Looking for Security-Oriented Information Systems: Risk Perception and Management in Italian Companies

Roberto Palmieri
Università Bocconi, Istituto di Organizzazione e Sistemi Informativi
SDA Bocconi, Area Sistemi Informativi, Italy,
roberto.palmieri@unibocconi.it
Antonio P. Volpentesta
Università degli Studi della Calabria, Italy,
Dipartimento di Elettronica, Informatica e Sistemistica
volpentesta@deis.unical.it

Paper prepared for presentation at the 99th EAAE Seminar 'Trust and Risk in Business Networks', Bonn, Germany, February 8-10, 2006

Looking for Security-Oriented Information Systems: Risk Perception and Management in Italian Companies

***Roberto Palmieri*[1] *and Antonio P. Volpentesta*[2]**
[1]*Università Bocconi, Istituto di Organizzazione e Sistemi Informativi*
SDA Bocconi, Area Sistemi Informativi, Italy,
[2]*Università degli Studi della Calabria, Italy,*
Dipartimento di Elettronica, Informatica e Sistemistica
roberto.palmieri@unibocconi.it, volpentesta@deis.unical.it

Abstract

This paper presents the results of an empirical investigation concerning the approaches adopted by Italian companies in dealing with information security issues. Such results are compared to an ideal, integrated information system planning approach where information needs and risk management are jointly taken into account. Data analysis shows that respondents ascribe to information security a rather high relevance for their business, and there is a formal conformity of business practices to the phases included in the proposed model, especially as far as high level, conceptual activities are concerned. Despite that, in the companies which have been examined, security systems appear to be still inadequate, especially as far as organizational issues are concerned.

Keywords: *security-oriented information systems, information security, risk perception, integrated planning model, empirical results*

1. Introduction

In recent years the strategic importance of intangible assets – that is, trust relationships with customers, suppliers and business partners, know-how, brand visibility, ability to innovate, market knowledge, business culture etc. - has greatly increased. Today, nearly all companies have a market quotation that exceeds their financial capital (Daum, 2002). In many cases the relationship between intangible capital and book value is comprised between five and sixteen (Stewart, 1999) especially in those fields characterized by largest investments in Research and Development, such as Pharmaceutics (Strassman, 1999). Provocatively, the economic importance of intangible capital could be associated with the difference between company market values before and after an accident erases all the information from any supports it is stored in (Nasseri, 1996). Actually, the growing spread of practices for information sharing and exchange via Internet, which favor the access to and the valorization of immaterial products and contents (Porter, 2001), dramatically increases the risks of incidents that directly trouble information resources and eventually, as a consequence, other intangible assets. Observing in figure 1 the evolution of the number of Internet Hosts since 1990 (ISC, 2005) and comparing it with the dynamics of computer incidents (figure 2) registered by CERT (1988-2005), a strong correlation can be easily found, on a temporal basis, between the spread of Internet-based business activities and incident occurrences.

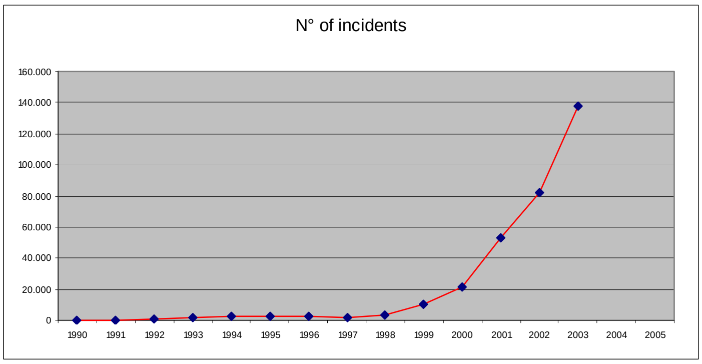

Figure 1. n. of Internet Hosts created from 1990 to 2005 (source:ISC, 2005; www.isc.org)

