31

Redefining Information Systems Security: Viable Information Systems

Maria Karyda, Spyros Kokolakis, Evangelos Kiountouzis
Maria Karyda, Evangelos Kiountouzis: Department of Informatics, Athens University of Economics and Business,
76 Patission Street, Athens GR-10434 Greece, tel. +301-8203555,
fax: +301-8237369, email: {mka, eak}@aueb.gr

Spryros Kokolakis: Department of Information & Communication Systems, University of the Aegean,
Samos GR-83200 Greece, tel. +30-273-82001, fax: +30-273-82009,
email: sak@aegean.gr

Key words: Information Systems, Information Systems Security, Cybernetics, Viable Information Systems

Abstract: Research on Information Security has been based on a well-established definition of the subject. Consequently, it has delivered a plethora of methods, techniques, mechanisms and tools to protect the so-called security attributes (i.e. availability, confidentiality and integrity) of information. However, modern Information Systems (IS) appear rather vulnerable and people show mistrust on their ability to deliver the services expected. This phenomenon leads us to the conclusion that information security does not necessarily equal IS security. In this paper, we argue that IS security, contrary to information security, remains a confusing term and a neglected research area. We attempt to clarify the meaning and aims of IS security and propose a framework for building secure information systems, or as we suggest them to be called, viable information systems.

1. INTRODUCTION

Research on Information Security has evolved on the basis of a well-established theoretical foundation, the essence of which being the commonly accepted definition of Information Security as the preservation of the so-called security attributes of Information, referring mainly to Confidentiality, Integrity, and Availability. Consequently, research on Information Security has produced significant results, which are rapidly turning into commercial products.

However, a number of security surveys show that Information Systems (IS) suffer severely from security breaches and even the most sophisticated systems appear to be vulnerable to well-coordinated attacks (see for example [CSI, 2000; Ernst&Young, 2000]). The above paradox reveals the significant gap keeping apart IS security from information security.

Contrary to Information Security, IS security lacks a widely accepted definition or at least a common understanding of the meaning and aims of IS security. Therefore, current research on the issue seems fragmented and difficult to be exploited by industry.

The attempt to apply the concept of "security attributes" to the area of IS has little chance of providing an adequate conceptual basis for research and practice. An information system cannot be simply defined as a system that processes data and delivers information. An IS comprises hardware, software, data, procedures and, above all, people. The above elements are in constant interaction and interdependence, forming a complex and dynamic whole. IS belong to a special category of systems usually referred to by the term "human activity systems" [Checkland and Holwell, 1998]. In our view,

> an information system is a human activity system comprising five elements, namely hardware, software, data, procedures, and people, interacting with each other and with the environment, aiming to produce and handle information, in order to support human activities in the context of an organisation.

In this perspective, the content and goals of IS security need further elucidation. In the rest of this paper we shall attempt to address the following issues:

- How do we perceive the meaning and aims of IS security?
- How can we build secure information systems?

2. PREVIOUS RESEARCH

The goal of IS security has traditionally been the protection of the three basic information security attributes, confidentiality, availability and integrity, along with some others, such as authentication, privacy, and non-repudiation. Often, security goals would be extended to include also the protection of the information technology infrastructure, such as workstations, servers, and communication lines. This can be achieved in a systematic and well-documented way, using for example the *risk analysis* methodology [Baskerville, 1991]. This systematic view, employed by many of the models, methodologies, techniques and tools, emphasize the protection of the technical components of an IS. As a result, security problems associated with the human factor, as well as managerial and social security problems have been either neglected or treated as technical ones.

Moreover, previous research in IS security stresses also the fact that "…while security traditionally has been focused on confidentiality of information, the problems of greatest concern today relate to the availability of information and continuity of services…" [Lipson and Fisher, 1999]. Many researchers criticize as well the view of security as the preservation of confidentiality, integrity and availability as "dangerously oversimplified" [Parker, 1996] and emphasize the need for addressing security at an "overall level" [Ellof and von Solms, 2000]. The need for a distributed and more flexible IS security management has also been recognized as a necessity, in contrast with the current rigid and centralized type of security management applied in most organizations [Baskerville, 1997].

