CONTENT, CONTEXT, PROCESS ANALYSIS OF IS SECURITY POLICY FORMATION

Maria Karyda[1], Spyros Kokolakis[2], Evangelos Kiountouzis[1]
[1]*Athens University of Economics and Business, 76 Patission Str., GR-10434 Athens, Greece. Email: {mka,eak}@aueb.gr, voice: +30-210-8203555, fax: +30-210-8237369.*

[2]*University of the Aegean, GR-83200 Karlovassi, Samos, Greece. Email: sak@aegean.gr, voice: +30-22730-82233, fax: +30-22730-82009.*

Abstract: Security management is now acknowledged as a key constituent of Information Systems (IS) management. IS security management traditionally relies on the formation and application of security policies. Most of the research in this field address issues regarding the structure and content of security policies; whereas the context within which security policies are conceived and developed remains rather unexplored. However, security policies that are formed without taking into account the specific social and organisational environment within which they will be applied, are often proven to be inapplicable or ineffective. In this paper we explore the issues pertaining to the formation of security policies under the perspective of *contextualism*. Within the framework of contextualism, we study the context, content and process of IS security policies development. This paper aims to contribute to IS security research by bringing forth the issue of context-dependent formation of security policies. In addition, it provides a contextual framework, which we expect to improve the effectiveness of IS security policies development.

Key words: Information systems, information systems security, contextualism.

1. INTRODUCTION

In the last decade security issues have emerged to the top of the Information Systems (IS) management agenda. Practice has shown that security tools and mechanisms alone cannot provide adequate protection to

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

modern ISs. Tools and mechanisms should be incorporated into a comprehensive *IS security policy*, i.e. a structured set of principles, strategies and detailed guidelines for the protection of an IS.

Several approaches have been proposed for the design of security policies, with *risk analysis* [ISO, 1996] being at present the most frequently used. Most of the research in this field is concerned with issues regarding the structure and content of security policies, whereas the context within which security policies are conceived and developed remains rather unexplored. However, security policies that are formed without taking into account the specific social and organisational environment within which they will be applied, are often proven to be inapplicable or ineffective.

In this paper we consider the development and application of security policies in their social and organisational context. Under this perspective we propose a framework with three dimensions, i.e. *context*, *content* and *process*, to support the development and application of security policies. Moreover, based on the experience gained from several security policy development cases we identify specific factors in the social and organisational context that play an important role in the development and application of security policies.

2. INFORMATION SYSTEMS SECURITY MANAGEMENT AND SECURITY POLICIES

2.1 IS Security Management: What kind of problem is it?

Security concerns have been of primary importance for firms and organisations, since most organisational activities have come to depend heavily on information and communication technology. Moreover, current reports show that the number of security related incidents and consequent financial losses increase in magnitude, as well as in severance [CSI/FBI, 2002]. Security problems, in most of the cases, have been addressed by means of technical solutions, i.e. tools and mechanisms, such as intrusion detection and access control mechanisms.

An IS, however, should not be studied with a focus on its technical dimension only. ISs comprise a set of diverse elements, namely information, software, hardware, procedures and people, all of which interact with each other. IS security, therefore, aiming to protect all its comprising elements, as well as its entity and unobstructed functionality, involves a wide range of actions, which are of quite different nature. For example, training and

awareness programs can be part of an IS security policy, to ensure that people involved in the operations of the IS take all appropriate actions to prevent disclosure of sensitive information and to reduce the probability of unauthorised use of software or hardware. Similarly, installation of special purpose software, such as anti-virus or network monitoring tools, could also be a part of the activities aiming to protect an IS.

It is evident, therefore, that technical methods on their own can neither adequately nor sufficiently provide for the security of an IS. Information systems security management, therefore, should also encompass other means of action, i.e. managerial activities, such as auditing and control, and human resource development activities, such as education and training, besides the employment of technical methods. The need for abandoning a 'pure' technical viewpoint in favor of a 'socio-technical' or even 'social' standpoint has, in the recent years, been acknowledged by a significant number of authors in the area of IS security research [Dhillon, 1997 and 2001, Dhillon and Backhouse 2001, Hitchings, 1995, Trompeter and Eloff, 2001, von Solms 2001]. We argue that the socio-technical analysis should not be restricted to the process of security policy formulation and its content. It should also include the analysis of the IS context.