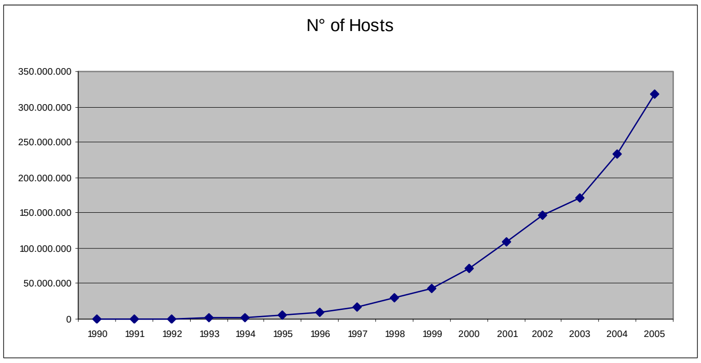

Figure 2. n.of incidents annually reported to CERT from 1990 to 2003 (source: CERT; www.cert.org)

Moreover, from the second half of the 90's both trends assume an exponential course. In this context, are emerging several information security issues that demand more attention than in the past from the managerial point of view. Organizations are facing new and multiple security threats such as computer fraud, theft of classified information, computer viruses, hacking, web site defacement, flooding, sabotage and denial of service attacks that very much impact, directly or indirectly, on trust and business value. These threats have become more and more frequent and sophisticated, while the transition towards distributed organizational structures and ICT architectures has weakened the effectiveness of control, becoming one of the main causes of business vulnerability increase. Such weaknesses correspond to inborn gaps in the change management process, especially due to the insufficient ability in managing coherently the design and implementation of important modifications in information systems, organizational models and operating procedures. Due to such a wide variety of risk typologies, sources and impacts, companies must define suitable policies and programs in order to implement security systems which can provide information resources with protections finalized to their own strategic business goals. Unfortunately, very often, information security is still perceived as an emergency issue, meaning a set of ex-post technical interventions to be carried out in order to minimize costs. Therefore, from the point of view of business management, one important step to be undertaken consists in understanding how the perception and management of these risks can be integrated in information processes according to a security-oriented perspective.

The paper is organized as follows: section 2 presents an organizational approach to effective information security management; section 3 summarizes an integrated planning approach for security-oriented information systems; section 4 reports some empirical evidence about the level of adoption of such an approach in a sample of Italian companies, and section 5 ends with conclusions.

2. Effective Information Security Management

Information security, that is the protection of intangible resources, cannot be limited only to the defense of the technical means employed for information processing and communication. On the contrary, it must be conceived as a continuous managerial process: it regards decisions to be taken under conditions of bounded rationality, within a complex and dynamic context. This managerial vision is supported by the evolution of quality assurance procedures for business production processes, which draw growing attention to the information system as an essential production infrastructure and to it's embedded security as an essential pre-requirement to standard compliance (BSI-DISC Committee, 1999).

In particular, an effective information security management system is based on some fundamental requirements: **confidentiality** (the ability to limit access to information resources only to those who are authorized and according to proper modalities), **integrity** (the ability to avoid improper modifications), **availability** (the ability to guarantee authorized customers well-timed access to resources in order to meet their specific operational needs).

Similar to any other investment, information system security must be estimated in both monetary and strategic terms, in order to assure that the cost of control does not exceed the value of benefits expected in terms of risk reduction. Therefore, the choice and successive implementation of security measures are a direct consequence of the importance and value of the resources to be protected, of the specific risks they are subordinated to and of the peculiar organizational structure, including the information system configuration. On the other hand, security measures aiming at the prevention of harmful events are not able to guarantee absolute immunity, although they are expected to lower the risk of incidents. The transition towards information systems characterized by network-based architectures and growing levels of complexity, has made the concept of "total security" inconsistent, imposing the companies to arrange measures for managing also security emergencies. Therefore, preventive measures must be integrated by a proper ability of the company to react to incidents (Allen & Sledge, 2002). Reactive measures are based on continuous control, skilled security managers, customer training as well as on planning suitable organizational procedures in order to promptly restore the *ex ante* situation. Prevention and reactivity represent two complementary elements, crucial in order to effectively face the inner/outer-company threats which the information system is potentially called to deal with.

Experience has demonstrated there are some critical factors that determine the effectiveness of an information security management program (BSI-DISC Committee, 1999).

