INFORMATION SYSTEMS SECURITY AND THE INFORMATION SYSTEMS DEVELOPMENT PROJECT

Towards a framework for their integration

T. Tryfonas and E. Kiountouzis

*Dept. of Informatics, Athens University of Economics and Business
76 Patission st., GR-10434, Athens, GREECE
{tryfonas, eak}@aueb.gr*

Key words: Development project, Development practices, IS Security integration.

Abstract: Information systems development practices often require trade offs between make-or-buy decisions. Contemporary practices tend along the ‘buy’ maxim, resulting in systems that are largely depended on commodity IT facilities. Such systems development however introduces new security problems. New ways of addressing and resolving security hazards, early within the development lifecycle, must therefore be introduced in the systems development field. To do so, we need to properly associate the existing development context with suitable concepts that introduce security within it. In this paper we address the challenges arising by new forms of systems development and describe the factors that are most likely to be taken under consideration for securing the system under development.

1. INTRODUCTION

In modern organisations critical assets can often take the form of data stored, processed and transmitted by information technology (IT) facilities, such as software or hardware products, systems or applications. Such organisations expect their data to remain confidential, be available to them when required and not be subject to unauthorised modification. Strategic information, or information required daily for work support require new forms of communication and trading, thus an efficient but also secure

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: [10.1007/978-0-387-35586-3_46](https://doi.org/10.1007/978-0-387-35586-3_46)

technological infrastructure. In the light of those requirements, security of information is considered largely important.

However modern technology solutions are procured and developed in ways that they make extensive use of existing commodity IT products. As those commercial off-the-shelf (COTS) products become more popular, researchers argue that little information is available on how they affect existing systems development processes or what new processes are needed (Brownsword *et al*, 2000). The case regarding their impact on information systems (IS) security is far clumsier, as developers and users of IT solutions may lack the knowledge, expertise, or resources that are necessary in order to decide whether they can trust their IT components (Moulinos *et al*, 2000). To resolve this issue, researches argue for a long time that incorporating security within systems development processes is the most appropriate way of introducing security in the complex context of an organisation (Baskerville, 1993).

Therefore, the development of information systems faces new challenges nowadays that have not yet been fully encountered through practice or theory. The IS literature fails so far to present a comprehensive framework that can integrate security with development, despite the plethora of approaches that have been recently introduced in the field of security, as most of them deal with few of the emerging aspects or have not yet been properly evaluated in the real world (Siponen, 2001).

Given the absence of a comprehensive framework to integrate development and security, we try in this paper to investigate and to trace important factors that could be incorporated in a formal scheme, capable of producing a framework to integrate existing security practices with a given development context (with regard to both its organisational and technological elements). In section 2 we introduce our research approach and comment upon its key directions, in section 3 we present an interpretive discussion of the role of the IS security within organisation, section 4 is an attempt to formalise our findings and finally in section 5 we discuss about the perspectives for further research on the issue.

2. RESEARCH APPROACH AND THE KEY DIRECTIONS

As our subject matter refers eventually to the organisation, it addresses 'soft' factors apart from the technical ones. Thus, the research approach, in order to be fruitful, it should be capable of interacting between the two (Gable, 1994). An appropriate way of conducting research in the organisational context is the interpretative paradigm (Jarvinen, 2000), which

we adopt for our research. This can be also justified through several surveys concerning IS security (e.g. Witty *et al*, 2001); IS managers don't usually will to report security issues occurred in their systems and this fact makes statistical analyses difficult, boosting the attempts for interpretive-intensive research. Here, based on literature review and comparison of personal knowledge and experiences, all those viewed under the analyst's point of view.

In this section we investigate some of the related literature and we try to trace ideas and keynotes for our subject. To start with, Anderson, in his analysis of cryptosystems failures (Anderson, 1993), argues that the models used till then, being traditionally asset-based, were not capable of including factors proved to have major contribution to failures. Such factors could be vendor involvement, employee mistrust or procedural mistakes/omissions. Moreover the lack of feedback for similar incidents is an important factor that bottlenecks the design of secure information systems. He traces a shift in facing information systems security, from assurance of the IT infrastructure and single-product certification (IT security), to a wider problem-solving context.

Mumford extends this reasoning and discusses cyber-crime as a result of misconceptions and faulty models for the description of the new, evolving information era and its means (Mumford, 1998). She argues that problems involving computer abuse should be a subject to be resolved within the regular managerial agenda, either it responds to issues concerning the wider societal context, or within the boundaries of a specific organisation. Incorporating IS security to the managerial problem-solving context can assure that important factors affecting the information system's ability to operate under legitimate conditions will be identified and included in the system security design process.

