their organisational context in two different cases. Within the IS literature, case studies are considered a useful and appropriate research tool for answering '*how*' or '*why*' questions (Yin, 1994) both by a positivist and an interpretive stance (Walsham, 1995). A significant number of interpretive case studies has been published in the IS literature, mostly for exploring, classifying and hypothesizing. Case studies in general, "*examine a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities*" (Benbasat et al., 1987).

In the next section we provide an overview of the two cases, where the authors have been involved in the project of providing the organisations with a risk assessment study and generic guidelines for managing the security of their information systems. The data for the case studies have been collected during interviews, by acquiring documentation concerning the information system and the organisational structure as well as other publicly available material on the organisations, and by using relevant resources on security management. This material has been subsequently codified according to the issues in our research agenda: we have selected and analysed the data relevant to the dimensions of the context, the content and the processes of security policy formulation, implementation and adoption in each organisation. The authors carried out several semi-structured interviews with members of the two organisations from all management levels. In several of these interviews the interviewees participated in small groups (two to four people at a time). The questions for these interviews have been formulated on the basis of the risk analysis and management method CRAMM (UK CCTA, 2002) and the duration of each interview lasted from half an hour to two hours. We decided not to use a tape recorder, because our previous experience in similar organisations has showed that people being interviewed on security-related topics were very self conscious and often reluctant to provide their opinion or point of view.

The analysis of these cases reveals the patterns of events that are related to the successful formulation, implementation and adoption of the security policy. We chose the specific organisations for conducting our research for the following reasons. Firstly, these organisations launched the process of applying a security policy from the beginning; none of them had a security policy in place before. This permitted us to study inclusively the processes of formulating, implementing and adopting a security policy within an organisation. Secondly, we could have access to historical data on these organisations with regard to the use of information systems and information technology; in one of the cases the data go back more than two decades and have been published before. This is very important, since the element of time is critical in contextual analysis. Lastly, these cases clearly illustrate the role that contextual factors play in the way the processes of applying a security policy take place within different organisations.

The processes described in the two cases can be compared as for their '*shape, character and incidence*' (Pettigrew, 1997) with patterns of events observed in other cases of security policies application. Furthermore, through these case studies we attempt to bring forth the underlying mechanisms that shape the processes involved in the application of a security policy. We believe that knowledge of these mechanisms and the identification of the contextual factors that influence the adoption of security policy, can help both researchers and practitioners to address critical issues in IS security management.

Description and analysis of the case studies

This section provides the description and analysis of the application of an IS security policy in two organisations. An overview of each case study is given, followed by a detailed analysis of the major issues pertaining the application of the security policy, based on the theoretical framework presented in earlier sections. The analysis of each case study involves a discussion of the content, the context and the processes involved in the formulation, implementation and adoption of the security policy.

The CTDI case: overview and findings

The Centre for the Treatment of Dependent Individuals (CTDI) is a non-governmental organisation operating for the last 17 years, that comprises more than 40 independent units (called "programmes") concerned with the prevention of drug abuse and the treatment of individuals with drug addiction problems. The CTDI keeps and processes, both manually and electronically, data concerning drug addiction as well as personal information on individuals who participate in its programmes. CTDI is bound by the National Data Protection Act to provide adequate protection for the personal data it keeps, and to have a security policy in place, for regulating the use and access to this information. As soon as the Data Protection Act came into effect, which was in 1998, CTDI invited an external group of security professionals to prepare an IS security evaluation study and make suggestions on security management issues. The external group, in which the authors participated, was assigned the project of evaluating the risk of the organisation's information systems and proposing guidelines for applying the designated security policy, based on the findings of the risk assessment. The suggestions included guidelines for security controls that should be applied for the protection of all information assets against the threats and vulnerabilities that were identified in the risk assessment. The suggestions also included alterations to the organisational structure that were required for the implementation of the proposed security management tasks and the application of the designated security controls. For the risk assessment of CTDI's information systems CRAMM was employed.