The obvious shortcomings of the use of the systematic approach described above are addressed in methodologies that apply a systemic view. These methodologies, such as the *Virtual Methodology* [Hitchings, 1996] and *SIM-ETHICS* [Warren, 1996], include human and contextual issues as well as technical solutions and emphasize on the analysis of the organization and relevant systems. The systemic view has also been applied to IS security education, in the holistic approach proposed by Yngstrom [1996].

The dependence of organizations on their IS to maintain their functionality stresses furthermore the importance of the unhindered function of the IS. To address this need, a new approach has been recently introduced focusing on the *survivability* of the IS, with survivability meaning "…the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents…" [Ellison et al., 1999]. The aim of this new trend is not only to thwart possible intruders or prevent accidents in the premises of the IS, but also to ensure that the required services are delivered, despite the occurrence of unwanted events [Lipson and Fisher, 1999].

The survivability approach emphasizes the importance of the protection of mission-critical systems, using a risk-management perspective that requires the participation of the organization. This approach, however, despite that it offers a very useful view of security, it is narrowly focused on risk-mitigation strategies and contingency planning concepts.

We argue that an IS should not only be considered in terms of its "own survivability", but in relation to the organization it serves. We therefore use instead the term "viability", as used in the field of organizational management, according to the *Viable System Model* proposed by Beer [1979; 1981]. In this paper we propose a methodology for building a *viable information system,* which not only retains its capability of offering the required services under different circumstances, but also it functions in the context of the organization, in terms of goal achievement and cost. In our view, this methodology extends the "survivability" approach, by using a systemic model that addresses both the problem of dealing with unwanted events, which threaten the system's functionality or performance, and the issue of selecting and implementing the appropriate countermeasures so as to achieve "viability".

3. SYSTEMS VIABILITY AND INFORMATION SYSTEMS SECURITY

Nowadays organizations depend heavily on their IS not only for their functions and operations on a daily basis, but also as a key organizational component in their strategic plans. Furthermore, new organizational forms, which rely almost entirely on their information technology infrastructure and their information systems, have already been established, usually referred to as the Virtual Corporation, Network Organization, or Virtual Organization [Davidow and Malone, 1992; Mowshowitz, 1997].

In general, most of the problems and challenges organizations and IS face today, are more or less similar: both the organization and the IS have to deal with their complexity and manage unexpected changes that occur in an accelerating rate. In addition to this, the effort to overcome these problems is obstructed by the interdependencies between their parts or subsystems. In order for organizations and IS to face the previously mentioned challenges in an effective way, these systems should at least:

- Be able to meet the demands and changes of the environment;
- Have internal structures that can deal with the demand for learning and for quick adaptation; and

- Have communication abilities for connecting and transmitting information

IS operate within the context of the organization they serve, so they can be considered as an organizational function that embraces information technology, information activities (roles, tasks and functions) and organizational activities. We can furthermore refine the IS function as follows [Jayaratha, 1994]:

i) Information processing and usability function.

ii) Education and learning function.

iii) Information systems development function.

iv) Management and control function.

v) Strategy and planning function.

Within this functional point of view, it is very hard to distinguish exactly between the IS and the organization it serves. Thus, it is easy to understand why threats to an IS and their impact concern in such a high degree the organization. However, the IS remains the serving system, whose functionality needs to be protected and preserved, in order for the served system, the organization, to maintain its existence within its environment.

Ashby [1964] argued that only variety can control variety (Law of Requisite Variety). By this he meant that if a situation was complex, with many variables, then the techniques for dealing with the situation would need to have the same amount and kind of variety. If Ashby's Law of Requisite Variety is accepted this means that the risk analysis techniques used to establish security measures must have at least the same kind and level of knowledge as the intruders themselves. However, while organizations change, technology changes, plain risk analysis techniques, usually based on software packages, i.e. CRAMM, remain unchanged, or, at least, change with a small rate (time lag). In other words, risk analysis techniques are static.

On the other hand, it is evident that there is consensus among many that the use of methodologies is positive and well advised. However, practitioners have been somewhat slow in adopting IS security methodologies. This could be explained variously as, for example, due to the ignorance syndrome among the designers, or the slow speed of technology transfer. However, although methodologies are attractive and have an intuitive appeal, the fact is that the methodology is merely a framework for organizing the process.

Moreover, IS security is a managerial problem and therefore should not be addressed as a separate problem, instead IS security management should be

incorporated into organization management and should change with it. This means that IS security should be a build-on characteristic and not and add-on one.

