Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2007 Proceedings

European Conference on Information Systems (ECIS)

2007

A Framework for Managing Predictable and Unpredictable Threats: The Duality of Information Security Management

Paolo Spagnoletti
CeRSI – LUISS, pspagnoletti@luiss.it

Andrea Resca
CeRSI–Luiss "Guido Carli" University–Rome, Italy, aresca@luiss.it

A FRAMEWORK FOR MANAGING PREDICTABLE AND UNPREDICTABLE THREATS: THE DUALITY OF INFORMATION SECURITY MANAGEMENT

Paolo Spagnoletti, CeRSI - Luiss "Guido Carli" University, Rome, pspagnoletti@luiss.it

Andrea Resca, CeRSI - Luiss "Guido Carli" University, Rome, aresca@luiss.it

Abstract

Information systems security is a challenging research area in the context of Information Systems. In fact, it has strong practical implications for the management of IS and, at the same time, it gives very interesting insights into understanding the process of social phenomena when communication information technologies are deployed in organizations. Current standards and best practices for the design and management of information systems security, recommend structured and mechanistic approaches, such as risk management methods and techniques, in order to address security issues. However, risk analysis and risk evaluation processes have their limitations, when security incidents occur, they emerge in a context, and their rarity and even their uniqueness give rise to unpredictable threats. The analysis of these phenomena which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach which is able to examine and interpret subjectively the detail of each incident. The aim of this paper is to highlight the duality of information systems security, providing an alternative view on the management of those aspects already defined in the literature as intractable problems and this is pursued through a formative context (Ciborra, Lanzara, 1994) that supports bricolage, hacking and improvisation .

Keywords: IS security, risk analysis, security incidents, drift, formative context

1 INTRODUCTION

Despite the trend in IS security, research is moving away from the narrow technical viewpoint, the socio-organizational perspective in dealing with security issues is still at an early stage (Dhillon & Backhouse 2001). Several research efforts in the field of interpretive analysis face the lack of any prescriptive component, and the apparent lack of value to the security manager. On the other hand, approaches based on the measurement and control of variables, following the positivist methodology, demonstrates limitations when applied to social phenomena. In fact, the simplification and abstraction needed for good experimental design can remove enough features from the subject of study that renders only obvious results possible (Kaplan & Duchon 1988).

In the IS domain, information security is a challenging research area. In fact it has strong practical implications for the management of Information Systems and, at the same time, it offers us very interesting insights into understanding the process of social phenomena when communication information technologies are deployed in organisations. Despite several research efforts that have been conducted within the academic community in order to understand which are the main issues in managing IS security, a prevalent part of the literature still refers to standards and best practices for the definition of concepts and methods to prevent, detect and react to computer incidents. This is in part due to the issues in developing theories, using widely accepted methods grounded in the positivist perspective, in a field where it is difficult to collate data in order to develop and test generalised solutions. Moreover, widely accepted structured and mechanistic approaches, such as risk management techniques, have proven to be limiting in their ability to predict computer incidents, especially those dependent on the behaviour of internal actors.

From this perspective, the subdivision of threats into predictable and unpredictable threats seems fruitful. These diverse threats are disparate in nature, and are characterised by a duality. That is to say their management requires a different perspective to maintain the IS security. This duality is reinforced by the fact that the nature of the threats requires a specific epistemological approach. Predictable threats seem apt for being investigated through positivist approaches, whereas unpredictable threats lend themselves to interpretive approaches.

The paper is organized as follows. Firstly, current approaches in the IS security management and their focus on predictable threats are introduced. An analysis of unpredictable threats follows, which will examine the limits of an integrated epistemological perspective. The concept of formative context is then presented as the instrument for outlining an organizational measure apt for managing these threats. A discussion of results and conclusions brings this paper to a close.