CTDI is organised in the form of a matrix, comprising of working groups that are formed by members from the different autonomous units that run the treatment programmes for drug addiction. These groups refer to the Board of Directors, in which all programmes' directors participate. Since the beginning of its operation, CTDI has also had a Committee for establishing a code of ethics and for managing ethical and other issues, that members of the CTDI face in their everyday activities and their interaction with external organisations and individuals. A major difficulty CTDI faced before establishing a security policy was requests for personal data on individuals with drug addiction who had participated in CTDI's programmes. These requests, often originating from public or governmental bodies, contradicted with the code of ethics and code of practice that the members of CTDI followed. Resisting the pressure from those requests was a difficult task for CTDI, due to the fact that although it is an autonomous and independent organisation, having the Board of Directors elected by its members, it receives most of its funding from the Ministry of Health.

When CTDI received the security guidelines, the Board of Directors declared their commitment to implement a security plan based on these recommendations. For implementing the security plan, new working groups were formed. These groups elaborated the security plan to meet the specific security needs and requirements that CTDI had. In this way, new work practices were established and the code of ethics and code of practice were accordingly adapted. It should be noted, however, that these codes were in the same direction with the security policy, so no major changes were required. Besides the new processes that were designed and the technical controls that were implemented, new norms and rules were also considered for the application of the security policy. The Board of Directors accepted and supported the recommendations made by the working groups and also created new organisational roles for the management of security, as was proposed in the security plan. The authors of the paper returned after some months to explore how the implementation of the security plan had progressed. The interviews that were carried out at that point revealed that the security policy was almost fully implemented, it was at the early stages of its adoption by the users and new work practices had already begun to establish.

Contextual analysis of the CTDI case

Overall, as a result of the implementation of the security policy in CTDI, its members were able to handle both external and internal requests for personal information on individuals with problems of addiction in a coherent manner and could base their actions on the directions of the formal security policy, which was adopted at its entirety. Moreover, the application of the security policy strengthened the inclination of the employees to follow the internal code of ethics, while new work practices with regard to the handling of sensitive personal information were developed. Although a formal code of ethics pre-existed, the introduction of the security policy promoted and helped the development of a security culture and broader security awareness. Table 3 presents the critical issues pertaining the successful formulation, implementation and adoption of the security policy that have been identified by our analysis, in the case of CTDI.

The SSI case: overview and findings

The Social Security Institute (SSI) is a large organisation providing social security services to its beneficiaries, including old age and disability pensions, benefits for sickness, maternity etc. The SSI is regulated by the Ministry of Health and is accountable to the Treasury. The Director General of SSI is appointed by the government and this place is considered highly political. The organisation employs a large number of staff, and is geographically dispersed with more than 300 regional offices, besides its central administration offices. Despite the fact that regional offices have a high level of autonomy in conducting their operations, such as collecting insurance contributions and issuing decisions on insurance benefits, the SSI operates under a bureaucratic and highly centralized management.

Since its establishment, many decades ago, several attempts have been made to introduce information technology and the use of information systems to the operations of SSI, mainly as a means to lift its major dysfunctionalities, to reform its structure and to enhance the quality of the services it offers (Avgerou, 2002). In general, all major IT projects in the past progressed very slowly and their results were significantly distant from their initial specifications. In fact, successive unsuccessful attempts to introduce the use of computer systems worsened operational efficiency of the SSI and also worsened the work conditions for its employees.

As in the case of the CTDI that was described in the previous section, the trigger for launching a security management initiative, which mainly entailed the formulation and implementation of a security policy, was the obligation of the SSI to comply with the National Data Protection Act, since it stores and processes personal information for its beneficiaries. Under this obligation, the management of SSI assigned the project of performing a risk analysis and formulating a set of security management guidelines to an external team of security professionals. At the time when this group, in which the authors participated, commenced with the project, a major Information System Development Project, that SSI had outsourced to a private software company, was at its final testing stage. The development of the Integrated Information System (IIS), as it was named, was intended to provide the SSI with an integrated platform that would support most of its operations, both at its central establishment as well as at the regional and local branches. Besides the operation of the IIS, a number of other independent applications were also in use, some of which would continue to run in parallel with the new information system, whereas the rest would be gradually abandoned.