In our view, IS security should preserve the ability of the IS to deliver the required services to the organization, but most important to achieve the most effective coupling between the IS and the organization. The goal of IS security should be the protection of the functionality of the IS, not necessarily of the IS itself or its components, provided that the IS achieves the goals, which have been established by the organization, and operates within a certain scope.

A system that is able to maintain an independent existence in the long run and within a dynamic environment is called a *viable* system. In this paper, we redefine the issue of designing *secure information systems* by designing *viable information systems.* According to this approach, a viable information system is capable of maintaining its existence by managing the risk that stems either from inside or the environment.

3.1 The Viable System Model

As one of the basic tools in our approach we use the Viable Systems Model (VSM) as proposed by Stafford Beer in the early 1970s. VSM is the outcome of Beer's thirty-year effort to elucidate the laws of management, by combining his expertise in cybernetics and his study of biological systems. Beer found that all organisms displaying viability (viability being the capability to maintain an independent existence in the long term) share five basic properties [Brocklesby and Cummings, 1996]. These properties are " *five necessary and sufficient subsystems interactively involved in any organism or organization that is capable of maintaining its identity independently of other such organisms within a shared environment."* [Beer, 1984] Beer also explains that this 'set of rules' has not been created by way of analogy between an organism and an organization, but the rules were *"developed to account for viability in any survival-worthy system at all"* [Beer, 1984].

In brief, these systemic functions are:

- *System One.* The 'operational elements' that produce the system and interact with the external environment. These elements are themselves viable systems.
- *System Two.* The 'co-ordination' functions that ensure that the operational elements work harmoniously.

- *System Three.* The 'control' activities, which maintain and allocate resources to the operational elements.
- *System Four.* The 'intelligence' functions that consider the system as a whole -its strategic opportunities, threats and future direction. They also interface with the environment.
- *System Five.* The 'identity' function, which identifies self-awareness in the system.

3.2 Viable Information Systems

We have already described the need to address security needs within information systems in a holistic and systemic way, arguing that attempts to introduce the well-founded concept of information security in the information systems field have not been fruitful. Our aim is to build a viable information system, rather than a secure one. A viable information system possesses the ability to maintain its existence, by managing risk and, hence, we can apply the Viable System Model (VSM) as proposed by Beer.

4. BUILDING A VIABLE INFORMATION SYSTEM

We propose a three-phase iterative process for building a viable information system, namely **diagnosis, re-design,** and **transformation** (see Figure 1).

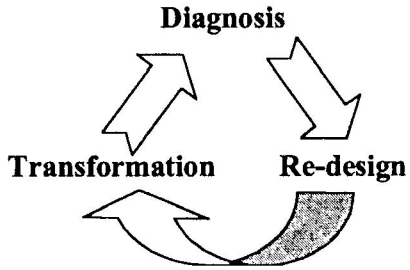

Figure 1. Three phases for building viable information systems.

4.1 Diagnosis

We call the first phase Diagnosis, since it is the phase at which one has to detect vulnerabilities, defects and other factors that threaten the system's

viability. This will determine the kind of intervention needed to resolve these problems. We use VSM for this task, since it is an effective and powerful tool for detecting inefficiencies and defects within a system, as well as for planning and implementing change. However, before addressing the issue of how to transform an IS into a viable system, one has to assess the IS, by evaluating its contribution to the achievement of the organizational goals. We suggest that three parameters should be considered, i.e. *performance, risk,* and *cost.*

4.1.1 4.1.1 Parameter evaluation

System performance refers to the degree the system achieves its goals. It is a measure of the system's contribution to the goals of the organization. If we consider, for example, a production system, the volume of the output it produces can measure the performance.

In real-life systems, performance is never guaranteed and there is always some risk involved. It is, therefore, unrealistic to evaluate a system by its regular performance and not to take into account the possibility of a breakdown. On the contrary, researchers have indicated the need to design IS that "anticipate breakdown" [Winograd and Flores, 1986]. Therefore, we argue that *risk* should also be evaluated. Risk expresses the possibility of a system failing to meet its goal in the future. Finally, a realistic assessment of a system should not overlook *cost,* i.e. the resources used in order to achieve the goals of the system and to mitigate risk.