2 COMMON APPROACHES TO IS SECURITY MANAGEMENT

Information system security is often defined in the practitioners' literature as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. The three widely accepted information security requirements are confidentiality, integrity and availability. Security administration is considered to be a management and not purely a technical issue. Therefore the establishment, maintenance and continuous updating of an Information Security Management System (ISMS) provides a strong indication that an organisation is using a systematic approach for the identification, assessment and management of information security risks. Furthermore, such a company will be capable of successfully addressing information confidentiality, integrity and availability requirements.

In order to better understand the systematic approach to information security management, we need to introduce some of the concepts used by standards and best practices. Looking at standards, many models are available, especially within the quality management area, which describe the common stages for managing the security of information systems. For example the PDCA cycle, described in the quality management literature by Deming (1986), consists of the four stages: plan, do, check and act. This model is adopted by the ISO27001 standard (ISO/IEC 2005) to describe the process for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's Information Security Management System (ISMS). A similar structure, based on a cyclical sequence of stages, can be found in other methods for the management of IT systems (see for example the COBIT 2005 framework). In fact, the adoption of the PDCA model reflects the principles set out in the OECD Guidelines (2002) governing the security of information systems and networks. Focusing on each stage of the above mentioned model, we find two main classes of activities. Firstly, the evaluation activities performed by the management of IS security, which consists of both the assessment of the current information security situation ("plan"), and the review of risk assessment results ("check"), taking into account several change factors such as the effectiveness of the implemented controls, and external events, etc. This phase is related to the initial evaluation of IS security and to the review of the overall ISMS. Secondly, the activities performed by the organisation in order to implement and operate ("do") and to maintain and improve ("act") the ISMS (See figure n. 1).

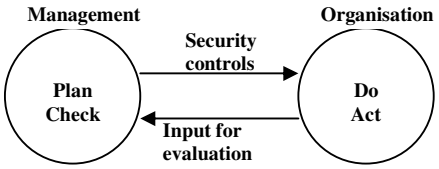

Figure 1. Common stages of an ISMS

Our attention will now concentrate on the management activities which are focused on the selection of security controls based on the results of the evaluation process performed in the organisation. In our opinion, the evaluation process, which is mainly based on a risk assessment approach, represents the most critical part of all these approaches based on this model and hence all of the widely accepted standard based approaches.

In the description of the "Plan" stage of the ISO27001 standard, the definition of a risk assessment approach is required for the organisation. Moreover, the organisation should "identify a risk assessment methodology that is suited to the ISMS, and to the identified business information security, legal and regulatory requirements" (ISO/IEC 2005). Furthermore, the organisation should "develop criteria for accepting risks, and should identify the acceptable levels of risks". This risk assessment methodology "shall ensure that risk assessment produce comparable and reproducible results". The same standard defines risk assessment as the "overall process of risk analysis and risk evaluation".

Traditional risk assessment processes are designed to identify (1), analyse (2) and evaluate (3) threats and vulnerabilities in order to decide on the appropriate measures and controls to manage them. A detailed and updated description of risk management concepts and methods, has been published recently by the ENISA Agency (ENISA, 2006). Here we summarize some of the information related to the three phases of the risk assessment process. During the identification phase (1), threats, vulnerabilities and the associated risks are identified. This process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. Methods and tools used to identify risks and their occurrence include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques. The risk analysis phase (2) involves a thorough examination of the risk sources, of their consequences

and of the likelihood that those consequences may occur. Moreover, it involves the assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks. The level of risk can be estimated by using statistical analysis and calculations combining impact and likelihood. Information used to estimate impact and likelihood usually comes from past experience or data and records (e.g. incident reporting), reliable practices, international standards or guidelines, market research and analysis, experiments and prototypes, economic, engineering or other models, and specialist and expert advice. Risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources. Analysis may be qualitative, semi-quantitative or quantitative or a combination of these. Finally, during the risk evaluation phase (3) decisions have to be made concerning which risks need treatment and which do not, as well as focusing on the treatment priorities. Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the context of risk management.