The generic security guidelines that were proposed by the external security professionals were based on the outcome of a risk analysis and evaluation process that was conducted by applying the CRAMM risk analysis and management method. This task involved numerous interviews with IS users, members of the IT department and members of the private software company that was developing the applications. The outcome of the security evaluation was then presented to the management of SSI, who commented on the risk assessment findings, provided their guidelines for prioritising the recommended countermeasures and requested specific instructions on how to accommodate the organisational hierarchy in order to assign the new roles that were proposed (e.g. the new role of the Security Officer) and the new responsibilities to existing roles. Finally, after all requested revisions and comments had been accommodated, the management of SSI adopted a security plan and launched the process of applying the security policy, declaring its commitment and will to support their implementation. The responsibility for the formulation and implementation of the security policy was assigned to the IT department.

The authors revisited SSI after a period of about 15 months in order to explore the progress of the implementation process of the security policy and the level of its adoption by the users. The interviews that were conducted with members of the SSI showed that the process of implementing the security policy was at very early stages. Applying the framework for analysis described above, the authors came to the conclusion that this was due to a variety of reasons, including: (a) lack of experienced or qualified personnel who could drive

Table 3 Contextual analysis of the CTDI case

Dimensions	Description
Content	Organisational level: • A new role, the Security Officer, referring to the Board of Directors was established. Work system level: • Work practices were reformulated as a result of the security policy implementation. • The members of CTDI who were assigned security responsibilities enhanced their knowledge on IS security and protection issues. • New practices were developed in order to accommodate required security management activities such as: monitoring the security policy and controls and keeping them up to date, handling security-related incidents, developing security awareness and providing security training. Information technology level: • Special software was used for encrypting personal information of addicted individuals that was kept in electronic files. • Special locks were used for the protection of non-electronic files.
Context	Outer context: • Legal and regulatory requirements with regard to data protection were fulfilled through the implementation of the security policy. • Relationships and interaction with external bodies and individuals is now based on new rules. • The trust relationship with individuals who participate in the programmes of CTDI has been strengthened and now is based on a formal basis. Inner context: • The code of ethics that had previously existed has been reinforced through the formulation and implementation of the security policy. • Organisational culture has been enriched with security and privacy concerns.
Process	Cultural perspective: • A common language and understanding on security issues has been developed due to the participation of CTDI members in working groups for the formulation of the security policy. • The members of the CTDI can now draw on the guidelines of the security policy for forming their response to external organisations requesting personal information on addicted individuals. • The members of CTDI adopted new norms for handling the personal data on individuals with drug addiction problems. Power perspective: • The Board of Directors allocated adequate human resources and funding for the implementation of the security policy. • The Directors of each programme took up the responsibility for complying with the security policy.

the processes of security policy formulation and implementation, (b) lack of organisational flexibility that would enable the recruitment of individuals with these qualifications, (c) the IT personnel was overwhelmed with the effort of putting the IIS in productive use, having at the same time to provide training to the users, (d) although the management of SSI had initiated the introduction of a security policy, there was lack of active involvement and effective support. Despite all this, however, the members of the IT department had included a number of security guidelines from the security policy in their agenda, and tried to adapt their activities accordingly, whereas the level of security awareness among users remained very low but slowly growing.