Similar evaluation methods are quite common in areas such as finance management, where candidate investments are evaluated in terms of anticipated profit, investment cost and risk. However, the application of such methods in the area of IS is not straightforward. Such an evaluation requires a thorough analysis of the IS. For this purpose we use process modeling, which offers a rich model of the IS in the context of the organization it serves. The process modeling technique used in the following example is based on IDEF∅, a popular modeling technique used in business process re-engineering [Mayer et al., 1995]. IDEF∅ uses five basic elements: process, input, output, control and mechanism (see Figure 2).

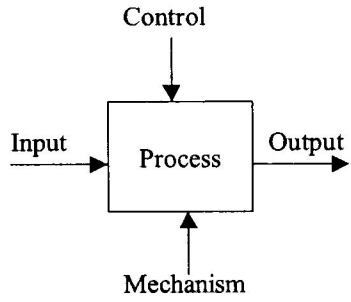

Figure 2. IDEF∅ Diagram

In Figure 3, we present the VAT (Value Added Tax) Collection Process, which is part of the Internal Revenue Information System. It should be noticed that this is actually a business process model with a focus on the informational aspects of the process. This is in accordance with our previous argument that in modern organizations IS should not be studied separately from the organizational processes they support.

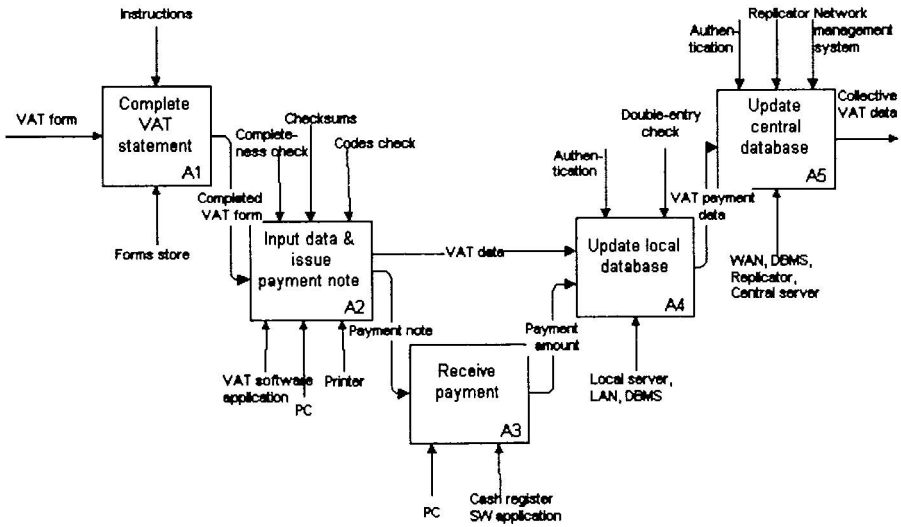

Figure 3. VAT Collection Process

The goals of the VAT Collection Process are: (a) to minimize the time needed to process a VAT statement, (b) to collect the full amount owned by the tax-payer and (c) to protect the privacy of the tax-payer. In the example presented here, the performance of the VAT Collection process is estimated

at an average of 10 VAT statements per hour, with 100% accuracy and 100% success in preserving the confidentiality of personal information given by the tax-payer. Of course, this is the ideal situation; unfortunately the system dues not operate as designed all the time.

In order to estimate the level of risk, it is required to identify threats and vulnerabilities in each sub-process and then estimate the total risk level for the VAT Collection Process. It is beyond the scope of the paper to indicate the method to estimate risk, since risk analysis is a well-studied area. The assignment of a risk level in every sub-process forms a "Risk Estimation Diagram" on which we estimate the total risk level for the VAT Collection Process (see Figures 4, 5 and 6). In this case we estimate risk for each of the three goals of the system. In Figure we present a " Risk Estimation Diagram " where a risk factor of 5 (in a 1-100 scale) is estimated, which means that we are only 95/100 confident that the process will achieve its goal.