Information Security Policy expresses the objectives, principles and reference guidelines which are used as input to security planning. In particular, the information security policy should be formally approved by the top management, published and properly communicated to all employees in order to bear witness of company management commitment. Its main elements are (Cresson & Wood, 2005): the objectives of information security, whose definition is related to the organization and its intangibles; the commitment of top management in supporting the objectives, from which the legitimacy and authority of the security manager also depend; security requirements and minimum-level standards; responsibilities of middle management and staff; incident reporting procedures. Because of its importance, the policy must be updated by the information security manager according to important modifications in the reference context (strategic changes, significant organizational or technological modifications, new vulnerabilities, new threats, incidents of remarkable entity).

Information Security Risk Analysis is the second main input to security management. In brief, it consists of the following activities (Peltier, 2001): survey of information system resources and analysis of their vulnerabilities; identification of threats; risk assessment and definition of intervention priorities; definition of protection measures typologies (prevention vs. reaction). Analogous to security policy, risk analysis activity should be carried on by the information security manager, who should also reiterate the analysis periodically or as a result of sensitive changes in the business context.

Information Security Planning is concerned with a series of activities meant for translating the policy principles and the results of risk analysis in operational plans. In the successive implementation stages, these plans will become the inputs for the definition of technical details and for the deployment of the correspondent security mechanisms. The main activities are: identification of critical elements to be protected (plan objectives), evaluation of actual threats to critical resources, specific risk analysis, definition of security functions, feasibility study and "project portfolio" determination, project selection and scheduling.

Implementation and Control begins with the formalization of the solution’s technical details, the definition of the mechanisms necessary to carry out the security functions, the acquisition of devices and their installation. The documentation of organizational procedures and behavioral rules is carried out as well. This stage practically puts into effect the policy principles by defining, in particular, control mechanisms and incident reporting activities (procedures, responsibilities, sanctions, etc.). In case of incidents, other issues are to be faced: the definition of intervention and outsourcer involvement procedures; the coordination between first-level intervention managers and security experts; the coordination with geographically dispersed units; the priority to be assigned to services during recovery etc. After a test activity, the new security system finally enters the operational stage. Monitoring takes place by means of continuous control activities. Una-tantum check-up activities and gap analysis between results and expectations may imply to reiterate the planning process in order to correct system failures or weaknesses.

3. An integrated approach to security-oriented information system planning

The organizational perspective induces the need for a structured, managerial approach in which information system planning and information security planning are integrated in order to better achieve company strategic goals (Palmieri & Marzotto, 2003). There are various points of contact between the two planning processes:

- information systems are the object of information security, which provides technical and organizational measures to make it compliant with the objectives defined by the security policy. On the other hand, information system development is constrained by the security requirements of the company. Ignoring this constraint in the evaluation of information system projects means neglecting serious economic, technical and organizational issues;
- both processes must guarantee the best possible use of information assets at business performance purposes: the analysis of information flows and the resource classification according to their strategic value represent in both cases fundamental stages;
- information system planning and information risk management are not standalone activities, but synergic means in the pursuit of company strategic objectives.

Therefore, the two processes shouldn’t be rigidly distinguished and security costs are not to be seen as a power subtraction from information system development. Although an information security plan can theoretically be developed in whichever stage of an information system life cycle, a more appropriate approach consists in contextually arranging both the security plan and the information system plan in such a way that security functions are identified before running the system. As a matter of fact, the implementation of these functions when the system is already operating would be more difficult and present higher costs and difficulties for the users. Moreover, implementing new security functions as a response to an incident, a system violation or a failure, often is also less effective than an ex ante definition. Hence, an approach to security based on the pure reaction to harmful events turns out to be incompatible with organizational effectiveness and efficiency requirements. Moreover, the definition of security functions within the information system planning allows a more accurate estimation of the projects in the feasibility study.

A framework for an integrated management model of the two planning processes consists of the following steps (Palmieri & Marzotto, 2003).