Contextual analysis of the SSI case

The application of a security policy emerged as a necessity for the Social Security Institute, resulting from its obligation to comply with legal regulations on the processing of personal and sensitive personal data. The higher management of the SSI stated their commitment to the realization of the security policy in order to comply with the legislation, but no linkage was made between security and the overall strategy of the SSI. The need for formulating a security policy originated from requirements that were posed from the environment of SSI (outer context). Despite the commitment expressed by the management, no significant progress with regard to the implementation of the security policy has been achieved several months after the security policy was formulated and the required security measures were identified. The lack of flexibility in employing qualified personnel and altering the organisational structure, due to the highly bureaucratic nature of the SSI, hindered the security policy implementation process. On the other hand, the competitive relationships and the unbalanced workload of the IT personnel also posed obstacles for the effective implementation of the security policy. In SSI, usage of information technology by the employees is being supervised by the IT department; users in general are reluctant to use or misuse the applications. Moreover, there is a clear lack of understanding from the side of the users, on the issues of IS security in general and the formulation and use of a security policy in particular. However, no awareness or employee education programmes have been undertaken, due mainly to the rigidness of the organisations and its inability to employ people with indicated qualifications. The overall level of security awareness among the employees of SSI seems to change very slowly, as a result of the introduction of the security policy. Table 4 summarizes the key findings from the analysis of this case.

Findings and conclusions from the case studies

The analysis of the two cases has provided us with indications on how the processes of formulating and implementing an IS security policy are affected by the different contexts within which they take place, as well as by the power relations and cultural elements developed in different organisations. In this section we summarize our key findings from the two case studies described above. Although these findings cannot be statistically generalised to a broader category of cases, however, we believe that they can be useful to practitioners and researchers, by providing an insight to the process of security policy application and by bringing forth significant contextual elements that have not been adequately investigated.

We believe that the *organisational structure* plays an important role for the successful implementation and adoption of a security policy. Organisations with employees who participate in various activities and have increased responsibilities are more likely to develop a security culture and establish a high level of security awareness among their personnel. A rigid hierarchical structure may be a problem for information security management since the application of a security policy often requires organisational flexibility, including the creation of new roles or the adaptation of existing ones.

Organisations with a coherent *culture*, especially when their employees follow a code of practice or code of ethics, are also in a better position for implementing and adopting an IS security policy. The successful adoption of a security policy requires that a common understanding and shared meanings be developed among employees; this is facilitated by the prior experience of following a common code of practice. Other researchers, as well, underline the critical role that codes of ethics/good practice/conduct play in the effective IS security management (Gritzalis, 1997; Trompeter and Eloff, 2001; Warren, 2002).

Another issue that is of major importance is the active participation and visible support provided by the *management* of an organisation. As the two case studies have showed, formulating and implementing a security policy usually entails a great amount of overhead work, not only by the IT personnel, but also by the IS users who have to take up new work practices and abandon or alter old ones. For this reason, the emphasis that the management places on the issue of IS security can significantly affect the outcome of the endeavour to apply a security policy. With regard to management, our research also indicates that the existence of an accordingly qualified, motivated person (usually appointed to the role of the *Security Officer*), who can lead the processes of formulating and implementing the security policy, can also help towards successful implementation and adoption. On the other hand, users are also more likely to adopt the guidelines and procedures of the security policy when the policy is aligned to their professional goals and contributes to fulfilling their duties more effectively.

Last, but not least, we believe that an ongoing security *awareness* programme, together with the continuous evaluation of the effectiveness of the security policy can also promote its successful implementation and adoption. Fig. 5 depicts all major contextual factors that have been identified in the analysis of the cases.