2.2 Security policies as a major IS security management instrument

With regard to security, management at the IS level faces a complicated and ill-structured problem domain. Most widely-adopted security management methods and tools (such as firewall systems, network monitoring tools, risk analysis methods, security evaluation criteria, encryption mechanisms) share a common 'technical' point of view, thus overlooking, most of the times, the social and organisational aspects of IS security.

Faced with a great variety of security threats, organisations develop and put in action security policies. A security policy, in general, might have a different meaning for different people. Nevertheless, for the purposes of our research, we consider a security policy to be a high-level statement of the goals and objectives with regard to security, as well as the description of the general means for their attainment.

In this way, the formulation of security policies constitutes one of the most important 'tools' IS management employs, in order to address the issue of IS security. However, whereas needs and problems regarding the security of individual IS components (such as servers, workstations, files or networks) may be easy to identify and evaluate, there is no single security solution, nor a single security policy that can fit all organisations, since

many security issues are organisation-specific and emerge in the organisational environment at a certain point of time.

There exist many ready-made, skeleton-type security policies, as well as standards that can be used as a reference guide or compliance target [ISO 17799]. However, researchers [Wood, 2000] as well as industry, i.e. [Control Data Systems Inc., 1999] still face the issue of 'why security policies fail'. A great variety of reasons and explanations have been put forth, such as that security controls constitute a 'barrier to progress' [Control Data Systems Inc., 1999], or that security policies are very likely to be circumvented by employees in their effort to perform efficiently their tasks [Wood, 2000].

3. THE SOCIO-TECHNICAL NATURE OF IS SECURITY POLICIES DEVELOPMENT

Despite the fact that security policies at the organisational level are a well-considered issue by a great number of organisations, there are still a number of factors that pertain the formulation and application of security policies and ultimately affect their success, which remain open issues and are still unexplored. Some of these issues, are presented in the following list:

a) What is the area of responsibility for the organisation with regard to IS security? In other words, who is responsible for the security of the IS?
b) Which management practices should be employed when developing and implementing an IS security policy?
c) What are the 'drivers' behind the formulation of security policies; who are the stakeholders and which factors should the author of the security policy take into consideration?
d) Which are the factors that may affect the implementation of a security policy and how can they be managed, so as to result to a 'successful' implementation?

We believe that one of the reasons that a great number of issues related to the formulation of security policies, still remain unresolved, is that current approaches to IS security policies mainly focus on the *content* of a security policy, but overlook two other aspects: the *context* and *process* of the formulation of a security policy, which are further analysed in Section 5.

4. CONTEXTUALISM IN INFORMATION SYSTEMS AND IS SECURITY RESEARCH

Information Systems is an interdisciplinary academic field, drawing from both systems engineering and social sciences, that is characterised by

methodological pluralism [Avgerou, 2000]. Having in mind that IS security is a 'socio-technical' problem [Dhillon, 1997], we argue that it is well justified to enrich our approaches by employing an approach widely used in the area of IS research, which is *contextualism.*

Contextualism [Pettigrew, 1985] is an interpretive approach, which provides a framework for understanding, within the realm of subjectiveness [Dhillon and Backhouse 2001]. In the IS field, contextualism has been adopted by several researchers. Walsham [1993] applies this methodological approach, combined with structuration theory, in order to explore the context and process of organisational change. Symons [1991] uses the framework of contextualism to build a categorization of the IS evaluation literature. Pettigrew and Whipp [1993] apply the same framework to capture a holistic image of the link between strategic change and competition, with regard to British firms. As depicted in Figure 1, the contextualist point of view acknowledges the importance of the content in all organisational activities, but also gives emphasis to the process that has resulted to these activities, as well as on the context, the surrounding environment, within which these activities are formulated and carried out. From the contextualist perspective the process, content and context are closely interrelated and they should be studied jointly, in order to understand issues, such as organisational change.

Hence, employing contextualism in the formulation of IS security policies aims to enhance our understanding, which has been intrigued by questions like the ones listed in Section 3, but not to provide explanations.