Definition of the intervention areas (plan objectives)

Apparently, the objectives and peculiar activities of the two processes are distinguished: whilst information system development should mainly take care of identifying unsatisfied information needs, information security planning must define the requirements and security functions that the information system should have to satisfy. Actually the two processes, besides the alignment of high-level strategies, also have in common the role of proposing new original strategic lines able to generate competitive advantages and, consequently, value for the company. Moreover, there is also a strong correspondence of objectives and methods between the definition of information needs and the security functions. In fact, both activities are based on the analysis of data and information flows with the aim of discovering information gaps rather than unsatisfied security needs. There is even a strong link between information gap analysis and risk analysis. The level of information risk that characterizes an organization depends on the configuration of its information system, so planning a lower risk level often means impacting on system configuration. Vice versa, planning substantial system modifications has an unavoidable impact on security. Because they are two parts of the same system, information system and information security are in an equilibrium status which is disturbed every time intervention occurs on one of the two elements. This strong interdependence leads to yearn for a combined and coordinated activity in defining intervention areas while avoiding the adoption of incompatible solutions. However, the main unifying element lies in data classification and information flow analysis which allow the definition of security functions and the design of the new information system. Both the quality of the planning process and the effectiveness of an integrated approach very much depend on these activities.

Definition of solution’s functional details associated to individual objectives.

At this stage the level of detail at which IT applications are defined is often rather insufficient (usually, the technical details are in fact defined later during the design stage), therefore projects are still indefinite. Since the new system architecture is unknown, it is hard to coordinate system development with security requirements: there are too many implementation alternatives. Therefore, priority is given to the functional definition of the application solution, giving the security experts a generic consulting and control role.

Feasibility study

Security measures are now analyzed and evaluated along with the technical, economic and organizational aspects of the application project. In particular, an analysis is performed on the technical chance to keep the new project related risk within the standards fixed by the security policy, on the sustainability of organizational impact related to the new security measures and on the cost of control.

Selection and scheduling

Projects are finally evaluated according to their suitability, ranked and scheduled with respect to their priorities, while the necessary financial and human resources are assigned to carry them out.

Empirical Evidence from a sample of Italian Companies

Which is the perception of information risk? Is security considered a cost that takes resources from the development of information systems or an investment that creates value for the company? Is the information security problem managed by patches or in a process perspective with the objective of developing security measures coherently with company strategies? Are there company organizational units or professional figures that are specifically responsible for information security in its strategic meaning? Answering these questions through an empirical survey has a twofold objective: by one side, we need to shorten the substantial information deficit that still characterizes these issues; on the other hand, a deeper knowledge of this phenomenon enables us to test theory-based information security models, in particular the integrated planning model proposed, with respect to companies' actual practices. Results are presented from an empirical survey on a sample of 400 Italian companies with an Internet connection (Palmieri & Marzotto, 2003). This sample has been formed according to the dimensional, territorial and industrial distribution adopted in the latest ISTAT census, with a minimum €15.000.000 turnover limit for companies not belonging to Public Administration.

Information Security Perception and Managerial Approach

The respondents believe information security is fairly important for their business (about 7/10 in average). Among the three main information security requirements - availability, integrity and confidentiality - availability is slightly considered the most critical, highlighting a certain emphasis on business continuity. From a methodological perspective, a substantial formal correspondence is found between business practices and the activities that characterize the proposed integrated planning model. This applies in particular for the more conceptual activities of the security strategy definition process – resource classification, definition of objectives and security functions - while more operative activities of the process - definition of measures, technical details and choice of security products/services available on the market - are considered less critical and are not generally included among the company inner-activities (Figure 3).

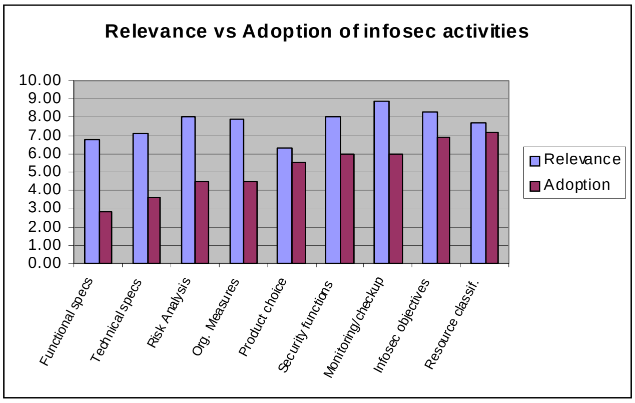

Figure 3. Relevance and adoption of information security activities (activity data are reported in %)