Conclusions and further research

This research was triggered by the need to explore the dynamics of applying IS security policies in

Table 4 Contextual analysis of the SSI case

Dimensions	Description
Content	Organisational level: • New roles were difficult to be created or assigned to the existing personnel. • The management claimed that this was due to difficulties in employing adequately qualified personnel. Work system level: • Work practices were slightly differentiated, users developed limited security awareness. • The members of the IT department carried out security management tasks (e.g. passwords management, logs monitoring etc.), besides their current ones, in an ad hoc way. Information technology level: • The implementation of security controls requires a long time and entails many bureaucratic procedures. • No significant changes were made to the IT infrastructure.
Context	Outer context: • Legal and regulatory requirements (European Directives and the national legislation) with regard to data protection were fulfilled through the implementation of the security policy. Inner context: • Competitive relationships were reinforced by the introduction of new roles and responsibilities.
Process	Cultural perspective: • Users acknowledged the need for protecting the IS, but had a negative attitude towards using many security controls, out of fear, lack of understanding and distrust to technology. • The level of security awareness among users remained very low. Power perspective: • The IT personnel requested more resources for implementing the security guidelines and controls. • Although the SSI management considered the issue of IS security as highly important, it failed to support in an adequate and effective way the implementation of the security policy.

organisations. Hardly any empirical accounts on the issues of implementing security policies exist. Furthermore, not any substantiated research on the factors affecting the successful implementation and adoption of an IS security policy can be found in the IS security literature. This paper has attempted to illuminate the mechanisms behind the formulation and implementation of IS security policies and relate these with the context within which they take place. We believe that the general conclusions we have drawn by the two studies, although they are not statistically generalised, can have implications in the areas of IS security management and especially in the development and use of IS security policies. These conclusions can be taken as starting points for further research on the topics of IS security policies development and use, as well as for the equally important issues of developing security awareness and the users' involvement in these processes.

We have also proposed a theoretical framework for analysis based on the theory of contextualism which has not been, up to now, applied in IS security research. We believe that the IS security literature will benefit from widening the range of research methods and theories available to researchers. Moreover, we believe that the theory of

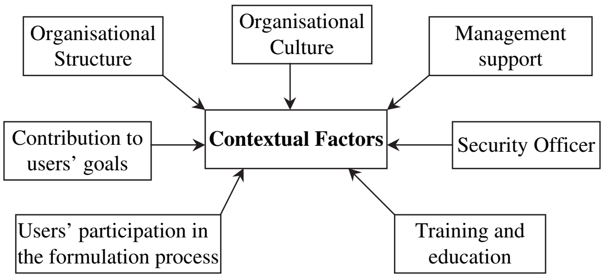

Figure 5 Contextual factors for the application of IS security policies.

contextualism can help illuminate several issues with regard to the practical impact of IS security that have not been explored yet. Thus, we think that the suitability of contextualism and other social oriented theories that are employed in the IS field and other related areas, such as organisation theory, should be further looked into.

Acknowledgements

The authors would like to thank the management and employees of the SSI and CTDI for their help and valuable contribution to our research.

References

Alter S. A general, yet useful theory of information systems. Communications of the Association for Information Systems 1, 1999. Article 13.

Ammeter A, Douglas C, Gardner W, Hochwarter W, Ferris G. Toward a political theory of leadership. The Leadership Quarterly 2002;13:751—96.

Avgerou C. Information systems and global diversity. Oxford University Press; 2002. p. 152—74.

Baskerville R, Siponen M. An information security meta-policy for emergent organizations. Journal of Logistics Information Management 2002;15(5/6):337—46.

Benbasat I, Goldstein D, Mead M. The case research strategy in studies in information systems. MIS Quarterly 1987:369—86.

Björck F. Security Scandinavian style. Interpreting the practice of managing information systems in organisations. Ph.D. thesis. Stockholm University and Royal Institute of Technology; 2001.

Dhillon G. Managing information system security. Macmillan Press; 1997.

Eisenhardt K. Building theories from case study research. Academy of Management Review 1989;14(4):532—50.

Eloff M, von Solms S. Information security management: a hierarchical framework for various approaches. Computers and Security 2000;19(3):243—56.

Gritzalis D. A baseline security policy for distributed healthcare information systems. Computers and Security 1997;16(8): 709—19.

Höne K, Eloff J. Information security policy — what do international information security standards say? Computers and Security 2002a;21(5):402—9.

