29

Security Concerns for Contemporary Development Practices

A Case Study [*]

T. Tryfonas and E. Kiountouzis
Dept. of Informatics, Athens University of Economics and Business
76 Patission St., GR-10434, Athens, HELLAS
{tryfonas, eak}@aueb.gr

Key words: Action Research, Contemporary IS Development Approaches, Information Systems Security Design, Information Systems Security Practices

Abstract: This paper presents a case of application of an interpretive framework, which intends to formally integrate information systems security concerns within the information system's lifecycle. Aspects that are not normally taken under consideration, such as the involved stakeholders, the development approach and their implication to security issues, are introduced in such a way to benefit and empower the IS security design process. In the case presented here, the framework is used to extract a powerful process model description focusing on security concerns, so as to enlighten the work of the security designer significantly earlier before the use of risk analysis and the construct of a security plan or policy.

1. INTRODUCTION

New forms of communicating and trading require a robust and secure technical infrastructure in order to be performed and be fully exploited. In modern organisations assets can often be found in the form of data stored, processed and transmitted by information technology (IT) facilities, in the form of products, systems or applications; such data is a critical resource that

[*] Supported in part through YPER97 programme by the Hellenic Ministry of Development.

enables organisations to succeed in their mission. Stakeholders of those assets often require that dissemination and modification of any such information representations are properly controlled, as organisations or individuals have a reasonable expectation that their data remain private, be available to them as needed, and not be subject to unauthorized modification; this might stem from organisational requirements (company's regulations, organizational policies) or environmental necessity (market trends, data protection acts). Thus, there is an expectation from IT management to facilitate the identification and implementation of security controls to ensure that data are protected against potential threats. Traditionally, such security controls come up as a risk analysis (RA) result. This is a particularly effort-consuming process and it is usually performed after the information system's (IS) development. When applying such a practice, an "instance" (model) of the existing IS needs to be extracted, a fact that requires study of the system's structure and processes and constant contact with experienced users and designers. From this picture security specialists shall try to evaluate the organizational information assets, whilst at the same time they must validate each assessment with the system's stakeholders.

There are many RA approaches for system's security, most of which based upon the scientific paradigm, and are applicable along with similar development approaches. For example Downs, Clare and Coe (1992) study the relation between the CCTA Risk Analysis and Management Method (CRAMM) and the SSADM development methodology. They say that the former has been designed in a way that could be exploited in every development project that uses SSADM-like rationale. The technique that they imply is quite simple and has to do with the enrichment of the system's requirements ("Requirements Catalogue"), with the security requirements regarding the organizational assets, as they emerged through CRAMM's Stage-1. Further studies address this topic and present in detail the SSADM/CRAMM interface (Baskerville, 1993).

On the other hand, modern technology solutions are procured and developed in ways that they make extensive use of existing commodity IT products (i.e. hardware, operating systems, middleware, general-purpose applications, ERP systems, communication services etc.). Several developers and users of IT solutions lack the knowledge, expertise, or resources which are necessary in order to judge whether they may trust the security level of their IT components. In addition, traditional RA techniques are not particularly successful when facing such requirements that stem from the way contemporary systems are developed.

In this context, modern information systems should perform their functions whilst ensuring information protection against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The existing definitions for information security as the protection of confidentiality-integrity-availability, or IT security as the protection of the computational infrastructure, do not take under consideration "soft" factors within an IS, such as the human account, legislation, market requirements etc. There is a need for a comprehensive, systemic approach capable to resolve IS security issues, taking into account such important factors that cannot be traced through traditional practices. In the light of that assumption, the integration of systems security with modern IS development practices could be used to prevent and mitigate the previous or similar hazards. In the complex context of an IS, combining people, information, software, hardware and procedures, information technology security cannot ensure by itself the security of the entire system. IS security is indeed a broader term, containing all principles, regulations, methodologies, techniques and tools we establish and use to protect an IS, or any of its parts, from potential threats.

This paper validates a conceptual framework capable of resolving security problems within systems development; we briefly summarize the systemic approaches for IS security (section 2), we present an interpretive framework constructed to exploit such approaches and empower the IS security design (section 3), we introduce our research method (section 4) and eventually the case under study (section 5).