As far as risk analysis is concerned, a significant inconsistency is found: a poor percentage of respondents that declare to carry this activity out (45%) corresponds to one of the highest critical values found (more than 8/10). It can be then assumed that the effort required to classify information resources, and the complexity that characterizes risk analysis techniques (both monetary and qualitative) represent significant obstacles that turn into serious operational difficulties in its execution. This discloses cognitive and methodological inhibiting factors towards an effective management of information risk. In the definition of technical and functional details a rather high differential between perceived criticality and percentage of respondents that carry them out is also observed. This reveals that, although specification definition is considered very important, it isn't normally carried out inside the company but outsourced from product/service dealers (consultants or technology suppliers), who are more capable of monitoring the rapid evolution of the market. Lastly, the attention to information security is demonstrated by the percentage of respondents (82%) who declare to have their own policy at work, even if only in 35% of the cases such policy is formalized and in 4% an ad hoc company communication program is provided (Figure 4).

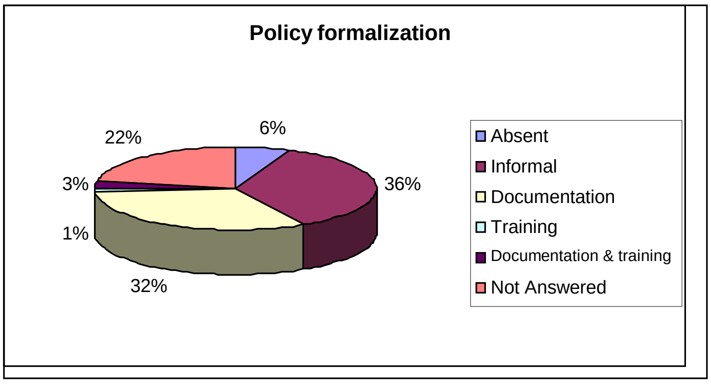

Figure 4. Security Policy level of formalization

Organizational Issues

Although above data prove a formal conformity between business practices and the integrated planning model, further analysis shows a certain difficulty in adopting an organization which is coherent to the model. Only one company out of four has a unit specifically dedicated to manage information security. In the remaining cases - with the exception of a minority (10%) that exclusively turns to external consultants - security is managed by the information system department. Moreover, even when a dedicated unit is formally established, in 55% of the cases it hierarchically depends from the information system department. The non-distinction of roles between information and security systems, however, is confirmed by the distribution of responsibilities: even among companies that have a dedicated information security department, strategic choices relating to security are charged to the information system manager in 60% of the cases, against 13% in which they are meant for the security manager (Figure 5). Instead, expenses are generally delegated to the latter (44% of the cases), as shown in Figure 6.Figure

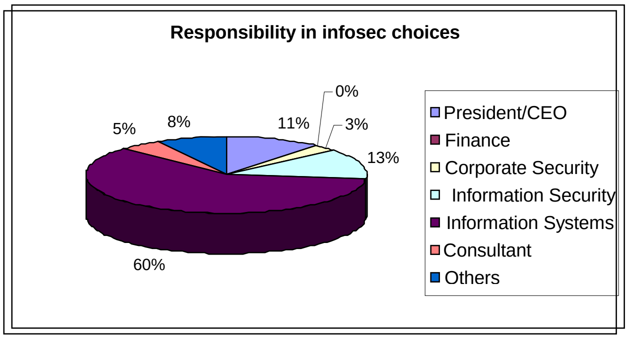

Figure 5. Responsibility in information security choices

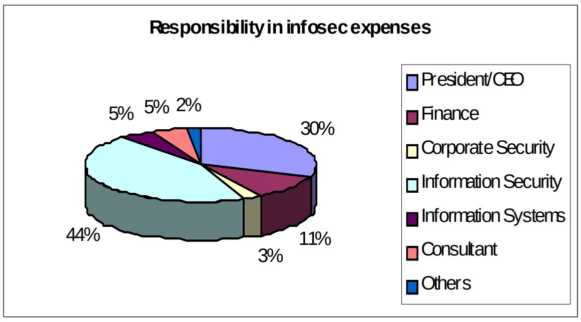

Figure 6. Responsibility in information security expense

The most outstanding element, so, is a muddled mixture between ICT decisions and security choices, which is in contrast with the necessity to implement specific information security responsibilities and control roles, as highlighted in the integrated planning model. This situation likely reveals the persistence of the concept that security is just a limit to information system management and, therefore, information security has a marginal role in the definition of company strategies.