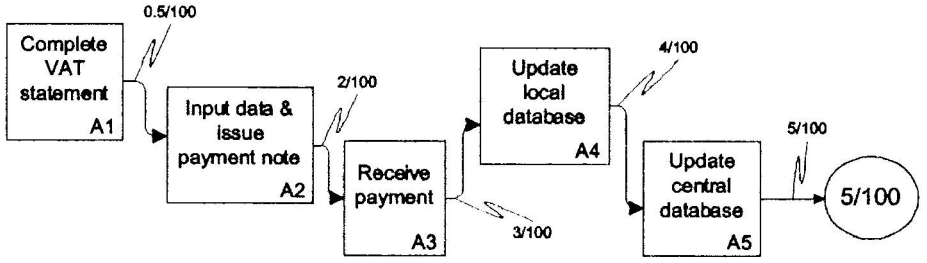

Figure 4. Risk Estimation Diagram for Goal "minimize time needed to process VAT statements"

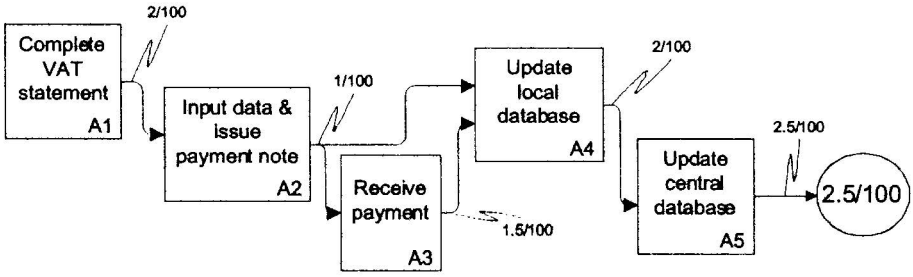

Figure 5. Risk Estimation Diagram for Goal "collect the full amount owned"

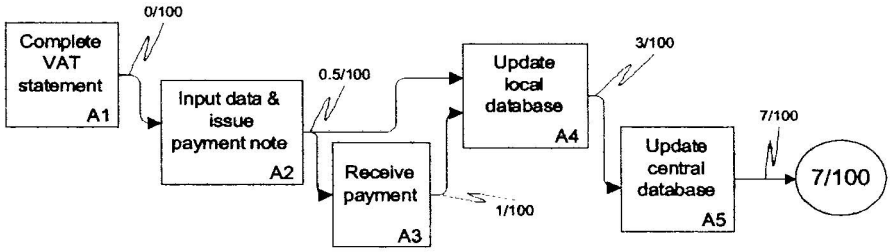

Figure 6. Risk Estimation Diagram for Goal " preserve tax-payers privacy"

In the above figures, we may notice that not all processes increase the level of risk, some processes mitigate risk. For example, A2 in Figure 5 includes several checks that minimize the risk of receiving a false VAT statement.

The last element missing is the estimation of the operation cost. In the case of the VAT Collection Process, cost has been estimated to be 20.00 Euro per hour. The above example is limited to a single process. In order to have a complete model, all processes should be considered and the total Performance, Risk and Cost for the system should be estimated.

4.1.2 4.1.2 VSM analysis

Based on the evaluation of the system, we may improve its current operation by decreasing risk in the processes with a high risk factor (e.g. by including more controls, or adding more resources). However, by this systematic approach we may only achieve minor improvements. Transforming the IS into a viable system requires a more radical approach.

At this point, we suggest the use of VSM as a diagnostic tool. According to VSM a viable system comprises five specific systemic functions (see Section

2). As a first step we should check whether these functions have been adequately developed in the system under study and how they perform. This may lead to designing new processes that implement the missing, underdeveloped or flawed functions.

At the next step we apply VSM techniques to control variety. Variety control provides us with a means to decrease the threats faced by the system. To do this we use the relevant mechanisms applied in VSM, namely the *attenuator,* that can be used to reduce the possible effect of a threat on the system, and the *amplifier,* that enforces the defense of the system.

4.2 Re-design and transformation

Following diagnosis, the IS should be redesigned. The redesign process may include the following steps:

1. Design processes that implement the missing, underdeveloped or flawed VSM functions.
2. Add processes that serve as attenuators or amplifiers.
3. Add controls and mechanisms to mitigate risk for the processes with a high risk factor.
4. Re-evaluate.

The first three steps should achieve the aim of minimizing risk. However, this may result in degrading the overall performance of the system, or increasing the cost. Therefore, re-evaluation is needed, in order to ensure that the proposed changes will really improve the current status of the system.