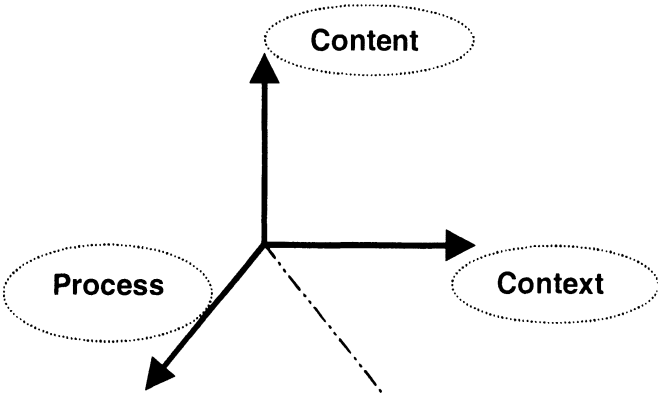

Figure 1. The framework of Content, Context, Process

5. CURRENT APPROACHES TO IS SECURITY POLICIES

Though most approaches used for the formulation of security policies address principally the technical aspects of security, a significant stream of

research acknowledges also the importance of human-related and organisational-dependent dimensions of the process of security policy development. Research in this stream stresses the need for considering IS security management from a 'socio-technical' point of view and encourages further investigation under this perspective (e.g. Siponen [2000], Baskerville and Siponen [2002], Peltier, [1999].) Other researchers, in order to offset the technical bias, propose a systemic-holistic approach, e.g. Yngstrom [1995], Kiountouzis and Kokolakis [1996].

Siponen [2000] classifies security policies into two categories, namely 'technical' and 'organisational', stating that the level of maturity of research regarding 'people-oriented/non-technical' policies is quite low, compared to research on computer-oriented policies. The vast majority of currently employed approaches to security policy place great emphasis on the content of the policy; this mostly has to do with the description of procedures that provide for the security of the 'target' system, may it be a network, an operation system, a computer etc. Little or no attention at all, is paid however to other factors that could affect the formation and application of the policy and which are related to the social or organisational surrounding of the 'security target'. Moreover, with the exception of some training and educational activities that are usually included in the security policy, no mention is made of the ways the policy is communicated to the users and other personnel involved with the operations of the IS.

Modern organisations however, which rely heavily upon their informational infrastructure, need a comprehensive security policy, that will address all issues concerning IS security, by taking into account both their technological environment and the specific features of the organisational domain they operate in, as well as their unique culture.

It is evident that current approaches to the formation of security policies fail to face issues that affect the formation and application of the policy and stem from the organisational and social context, thus failing to meet current organisational needs for integrated IS security management.

6. APPLYING THE CONTEXTUALIST FRAMEWORK

In the following paragraphs we analyse the three dimensions of the framework presented above. In order to achieve this we have examined nine cases of organisations that have developed a security policy in the period 1997-2002 [Lambrinoudakis et al., 2001]. These include six government organisations, one non-governmental organisation and two private enterprises, in the areas of petroleum trade and pharmaceutics.

In these cases the authors were involved as consultants assigned the task of developing an IS security policy. Several variations of risk analysis were employed gradually adding elements of contextual analysis to the rather technical risk analysis methodology.

This was the first phase of the empirical research. In the second phase, the authors surveyed the security policy implementation in the above organisations. Several interviews were conducted with key persons that were involved in the implementation stage with the aim to identify the factors that affect the success of the security policy. Consequently, these factors were categorised in the three dimensions of the contextual framework presented in Figure 1.

6.1 IS Security Policies: Context

Context can be distinguished into social, organisational and technical. The majority of the currently employed methods for developing security policies provide the means for the analysis of technical context. However, the organisational and social contexts are equally important for the effective application of security policies. The main issue remains to identify the elements of the social, organisational and technical context, which are critical for the successful development and application of a security policy.

In order to identify these elements we have relied on the empirical study presented above. Throughout these nine cases, the authors have interviewed key persons in the operational, tactical and strategic managerial level. Through these interviews, several key issues with regard to the effectiveness of IS security policies have emerged. Then, reflecting upon the empirical evidence we have elicited a set of generic elements, which are presented in the following tables.

Table -1. Social context

Contextual elements	Description
Ethical considerations	Users would not accept policies that contradict to their ethical principles. Policy developers should be aware of any such conflicts and seek for consensus.
Legal and regulatory constraints	In the last decade there has been a plethora of laws concerning data processing and ISs in general, e.g. regulation on personal data protection, intellectual property protection etc. Thus, the legal and regulatory framework may be quite complex and need thorough examination before a security policy is launched.
Power structure and politics	Security policies control the access to and use of information, which is a significant source of power. It should be expected that the security policy would be at the center of the political arena. No matter how technically brilliant it may be, it is bound to fail, unless it finds political support.
Communication structures	For a security policy to succeed, it needs to be properly communicated to stakeholders. If it is expressed in a too technical language, it may be received with doubt.
External stakeholders	With this term we refer to stakeholders which are outside the organisational boundaries. They may be clients, consumers' organisations, data protection authorities etc. It is often the case that stakeholders exercise significant influence to policy making.