Vulnerability, technical orientation and organizational gaps

Among the companies that declare to have suffered at least one incident in the last year, less than 50% have subsequently been capable of carrying out the corresponding protection measures, and their evaluation of the current system capability to reach prefixed objectives is not generally that much reassuring (6,5/10). In order to match protection requirements, in 88% of the cases they believe preventive security measures are more effective than reactive ones, and in 92% of the cases they consider prevention as a priority for the future. The limits in protecting effectively information resources are due to technological causes only in minimal part (12%). On the contrary, the main reasons of the inadequacy lie in organizational causes: poor management support (16%), scarcity of resources (23%), lack of competences (15%), training shortage (14%), absence of proper policies (13%). Organizational difficulties are also revealed by control procedures inefficiencies. Lastly, the fact that 64% of those interviewed expect that in the next year no incidents will involve their own information system shows a limited perception of information security among the responding companies. In fact, this expectation is essentially due to their confidence in technology robustness and to a substantial underestimation of the potential risks burdening immaterial resources, which is promptly confirmed by a low percentage of respondents (7%) that mention threat dynamism as one of the causes why their own security systems could fail.

5. Conclusions

The situation that emerges from the empirical analysis can be summarized as follows:

- there's a substantial formal correspondence between stages that characterize the integrated planning model and business practices;
- information security is generally considered a rather important factor for company success, especially in consideration of the need to guarantee business continuity by means of data and information availability;
- business practice shows insufficient emphasis and poor operational ability with reference to the criticality of information security;
- companies are not particularly worried about the occurrence of possible incidents involving their intangible capital;
- no prevailing model emerges with regard to the assignment of responsibility for company information security;
- security systems are still rather modest, especially with reference to organizational aspects.

The sampled Italian companies have approached security mostly in a technological way. Probably, the need for formal compliance with an increasing number of laws that impact on information security (privacy, digital document, copyright etc.) has pushed the implementation of technical measures that seem to have given companies a certain sense of invulnerability. Although those interviewed declare to carry out a fairly good part of the activities included in the proposed model, however an approach to security which is coherent with the need for strategic management of intangible assets in network-based business contexts is substantially absent.

References

Allen J.H., Sledge C.A, 2002, Information Survivability: Required Shift in Perspective, CrossTalk-The Journal of Defense Software Engineering, July (http://www.hill.af.mil).

BSI-DISC Committee, 1999, Information Security Management. Part 2: specification for information security management systems, BS 7799-1:1999, British Standard.

CERT Coordination Center, CERT/CC Statistics 1988-2005 (http://www.cert.org)

Cresson Wood C., 2005, Information Security Policy Made Easy, vs. 10, Information Schild Inc., Houston, Texas.

Daum J.H., 2002, Intangible Assets and Value Creation, Wiley, New York.

ISC, 2005, ISC Domain Survey: Number of Internet Hosts (http://www.isc.org).

Nasseri, T., 1996, Knowledge Leverage: The Ultimate Advantage, BRINT (www.brint.com).

Palmieri R., Marzotto M., 2003, La gestione del rischio informativo nelle imprese italiane, research report, SDA Bocconi., June.

Peltier T.R., 2001, Information Security Risk Analysis, CRC Press LLC, Boca Raton, Florida.

Porter, 2001, Strategy and the Internet, Harvard Business Review, March.

Stewart T.A., 1999, The New Wealth of Organizations, Doubleday, New York.

Strassman P.A., 1999, Does Knowledge Capital Explain Market/Book Value ?, Knowledge Management Magazine, September.