2. A BRIEF SUMMARY OF PREVIOUS RESEARCH

As an IS introduces managerial problems to the lifecycle of an organization, IS security problems should therefore be considered to be managerial and therefore be approached through problem solving techniques. Successful resolution is the procedure where a carefully designed and planned change takes place within an organizational context and becomes the body of relation between the present reality (problematic situation) with the desired ending (designed situation). Mumford (1998) sustains that action research is the most suitable way of resolving managerial problems, as the production of good theory cannot be done in isolation and without the involvement of the researcher to the organizational problems. Kiountouzis and Kokolakis (1996) argue that regarding information systems development there is a constant transformation of the analyst's way of thinking from the systemic to the systematic paradigm and vice versa, as like walking onto a Moebius band. The understanding and analysis of the problems is achieved by a systemic way, whilst the design and the implementation of the solutions through a well defined systematic way; thereafter the evaluation and assessment of the solution that shall lead to a possible success, failure or an IS redesign is achieved through systemic procedures, so as to document new requirements and start this process all over again. Similarly, IS security problems can be resolved only if the practitioners could continuously change their way of thinking from systematic to systemic and vice versa.

Existent methodologies for IS development do not meet the needs for resolving the security-related IS problems as most of them neither do include specialized handling of the security requirements nor can create a design for security controls early in the development process. In addition there are not many adequate studies for the exploitation of existing techniques and tools that could contribute to the formal and convenient integration of the security requirements within the IS development requirements (Hitchings, 1995a). Furthermore, the existing formalisation attempts (models, mathematical foundation) are limited in scope and cannot capture either in detail or in a comprehensive way the dynamics of the security concerns of contemporary information systems within the context of modern organisations and the technological progress (Kokolakis, 1996).

To cope with this Hitchings proposed a systemic theory for IS security design (Hitchings, 1995b); in particular her work, the *virtual methodology* (VM), along with the risk analysis method *Security By Analysis* (SBA) are two of the few systemic approaches for systems security. Such approaches seem to be the appropriate way of resolving problems, as within information systems "soft" factors (ethics, legislation, training, familiarization, user satisfaction etc.) are of major importance for its security and protection.

The VM takes under consideration the dynamic nature of the IS and the variations and uncertainty that the human factor introduces to it. Using the technique of consensus as used in the Soft Systems Methodology (SSM) (Checkland, 1981), where the establishment of designs is achieved upon agreement of the involved stakeholders, an organisation model is firstly introduced, then the IS model that corresponds to it and finally risks against them are defined. From that point and thereafter one can build up a control environment tailored to the particular organisational and informational needs.

A clearly systemic approach as well is the SBA risk analysis method. It was developed in Sweden and became an RA standard; it reflects the Scandinavian culture and attitude towards security aspects, as it is a product of an environment where the socio-technical design of systems flourishes. It is based on a thorough review of security breach scenarios, as they are identified through meetings amongst the various stakeholders. The control environment set-up comes through mutual agreements and consensus about what is important for the system (asset valuation) and what risks are there for those assets (risk assessment).

This approach tries to encapsulate all factors that have a potential security impact, as the meetings include every stakeholder (analysts, end-users, management etc.) and therefore each single perspective of the CATWOE analysis is included (Checkland, 1981). The previous term is an acronym referring to: the Customers of the system, the Actors involved, the Transformation of the input to the desired output, the Worldview under which the transformation has a meaning, the Owners of the system and the Environment. Ideally through that practice the stakeholders shall pinpoint the assets and the risks against them so as to design security countermeasures. The problem of such participatory approaches is that they need to be guided by extremely skilled analysts that shall act as facilitators of the entire process.

Information security problems in contemporary product/component oriented development practices could be resolved in the broader context of

QA assurance, since each single product could be validated and assured properly. Eloff and Von Solms propose a holistic approach based on the validation of products along with process assurance, combining both system components and system processes (Eloff and Von Solms, 2000). They argue that lack of quality assurance in IT production is the heart of the problem. However, assurance of high-quality development cannot by itself ensure security, as even the perfect product could be a subject to misuse.

Finally, Ynström (1999) proposes a systemic-holistic framework to approach IT security exploiting systems principles, control theory, SSM and cybernetics. Such theoretical frameworks are largely suitable for the resolution of security problems that are not strictly technical, but also other systemic ("soft"), factors could have an important role in a problematic situation.

3. THE NEED FOR A NEW FRAMEWORK

In the light of the previous systemic approaches information systems security design is viewed as the process that includes all tasks that aim to establish a mature level of security and protection for the information system as a dynamic comprehensive organisational subsystem. When designing a security plan for an organisation it is very important to rely upon a "rich picture" of the problem, i.e. an appropriate organisational model that shall help analysts to understand processes and focus on potentially problematic areas in designing safeguards. This model's operation is twofold as:

- On the one hand it is a means for validating common perceptions amongst the various stakeholders, and as a result the analysts can have a complete description of the organization.
- On the other hand it is the basis for the safeguards design, as it helps in tracing all deficiencies, potential risks etc.