A verification by-example in a very specific field of the apparent success of this shift is in (Kephart, 1994). He shows how the capabilities of a traditional computer virus confrontation approach enlarge by far by using a living analogy that enables the computer system to defend itself better. Kephart argues that the traditional techniques for computer viruses detection and removal used till then were extended to the maximum, when the underlying base of inquiry models shifted from mechanistic to biological and the technology-related issues faced within a problem-solving context.

Others argue that the combination of different security approaches is the key to succeed in environments, in which 'soft' environmental factors are strongly involved (Tryfonas & Kiountouzis, 2001). Asset identification and valuation (as in traditional risk analysis) and risk-driven process descriptions (as in process driven approaches) along with stakeholder analysis were used to produce the IS security plan for a drug-addict therapeutic institute, that

was operating and further developing its information system. It seems that the more complex the organisational model is, the more security-focusing enabling concepts we have to involve in the security design (e.g. asset, process, stakeholder).

We have presented literature evidence implying, or explicitly claiming, that for particular infrastructure-related security issues, solutions exist and are largely depended on specific technology countermeasures. However, securing the technical infrastructure alone (IT security) is not enough and there is a need for a change in the pattern to approach and add security to an information system, as in the wider organisational context threats could be unlimited, measures can be incapable of meeting the environmental requirements and so forth.

3. AN INTERPRETATION OF SECURITY ISSUES WITHIN ORGANIZATIONS

The discussion so far verifies that development efforts for secure information systems introduce new challenges to the field of contemporary IS and therefore in the organisations to which they are introduced. Researchers could potentially locate many important factors facilitating the development of secure systems, but there is no formal classification, not even a proper itemisation of them. Adopting an analyst's point of view we shall address where and how information systems security emerges as a matter to be dealt with within a modern organisation. Locating it within the organisational life and the process of systems development that produce the information system as corporate tool is important, as it will be the start to incorporate the IS security to the managerial agenda and start the integration with the development project from there.

The nature of the organisation defines to a large extend its information system. However, this relation is interactive and the information system can have impact on the organisation as well. The organisational culture combined with the nature of inquiries within its context is the key to understand the phenomena within it and their impact on the IS. The nature of the inquiry could be systematic, i.e. structured and formally founded, or systemic, a process that perceives the reality problematic and provides systems to resolve the problems (Checkland, 1981).

In many cases we understand a problem or a phenomenon by attributing to it elements of other familiar concepts. Those mechanisms ('metaphors') are conceptual models used to enhance our understanding and describe a situation in terms of something familiar. Several metaphors have been used in the management sciences (Walsham, 1991), but they all could be

summarised in three major categories: those describing the organisation as a machine, as a living system (organism) and as a social system.

With regard to the information system itself, its lifecycle has changed over the years, even with regard to conventional development practices, such as customary in-house systems development. Off-the-self systems can be purchased and used in association and this alienates the lifecycle of the traditional development project. The scope of such a ready-made solution can vary from a single package (considered as a simple component) to a comprehensive product suite of compatible and interacting modules, serving as a comprehensive IS (product-based).

All the legitimately involved parties ('stakeholders') maintain implicit perceptions of information security and they formally express them in terms of security requirements. The process of realising their implicit understanding to formal explicitly defined requirements is assisted through familiar organisational concepts such as the *asset* or the *process*. We argue that the concepts that introduce information systems security to the organisation, define to a large extent the nature of the tools that should be used to secure the information system, either after its development or within the development process. Our observation here is therefore that there are organisational concepts that serve as means to focus on IS security within the organisational environment.

It also seems that those security-focus concepts determine the nature of the method/tool to be used for the project along with the expressed system's security requirements. Security tools come to a variety of platforms and applications and could assist methods and techniques used elsewhere within the development life cycle. Risk analysis methods and assisting tools, IT security standards, access control mechanisms, data encryption facilities etc. are all based on concepts such as assets, processes etc. For example, a practice utilising the concept of the asset is the CCTA Risk Analysis and Management Method (CRAMM), where groups of assets are identified and countermeasures that match the stakeholders' perspective of the value of a particular asset are extracted through a knowledge base. Such an approach of signifying security requirements concerning informational assets has been identified as a mechanism of integration of security within traditional lifecycle development projects by many researchers (Downs et al, 1992 and and Hayam and Oz, 1993).

Several other information security specialists observed the fact that a number of security issues arise from mistakes, omissions or failures within the development process (Anderson, 1993, Wood & Snow, 1995 and Eloff & von Solms, 2000). The result is a defected product/system that its defects could potentially abused, so as to compromise an information system. Therefore information security problems in contemporary

product/component oriented development practices could be resolved within process assurance. This could be whether within the development process (early risk elimination) or within the supported business process (security management), as each single product could be validated and assured properly.