Table -2. Organisational context

Contextual elements	Description
Management structure	Management structure is usually depicted in the organisational chart. Policy developers should examine whether the current management structure is able to support the application of the security policy. Otherwise, re-structuring may be required.
Organisational culture	Norms and practices prescribed within a security policy usually require some sort of change in the way people perform their organisational activities. Flexibility to change, however, is closely related to the organisational culture that may or may not favour changes.
Motivation	Policy developers should consider the motives, which have led to the decision to develop a security policy.
Structures of responsibility	Policies should address the question: who will take responsibility for the implementation of the policy? Without unambiguous allocation of responsibilities, policies run the risk of remaining inactive.
Internal stakeholders	Stakeholders within the organisation, IS users in particular, may resist the implementation of a security policy. Therefore, their acceptance is also important.

Table -3. Technical context

Contextual elements	Description
IS technical elements	Hardware, software and data, with their relationships, lie at the core of the technical context.
Plans for future developments	Since ISs rarely remain static, policies should take into account any plans for future modifications to the current system or the development of new systems.
Threats and vulnerabilities	Threats exploit vulnerabilities to cause damage to the assets of the IS. Threats may be of human origin, or they may be related to physical disasters, technical failures etc.
Technology trends	Since technology evolves continuously, current technology trends need to be taken into account, in order to expand the life period of the security policy.
Currently available security technology	The selection of technical countermeasures should consider the current state-of-the-art.

6.2 IS Security Policies: Content

A wealth of resources, including sample policies, baseline policies and lists of measures, is available to policy developers. In the following table, we delineate the issues that should be covered by a security policy.

Table -4. Content

Categories	Description
Organisational re-structuring	In most of the cases a new organisational framework needs to be established, in order for the security policy to be implemented successfully.
Administrative procedures	A broad category of procedures is included in security policies, comprising personnel related procedures, system administration procedures etc.
Terms and concepts	Establishing and elucidating the conceptual framework of the security policy appears as a prerequisite for the effective communication of the policy.
Awareness, education, training	Awareness, education and training constitute an important element in a security policy, since the levels of security awareness in the public remain low.
Technical measures and tools	Security goals stated within a security policy are achieved by applying a set of technical measures and tools, which are prescribed within the security policy.
Policy evaluation, monitoring and review	Procedures and criteria for the evaluation, continuous monitoring and reviewing in designated time, should also be part of a security policy.

6.3 IS Security Policies: Process

6.3.1 Development process

Several methodologies for the development of security policies are currently available. It is not within the scope of this paper to review them or to propose yet another methodology. However, we may suggest that regardless of the methodology adapted, the process of developing a security policy should employ a contextualist view, by including the following tasks:

- Define the problem.
- Obtain stakeholders' support and resources for the development and implementation of the policy.
- Analyse the social, organisational and technical context by recognising the aforementioned factors (see Tables 1 to 3).
- Define the content of the policy.
- Define evaluation criteria, monitoring processes, review and update procedures.
- Develop an implementation plan.
- Evaluate impact on social, organisational and technical factors due to planned changes introduced by the security policy.

6.3.2 Implementation, monitoring and maintenance

It is often the case that security policies remain inactive or are rendered ineffective. This justifies the need for a strategy that will guide the implementation of the policy, also covering issues such as monitoring and maintenance of the policy. Although there are currently no methods to guide this process, we may provide an indicative list of factors to be considered.

- **Implementation**: Who will have the responsibility to implement the security policy (e.g. Security Officer, System Administrator)? What means will be employed for this purpose? When is the appropriate time for the implementation of each module of the policy? What are the priorities for the implementation?
- **Acceptance**: How will the policy be communicated and acceptance will be obtained?
- **Contextual integration**: How to overcome hindrances stemming from the social, organisational and technical context?
- **Evaluation and monitoring**: Which are the criteria and the processes that will be used for the evaluation and monitoring of the effectiveness of the policy?

- **Review**: Which are the procedures for reviewing and updating the policy?