Finally, when re-design is completed and the proposed changes are approved, the changes should be implemented, in order for the IS to acquire the attributes of a viable system.

5. SUMMARY AND FURTHER RESEARCH

In this paper, we address the issue of building a secure information system. The term IS Security is usually used to refer to the protection of the security attributes of an IS, which, in our opinion, is a very limited way to view the issue. We argue that the term *viable information system* expresses more adequately the concept of the IS which is capable of dealing effectively with threats and contingencies. Furthermore, we suggest that the process of

building a viable information system should follow three phases, namely *diagnosis, re-design,* and *transformation.*

The paper, also, contributes a technique for the evaluation of information systems. The proposed evaluation technique considers three parameters, namely *performance, risk,* and *cost.* Finally, we show the use of the Viable System Model in building viable information systems.

Further research, may elaborate on the IS evaluation technique and provide a formal specification of it. Moreover, the process-oriented risk modeling diagrammatic technique presented in Section 4 requires further elaboration so as to become an integral part of business (and IS) process modeling.

6. REFERENCES

Ashby, R.W. (1964). *An introduction to cybernetics.* Chapman and Hall, London.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems,* **1**(2), pp.121-130.

Baskerville, R. (1997). New organisational forms for information security management. In Proceedings of the IFIP/TC11 13th International Conference on Information Security, May 1997, Copenhagen.

Beer, S. (1984). The Viable System Model: its provenance, development, methodology and pathology. *Journal of Operational Research Society,* **35,** pp.7-26.

Beer, S. (1979). *The heart of the enterprise.* John Wiley, Chichester, England.

Beer, S. (1981). *Brain of the firm.* (2nd Edition) John Wiley, Chichester, England.

Brocklesby, J. and Cummings, S. (1996). Designing a viable organization. *Long Range Planning,* **29**(1), Elsevier Science Ltd.

Checkland, P. and Holwell, S. (1998). Information, systems and information systems. John Wiley and Sons, Chichester, England.

CSI – Computer Security Institute (2000). *Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey.* Computer Security Institute, USA.

Davidow, W. and Malone, M. (1992). *The virtual corporation,* Harper Business, New York.

Ellison, R., Fisher, D., Linger, R., Lipson, H., Longstaff, T. and Mead, N. (1999). Survivable systems: an emerging discipline. In the proceedings of the 11th Canadian Information Technology Security Symposium (CITSS), Canada.

Ellof, M. and von Solms, S. (2000). Information security: process evaluation and product evaluation. In the proceedings of IFIP/TC11, 16th Annual Working Conference on Information Security, August 2000, China.

Ernst&Young (2000). 2nd Annual Global Information Security Survey. Ernst&Young LLP, USA.

Hitchings, J. (1996). Achieving an integrated design: the way forward for information security. In Ellof, J. and von Solms, S. (eds), *Information Security – the Next Decade,* IFIP SEC'95, Chapman & Hall, London.

Jayaratha, N. (1994). *Understanding and evaluating methodologies: NIMSAD, a systemic framework.* Mc Graw-Hill, London

Lipson, H. and Fisher, D. (1999). Survivability – a new technical and business perspective on security. In the proceedings of the New Security Paradigm Workshop June 1999, Canada.

Mayer, R.J., Benjamin, P.C., Caraway, B.E. and Painter, M.K. (1995). A framework and a suite of methods for business process reengineering. In Grover, V. and Kettinger, W.J. (eds), *Business process change: concepts, methods and technologies.* IDEA Group Publishing, Harrisburg, USA.

Mowshowitz, A. (1997). Virtual organization. *Communications of the ACM,* **40**(9), pp. 30-37 .

Parker, D. (1996). A new framework for information security to avoid information anarchy. In Ellof, J. and von Solms, S. (eds.), *Information Security – the Next Decade,* IFIP SEC'95, Chapman & Hall, London.

Warren, M. (1996). *A security advisory system for healthcare environments.* PhD Thesis, University of Plymouth. U.K.

Winograd, T. and Flores, F. (1986). *Understanding computers and cognition: a new foundation for design.* Addison-Wesley, USA.

Yngstrom, L. (1996). A holistic approach to IT security. In Ellof, J. and von Solms, S. (eds.), *Information Security – the Next Decade,* IFIP SEC'95, Chapman & Hall, London.