Höne K, Eloff J. What makes an effective security policy? Network Security 2002b;6(1):14—6.

Jarvinen P. Research questions guiding selection of an appropriate research method. In: Hansen HR, Bichler M, Maher H, editors. Proceedings of the eighth European conference on information systems. Vienna University of Economics and Business Administration; 2000.

Karyda M, Kokolakis S, Kiountouzis E. Redefining information systems security: viable information systems. Proceedings of the 16th IFIP international conference on information security (SEC 2001), June 2001, Paris, France: Kluwer Academic Publishers; 2001.

Karyda M, Kokolakis S, Kiountouzis E. Content, context, process analysis of IS security policy formation. In: Gritzalis D, et al, editors. Security and privacy in the age of uncertainty, Proceedings of the 18th IFIP international conference on information security. Kluwer Academic Publishers; 2003.

Mintzberg H. The organization as political arena. Journal of Management Studies 1985;22:133—54.

Peltier T. Information security policies and procedures: a practitioner's reference. CRC Press; 1999.

Pettigrew A. Context and action in the transformation of the firm. Journal of Management Studies 1987;24(6):649—70.

Pettigrew A. What is processual analysis? Scandinavian Journal of Management 1997;13(4):337—48.

Pettigrew A, Whipp R. Managing change for competitive success. Blackwell; 1993.

Siponen M. A conceptual foundation for organizational information security awareness. Information Management and Computer Security 2000a;8(1):31—41.

Siponen M. Policies for construction of information systems' security guidelines. In: Qing S, Eloff JHP, editors. Information security for global information infrastructures. Kluwer Academic Publishers; 2000b. p. 112—20.

Siponen M. Designing secure information systems and software Ph.D. thesis. University of Oulu, Oulu University Press; 2002.

Symons V. A review of information systems evaluation: content, context and process. Journal of Information Systems 1991; 1(3):205—12.

Trompeter C, Eloff J. A framework for the implementation of socio-ethical controls in information security. Computers and Security 2001;20(5):384—91.

UK Central Computer and Telecommunications Agency. CCTA risk analysis and management method: user manual. London: HMSO; 2002. Version 5.0.

Walsham G. Interpretive case studies in IS research: nature and method. European Journal of Information Systems 1995;4: 74—81.

Walsham G, Waema T. Information systems strategy and implementation: a case study of a building society. ACM Transactions on Information Systems 1994;12(2):150—73.

Warren M. Security practice: survey evidence from three countries. Logistics Information Management 2002;15(5/6): 347—51.

Whitman M, Towsend A, Aalberts R. Information systems security and the need for policy. In: Dhillon G, editor. Information security management: global challenges in the new millennium. Idea Group Publishing; 2001.

Wood C. Security policies made easy. Baseline Software; 1999.

Wood C. An unappreciated reason why security policies fail. Computer Fraud and Security 2000;10:13—4.

Yin R. Case study research: design and methods. Sage Publications; 1994.

Maria Karyda is currently a doctoral candidate at the Department of Informatics, Athens University of Economics and Business, Greece. She obtained a B.Sc. in Informatics and M.Sc. in Information Systems from the same university in 1998 and 2000, respectively. Her research interests include organizational aspects of information systems security management, the use and application of security policies and security culture and awareness.

Evangelos Kiountouzis is a Professor of Information Systems with the Department of Informatics of the Athens University of Economics and Business, Greece. He studied Mathematics at the University of Athens, Greece, and received a PhD in Informatics from the University of Ulster, UK. His professional and research interests focus on information systems analysis and design methodologies and on information systems security management. He is the author of several books on the topics of information systems and information systems security management and he has published numerous papers in international conferences and journals.

Spyros Kokolakis is a lecturer at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a B.Sc. in Informatics from the Athens University of Economics and Business in 1991 and a Ph.D. in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis, and security policies design and implementation. He is a member of IEEE and ACM.

Available online at www.sciencedirect.com

SCIENCE DIRECT®