7. SUMMARY AND CONCLUSIONS

In this paper we have explored the relationship of the security policy formation with the environment within which the policy shall be applied. For this reason we applied the perspective of contextualism to a set of nine cases of organisations (including government and non-government organisations, as well as private companies) that have developed a security policy in the period 1997-2002. In these cases, at which the authors were involved as consultants, several variations of risk analysis were employed, gradually adding elements of contextual analysis to the rather technical risk analysis. In the aftermath, the authors studied the implementation of the security policy in the above organisations, by conducting several interviews with key persons that were involved in the implementation stage, aiming to identify the factors that affect the success of the security policy. These factors were then categorised in the three dimensions of the contextual framework presented in Figure 1. The conclusions resulting from our research include the following:

- the relationship between a specific organisational context and the security policy formation should not be overlooked when developing the policy;
- research and practice should pay equal attention to factors that characterise all three dimensions, namely the content, the context and the process of the policy formulation;
- most widely used approaches currently overlook the context of the policy, thus resulting in inapplicable and inefficient security policies.

This paper aims to contribute to IS security research by bringing forth the issue of context-dependent formulation of security policies. In addition, it provides a contextual framework, which we expect to improve the effectiveness of IS security policies development.

8. REFERENCES

Avgerou C. (2000), 'Information systems: what sort of science is it?', *Omega*, Vol., 28, pp.567-579, Elsevier Science Ltd.

Baskerville, R. and Siponen M. (2002) 'An Information Security Meta-policy for Emergent Organizations', forthcoming in *Journal of Logistics Information Management.*

Control Data Systems Inc. (1999) 'Why Security Policies Fail - White Paper' available at http://www.cdc.com

Dhillon G. (1997) *Managing Information System Security*, Macmillan Press Ltd.

Dhillon G. (2001) *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing.

Dhillon G. and Backhouse J. (2001) 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, Vol. 11, pp. 127-153.

Hitchings J. (1995) 'Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology', *Computers and Security* Vol.14, No.5, pp.377-383.

ISO 17799 Directory: Services and Software for ISO 17799 Compliance, ISO 17799 Audit, ISO 17799 Implementation and Security and Risk Analysis (also available at: http://www.iso17799software.com).

ISO/IEC/JTC1 (1996) Information Technology - Security Techniques - Guidelines for the Management of IT Security, GMITS, ISO/IEC DTR13335.

Kiountouzis E.A. and Kokolakis S.A. (1996) 'An analyst's view of information systems security', in *Proc. of the 12th International Information Security Conference (IFIP/SEC '96)*, Samos, Greece, May 1996, Chapman & Hall.

Lambrinoudakis C., Kokolakis S., Gritzalis D. (2001) 'Recurrent IT security issues and recommendations: learning from risk assessment reviews', in *Proc. of the Security and Control of IT in Society (SCITS-II), IFIP Conference*, Bratislava, Slovakia, June 2001.

Lindup K.R. (1995), 'A New Model for Information Security Policies', *Computers and Security*, Vol. 14, pp. 691-695.

Peltier T. (1999) *Information security policies and procedures: a practitioner's reference*, CRC Press.

Pettigrew A.M. (1985), *The Awakening Giant: Continuity and Change in ICI*, Blackwell, Oxford.

Pettigrew A.M. and R. Whipp (1993) *Managing Change for Competitive Success*, Blackwell.

Siponen M. (2000), 'Policies for Construction of Information Systems' Security Guidelines', *Information Security for Global Information Infrastructures*, Qing S., Eloff J.H.P. (eds.), pp. 112-120, Kluwer Academic Publishers.

Symons V. J. (1991), 'A review of information systems evaluation: content, context and process', *Journal of Information Systems*, Vol. 1, No 3, pp205-212.

Trompeter C. and Eloff J. (2001) 'A Framework for the Implementation of Socio-ethical Controls in Information Security', *Computers and Security*, Vol. 20, No 5, pp.384-390.

von Solms B. (2001) 'Information Security – A Multidimensional Discipline', *Computers and Security*, Vol. 20, No 6, pp. 504-508.

Walsham, G. (1993) *Interpreting Information Systems in Organisations*, J. Wiley & Sons Ltd.

Wood C. (2000) 'An Unappreciated Reason Why Security Policies Fail', Computer Fraud and Security, 10, pp. 13-14.

Yngstrom, L. (1995) 'A Holistic Approach to IT Security', in *Information Security - the Next Decade* (eds. Eloff, J. and S. von Solms), Chapman & Hall, London, pp.98-109.