Finally, in terms of security approaches based on organisational concepts, researchers (e.g. Hitchings, 1995) have found that security within IS comes through discourse and final agreement on what is important for the system, within which operations, and agreement on what risks are there for those and for the involved stakeholders. Thus, this approach tries to encapsulate dynamically all concepts traced in this section. Ideally through that practice the stakeholders themselves shall pinpoint the assets and processes throughout the organisational structure (strategic management, tactical management and operations management) and the risks against them, so as to produce a security design.

A number of other approaches are currently under research. We only discuss here though the approaches that, throughout the literature or practice, have rigidly exploited the previously introduced ideas (asset, process, system, stakeholder).

The results as such of the security-pursuing process are interesting to further comment upon to as well. For example, there could be as a result an explicitly documented security policy for the IS. On the other hand, there could be a change in terms of culture of the way data is processed (e.g. compliant with data protection acts), something that is not tangible. Thus, the outcome could be tangible in terms of *milestones* or non-tangible in terms of the *impact* it has on the organisational environment. Security-related projects usually produce documented descriptions (deliverables) of actions securing the organisational infrastructure (security policies and other formally documented plans). The non-tangible outcomes are sometimes impressive as they contribute to organisational change and ideally improvement. This fact is evident, despite the common perception of security being a 'burden', especially amongst system end-users (Tryfonas *et al*, 2001).

Hence, the conclusion is that the organisational context, potential security approaches and the development practice are important factors that seem to determine the way that security can be integrated in a development project within a specific organisation. Consider for example the case where the IS is a proprietary system, developed for an organisation perceived by the analysts as a machine and its security is based on the concept of assets. In such cases it seems that a suitable security approach is an asset-based information systems risk-analysis, such as CRAMM for example. It will be interesting to see whether there is indeed an emerging suggested combination of such

factors that could evidently lead to a harmonic choice of appropriate IS security controls within an organisation.

4. TOWARDS SECURITY INTEGRATION WITHIN SYSTEMS DEVELOPMENT AND ORGANISATIONAL LIFE

We have made clear that each organisational concept used to introduce security to a development project serves as a driver for the accompanying security methods and tools to be used. For example the concept of the asset signifies the use of IS risk analysis which gives particular emphasis in asset identification and valuation (Finne, 1998). Each tool underlies an epistemological approach to the problem and realises a solution to comply with it. Risk analysis is for example a methodical and systematic way of resolving hazards using and evaluating the pattern asset-threat-impact to produce countermeasures. We think that assets and processes are usually the organisational concepts to use when the organisation is perceived as a machine, whereas systems are identified when the environment is explored through societal metaphors.

It is generally accepted that the appropriate way to introduce IS security into an organisation is to identify, introduce, manage and maintain an effective set of security controls (Barnard and von Solms, 2000). But we argue that the context of the development project dictates the security approach that is mostly appropriate. Particularly, it seems that for cases where the target organisation is perceived as a machine, systematic tools are more suitable. Systems that can fully exploit such approaches are those that are characterised by order and they are expected to retain a certain behaviour and nature, whatever the circumstances, at any cost (e.g. the critical infrastructure). On the other hand, systems that deal with a changing environment and must adapt to it so as to gain competitive advantages tend towards a mixture of systematic and systemic security approaches (for example in the field of Management Information Systems). Last but not least, systems characterised by their strongly social character tend to purely systemic approaches (systems serving research/educational purposes or household computing).

After the discussion in the previous sections we have visualised all the important aspects in table 1. In a mechanistic context, well-defined problems concerning data (asset) security can be resolved by IT security facilities, such as cryptographic means. In the wider context of an organisation though, as the number of the stakeholders increase and the descriptions of the context become more complex, security concerns must focus on and

expressed through multiple concepts (processes, systems etc.). Patterns such as asset/machine/custom development should be applied when the problems in a sector are well defined. On the other hand patterns like systems/society/combinations should be the driver for open and turbulent systems. A misjudge or an alteration in the underlying pattern of a systems development case could potentially be the source of the security problems to be faced later on.

Table 1. A visualisation of important factors concerning the integration of systems development with systems security

Important Factors	Range of possible values			
<i>Stakeholders</i>	User	Developer	Consultant	Others
<i>Analyst's organisational perception</i>	Machine	Organism	Society	
<i>IS development practice</i>	Single-Product based	Custom	Component-based	Combinations
<i>Base of the security approach</i>	Asset	Process	Stakeholder	Systems
<i>Expected outcome</i>	Measured in milestones	Change in context (Intangible)		

The interested party (developer, consultant or user organisation) should know how the target organisation is structured and viewed (e.g. metaphors, models) and which development practises are better to apply because of that structure. Ideally their successful matching with security concepts shall reveal what are the security needs and requirements of the application domain. Such an approach serves as an enhancement of the analyst's armour for tackling security-related problems early within the systems development life cycle.