Security design should be accomplished through disciplined ways, as this is a practice to ensure reusability of the results and of the gained experience and knowledge and have guidelines of how to deploy them in the future. The use of methodologies for system development and related issues (and therefore security) is necessary indeed because of the complexity and volume of such projects. There are strong arguments for choosing to do so, such as (Fitzgerald, 1998):

- The analysis of complex processes to easier to-be-handled sub-areas.
- The facilitation of project management.
- The reduction of the total uncertainty and of potential risks against the project.
- The facilitation of standardisation processes and repeatability of the method.

But many projects are implemented virtually without any methodological support due to limitations, such as:

- The great number of methodologies to choose from and an important lack of standardization of tools, deliverables and products.
- The fact that many are generalizations of theoretical or empirical research work and have not been properly validated with regard to whether they can be efficient and effective to other projects as well.

The information systems literature, in which the methodologies movement flourished in the eighties and early nineties, has not addressed sufficiently the new norms of practice and there should be introduced a classification of contemporary systems development practices along the well-known ‘make or buy’ divide (Tryfonas et al, 2000). Most systems projects are now anchored on the ‘buy’ maxim; on that, two development approaches are introduced namely the *single-product based* and *component-based* development. On the ‘make’ side we have proprietary development. Each of these three approaches introduces different challenges to developers, consultants and users (considered to be the high-level involved stakeholders in the framework, introduced in Table 1) regarding security concerns. A stakeholder is anyone involved in the situation that could gain benefits from it (Pouloudi, 1999).

Table 1: Integration of IS development with security issues (Tryfonas et al, 2000).

			IS SECURITY				
			ABSTRACTION LEVEL			EXPRESSION MODE	
			Strategy *(Appear in corporate strategic plan)*	***Design*** *(Embedded in development practices/methodologies adopted)*	***Implementation*** *(Embedded in acquired technology and products)*	*Explicitly declared security concerns*	*Implicit security understanding («metaphor») – Security is ...*
IS DEVELOPMENT	APPROACH	*Product-based*	All security concerns that appear and influence an organisation's planning; policies etc.	Securing techniques and methods that accompany systems development practices	Security tools and specific technologies, which are appropriate to be used when a particular method is selected.	All issues declared to be concerned with systems security within development approaches.	Security issues implied by the epistemology and the discipline followed (e.g. cultural concerns)
		Component-based					
		Custom/Proprietary					
	STAKEHOLDERS	*User organization*	Perception of the stakeholder for IS security in strategic level	Perception of the stakeholder for IS security in design level.	Perception of the stakeholder for IS security in implementation level	All declared statements of referenced organisations about security: describe their understanding of the subject.	All implied concepts concerning security within the referenced organisations.
		Developer organization					
		Consultant organization					
		Environment	Environmental influence on IS Security strategies.	Environmental influence on IS Security Design	Environmental influence on countermeasures implementation and use.	Explicitly recognized environmental influences (e. g. data protection acts).	Implicit influential parameters (market trends, user satisfaction etc.).

This interpretive framework is to be applied in development/research projects. Such kind of verification and redesign is a proper way of approaching organisational research problems related to information systems because it can collaborate the theoretical solution design phase with its practical application and evaluation through practice (Checkland, 1999). Systems theory and organisation theory for the inspection of the relation between the organisation, its IS and the IS Security, are very suitable approaches to this action research paradigm. These ideas along with SSM constitute the foundations of this theoretical framework. Those tools do not only resolve the problem of what technology to use and how to use it, but also address who require the solution, which get benefited from it and what could be the social, legal and political impacts of a design.

4. RESEARCH APPROACH AND METHOD OF INTERVENTION

An appropriate way of validating an interpretive theoretical design is by applying it to real-world cases and eventually refining it based on findings and gained experiences (Walsham, 1995). In general that kind of research (action research) includes active application of solutions/proposals and is a process that leads from practice to corresponding theory and vice versa (Eden and Huxham, 1996). This circular process begins with the informal understanding of the problem that leads to formal documentation of the theory that leads in consequence to resolution actions that can be verified across other similar cases and eventually introduce a robust theoretical framework for facing the problem.

Basic characteristics of action research are (Klein and Myers, 1999):

- It is an iterative and incremental approach.
- Intervention of the researcher to the cases under study is necessary.
- It is always context dependent.
- It produces customer-centred solutions.
- It is a process where generalization without thorough repeatability evidence is a rough to resolve issue and the validation of results is achieved through successful application to similar cases.
- When successful it reflects theory to a robust formal system.
- The presentation of results and findings is rather loose and quite radical.

Those principles lead to research conduct that deals with the heart of problematic situations and when they are successful they lead to production of real and viable theory construction.

5. THE CASE UNDER STUDY

The goal of the case under study was the implementation of a comprehensive security plan for the IS of a non-governmental non-profit organisation, offering treatment programmes for addictive individuals. In detail this project aimed at:

1. Modelling and documenting all information systems supported processes, especially those related to sensitive data.
2. Conduct of risk analysis for the IS.
3. Development of a security policy for the organisation.
4. Documentation of all security countermeasures.

Objectives (3) and (4) comprise the Security Plan and were the project's final deliverable.

5.1 Organization profile

The organisation under study is responsible of running eight different programmes to support addictive individuals (mainly drug-addicts and partially alcoholics). Its programmes are distributed all over the country, based on major cities. Stakeholders of the organisation are:

- The management.
- The staff and the major end-users of the IS.
- Program members and their families.
- The Ministry of Health and Social Security Affairs.
- The Data Protection Authority.

The model we shall construct shall introduce and present in detail processes within the organization that utilize information and could have potentially implications by a security incident, as well as all services to end-users, of any kind (drug addictives, researchers, therapeutists etc.). For the identification of security concerns depending on the type of the system (from the way it was developed point-of-view) and the involved stakeholders we shall combine the framework presented in Table 1 with a traditional risk analysis rationale (asset identification and valuation and potential risks against them) so as to facilitate the dissertation of the security plan.

The following sectors constitute concrete organization functions:

- Research sector,
- Treatment design and delivery sector,
- Administrative and financial services,
- Public relationships sector,
- Public awareness and forestalling unit,
- IS development and support sector, and
- Training sector.

5.2 Information system characteristics

The information system of the organization serves two major goals:

1. Financial and administrative support.
2. Support of research and of design of therapy, evaluation programmes and training.

To meet the second goal, processing of data considered to be sensitive (medical records, contact info of addictive individuals etc.) is required. Ensuring security of the sensitive data that the organization utilizes is a twofold necessity; on the one hand, legislation and the data protection act in Greece explicitly state that these data should be properly secured and on the other hand, trust is a major quality of such a kind of organization and therefore should be safeguarded at any cost.

The corresponding informational infrastructure for the organisational sectors and their processes shall be briefly introduced here; all workstations are interconnected PCs through two local area networks. One is for use by the financial administration services and one for use by the research sector. The information system consists of various independent applications and platforms that include an accounting package, office automation software, statistical analysis tools and custom applications. Those applications are hosted in a Windows NT/98/95 network (1 server, 22 w/s in the central building), 1 Novell network (accounting, 6 w/s), 1 independent Macintosh and four laptop computers.

Communication with third parties takes place through phone, fax and e-mail, the latter being provided by an Internet service provider through a dial-up connection. Informational support per process can be seen in detail in

Table 2, where we construct a security requirements-driven organisational process model.

5.3 Experiences and lessons learnt

Practitioners that try to resolve security problems of information systems should work their way towards it by developing common understanding between stakeholders by the use of and compliance with standards or other "disciplined" approaches (like risk analysis), a key role in which have:

(a) the efficient modelling of the organizational environment and

(b) the proper exploitation of those models extracted.

In the light of the previous argument, we could say that with regard to the case under study the proposed technique was rather suitable. The sensitive nature of the processed information and the organizational requirements were such that success could be achieved only through a systemic, disciplined way. There was an explicit statement of the need for a methodological support of the IS security design.

Modelling inscriptions of the processes and their association with security issues per development approach is a powerful tool in the process of security design because Representing the organizational activities, including models for an efficient description of involved roles and their corresponding perceptions and responsibilities and associating them with security issues, enlightens the security design at any time and especially facilitates the early integration of security concerns within the IS requirements/analysis and design phases.

Table 2: IS security requirements driven organisational process model.