5. CONCLUSIONS AND FURTHER RESEARCH

In the contemporary organisational context the security design has to focus on approaches that ensure early tracking of potential problems and their effective dissolution. Furthermore, as products and services being

developed to support organisational activities require advanced security features, the importance of integrating security to them grows fast. But there are currently very few disciplined approaches to information security integration to systems development, mainly because there seems to be a lack of understanding that it is a problem to be faced within a “new security paradigm” and not as a traditional IT security problem (Anderson, 1993, Hitchings, 1995 and Mumford, 1998).

It is not easy for an implementer or a user organisation to have such an expert knowledge of all the available security systems/tools and their particulars, so as to choose the most appropriate ones for a system under development. Therefore, there is an evident need for a framework to indicate the most appropriate security features and components. Our discussion provides the reasoning to investigate the suitability of the security approaches within a given organisational environment and a development practice in mind.

A primary concern for further research should be to formalise and further enhance this reasoning framework with several other meaningful concepts and variants. Such an approach could assist the analysis and identification of all compatible security practices for a given context. It could also be useful for studying the security compatibility of domains, or for change-impact analysis. This framework might serve as a means of facilitating security consulting work for systems planned for, or currently under, development. It is the authors' intention to continue working on this area and present a complete and comprehensive methodological framework to do this.

6. REFERENCES

- Anderson, R.J. (1993), “Why cryptosystems fail”, *Communications of the ACM*, 37(11), pp. 32-44.
- Barnard, L. and von Solms, R. (2000), “A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls”, *Computers & Security*, Vol 19 No 2, pp.185-194.
- Baskerville, R. (1993), “Information Systems Security Design Methods: Implications for Information Systems Development”, *ACM Computing Surveys*, Vol. 25, No. 4, pp. 375-414.
- Brownsword, L., Oberndorf, T. and Sledge C.A. (2000), “Developing New Processes for COTS-Based Systems”, *IEEE Software*, July/August, pp. 48-55.
- Checkland, P. (1981), *Systems thinking, systems practice*, Wiley Publications.
- Downs, E., Clare, P. and Coe, I. (1992), *SSADM: Application and Context*, Prentice Hall.

- 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.
- Finne, T. (1998), "A conceptual framework for information security management", *Computers & Security*, Vol 17, pp. 303-307.
- Gable, G.G. (1994), "Integrating case study and survey research methods: an example in information systems", *European Journal of Information Systems*, Vol. 3, No. 2, pp. 112-126.
- Hayam, A. and Oz, E. (1993), "Integrating Data Security into the Systems Development Life Cycle", *Journal of Systems Management*, Vol. 8 No 44, pp. 16-20.
- Hitchings J. (1995), "Achieving an Integrated Design: The Way Forward for Information Security", in *Information Security – the next decade*, J. Eloff and S. von Solms (Eds.), Chapman & Hall.
- Jarvinen, P.H. (2000), "Research Questions Guiding Selection of an Appropriate Research Method", Proceedings of the 8th European Conference on Information Systems (ECIS).
- Kephart, J.O. (1994), "A Biologically Inspired Immune System for Computers", in *Artificial life IV*, R. Brooks and P. Maes (Eds.), MIT Press.
- Moulinos, K., Kyrloglou, N. and Tryfonas, T. (2000), "A Framework for Comparing Cryptographic Libraries", in *IFIP/SEC 2000: Information Security*, S. Qing and J. Eloff (Eds.), International Academic Publishers, pp. 9-12.
- Mumford, E. (1998), "Problems, knowledge, solutions: solving complex problems", *Journal of Strategic Information Systems*, 7, pp. 255-269.
- Siponen, M. (2001), "An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications", in *Information Security Management: Global Challenges in the New Millennium*, G. Dhillon, Idea Group Publishing, pp. 101-124.
- Tryfonas, T. and Kiountouzis, E. (2001), "Security Concerns for Contemporary Development Practices: A Case Study", in *Trusted Information: The new decade challenge*, M. Dupuy and P. Paradinas (Eds.), Kluwer Academic Publishers, pp. 421-435.
- Tryfonas, T., Kiountouzis, E. and Poulymenakou, A. (2001), "Embedding security practices in contemporary information systems development approaches", *Information Management & Computer Security*, Vol. 9 No 4, pp. 183-197.
- Walsham, G. (1991), "Organisational metaphors and information systems research", *European Journal of Information Systems*, Vol. 1, No. 2, pp. 83-94.
- Witty, R. et al (2001), *The price of information security*, Strategic Analysis Report R-11-6534 (June), Gartner Research.
- Wood, C.C. and Snow, K. (1995), "ISO 9000 and Information Security", *Computers & Security*, 14, pp. 287-288.