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Administrative and financial services	Windows and Novell w/s with • accounting (package), • payroll system (package), • balance-sheets administration (custom-made)	management, staff	Financial data	• Corporate strategy compliance • Assurance of contracts • Control & audit • Security standards certification/compliance • Technology transfer (in-house) • Copyright protection (outsourced) • Concern for scientifically sound approach • Market acceptability
Training	Windows w/s with: • database applications (custom-made)	management, staff	Employee personal data, employee evaluations	• Integration to system specifications & requirements • Non-functional requirements • Risk prioritisation • System modelling plus risk analysis
Public relationships	Windows w/s for elementary word processing	management, staff	Press releases, journals,articles, announcements, newspapers etc.	
Research	Windows w/s with: • statistical analysis (package)	management, staff ministry of health, data protection authority	"Anonymised" sensitive data of subjects partaking in durg-addiction programmes	• Product's features configuration • System configuration features • Authenticity • Non-repudiation • Continuity of service • Access control • Authorizations
Treatment design and delivery	Windows w/s with: • full office automation applications (packaged solution)	staff, programmes members, data protection authority	Sensitive information (personalized contact info, medical records, other information)	
Forestalling	Windows w/s for elemantary word processing	staff, potential programmes members	Press releases, journals, published reports, articles, announcements etc	

6. GENERALIZATION OF CASE EXPERIENCES

Development practices and scenarios vary, so do practices of IS security. In general we can identify the following high level counter-practices:

- analysis of the system under study and risk assessment,
- set-up of a security policy,
- assurance that it complies with industry standards/laws,

- verification of the policy's competence and the system's security level by repeatedly analysing the risks against it.

We argue that even before the security designers can benefit from risk analysis and the establishment and use of security policies, they could benefited very early in the IS development and security design process from particular domain analysis and modelling inscriptions (e.g. Table 2) so as to identify early the major security concerns.

Modern information systems in their contemporary organizational context (rapid technological progress, changing forms of applying business, changing norms of communications, informational added value to organizational processes) need now, more than ever, approaches to assure their security in a convenient, dynamic and effective way; the luxury of "enough time" to study the system and conduct risk analysis in the traditional way, over a static image of it, is not applicable any more and security design needs to centre around approaches that ensure early tracking of potentially problematic areas and their effective counteraction.

Approaches like the interpretive framework we presented in action through this essay, we believe that shall contribute to the empowerment of the process of information systems security design and that it shall make it possible to integrate security to the information system's development processes.

7. REFERENCES

Baskerville, R. (1993), "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys,* Vol. 25 No. 4.

Checkland, P. (1981), *Systems thinking, systems practice,* Wiley.

Checkland, P. (1999), *SSM: a 30-year retrospective,* Wiley.

Downs, E., Clare, P. and Coe, I. (1992), *SSADM: Application and Context,* Prentice Hall.

Eden, C. and Huxham, C. (1996), "Action Research for the Study of Organizations", in *Handbook of Organization Studies,* S.R. Clegg, C. Hardu, W.R. Nord (eds), Sage.

Eloff, M., and Von Solms, B. (2000), "Information Security: Process Evaluation and Product Evaluation", in *Information Security for Global Information*

Infrastructures, S. Qing and J. Eloff (Eds.), Kluwer Academic Publishers, pp. 11-19.

Fitzgerald, B. (1998), "An empirical investigation into the adoption of system development methodologies", *Information & Management,* 34, pp. 317-328.

Hitchings, J. (1995a), "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology", *Computers & Security,* 14, pp. 377-383.

Hitchings J. (1995b), "Achieving an Integrated Design: The Way Forward for Information Security", in *Information Security – the next decade,* J. Ellof and S. von Solms (Eds.), Chapman & Hall.

Kiountouzis E.A. and Kokolakis S.A. (1996), "An analyst's view of IS Security", in *Information System Security facing the information society,* S. Katsikas and D. Gritzalis (Eds.), Chapman & Hall, pp. 23-33.

Klein, H. and Myers, M. (1999), "A set of principles for conducting and evaluating interpretive field studies in information systems", *MIS Quarterly,* Vol. 23 No. 1, pp. 67-94.

Kokolakis, S. (1996), "Is there a need for new information security models?", in *Communications and Multimedia Security II,* P. Horster (Ed.), Chapman & Hall.

Mumford, E. (1998), "Problems, knowledge, solutions: solving complex problems", *Journal of Strategic Information Systems,* 7, pp. 255-269.

Pouloudi, A. (1999), "Aspects of the Stakeholder Concept and their Implications for Information Systems Development", *Proceedings of the 32nd IEEE International Conference on System Sciences.*

Tryfonas, T., Kiountouzis, E. and Poylimenakoy, A. (2000), "Embedding security practices in contemporary information systems development approaches", submitted to *Information Management and Computers security.*

Walsham, G. (1995), "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems,* 4, pp. 74-81.

Ynström, L. (1999), "Systemic-Holistic Approach to IT Security", in *IPICS 99 lecture notes volume,* University of the Aegean.