Risk analysis is a well established technique with a long history. The limitations of risk analysis have been widely recognized for many years. In a recent work, Baskerville (2005) describes two intractable problems that limit the effectiveness of common risk analysis practices. These problems include the lack of reliable empirical data concerning the frequency and amount of losses attributable to information security compromises, and the relative rarity of many kinds of information security compromises. In fact, the collection of incident data is often collated after the incidence with questionable thoroughness and accuracy. Moreover, managers consider this data extremely sensitive and highly confidential. Therefore, there is very little motive for any organization to disclose data regarding the costs and frequency of information security compromises. The second intractable problem in information security risk analysis is related to the invalidity of probability arithmetic where the attacks are uniquely targeted, and of a relatively low frequency (i.e. insider fraud). However, the ability to communicate to general management the expert opinions concerning an organization's information risk profile in terms of threats and safeguards, is often recognized as the best risk analysis characteristic (Baskerville, 1991).

3 THE NATURE OF UNPREDICTABLE THREATS

In order to study the IS security phenomenon, an analysis of the nature of information systems is considered a prerequisite. Only from a deep understanding of the role of information and communication technology (ICT) in the organizational life can it throw light on the different aspects that determine security. Moreover, this technology is playing an ever-increasing role in organisations: intra- and interorganizational coordination, knowledge sharing, standardization of business practices are simple examples of some organizational objectives reached through a large implementation of ICT.

Enterprise systems (Gosain, 2004) and information infrastructures (Ciborra, Hanseth, 2000) outline an organizational scenario in which the role of ICT is pervasive. A scenario where business functions are tightly integrated, and the database is shared due to an enterprise system and where the notion of information infrastructures represents the integration of equipments, systems, applications and processes, at a corporate level, supporting people managing information and communications. This differs from the past, these systems and infrastructures connect multiple communities of practice whilst traditional systems tend to support a single community of practice.

From this perspective, ICT can be seen as an instrument capable of profoundly restructuring the organizational background. Practices and communications, the structure of organizational relationships and economic transactions can be completely redesigned. Nevertheless, the result of this organizational redesign is not easy to predict. Established practices and the presence of informal practices and rules based on a continuous evolutionary process interact with technical systems characterized by an immense range of actions. Therefore, the end result of the implementation process of these systems is an open issue, subject to varied and subtle factors (Chae, Lanzara, 2006).

The notion of drift has been introduced in order to further investigate these factors (Ciborra, 2002). Drift represents a phenomenon that can affect both technologies and processes when the result of an implementation process of a technological system does not match the original design. Two diverse, but at the same time intertwined dynamics are at the source of this phenomenon. On the one hand, the openness of the technology to the eventual re-inventions employed by users, and the unforeseeable technical interdependences based on the overlapping of old (legacy) and new platforms or on different standard interferences. On the other hand, actors, through unexpected interventions, tinkering and improvisations, can outline a new way of technology adoption.

According to this understanding, the term evolution does not seem appropriate to define this phenomenon. Evolution suggests an idea of a linear process of adoption, but this is not so in the case of enterprise systems and information infrastructures. Surprisingly, user resistance, and the eventual effective functioning of legacy systems and learning processes caused by the introduction of such innovation are elements that contribute to outlining an out of control scenario where surprises, inventions, obstructions, opportunistic behaviours and vicious circles give way to multiple forms of implementation according to different circumstances.

Moreover, Ciborra (2004) maintains that ICT is increasingly substituting the user's reality and life. Indeed, users entrust this technology in order to transform aspects of life like concern and care into a resource that can be formalated and calculated. However, formalizations and calculations can be considered the springboard for further concern that may require further formalizations and calculations and so on. Inherent in this discourse are the disruptive and potentially hazardous events that are not understood within the sphere of the formal knowledge related to the technology. The role played by ICT enables it to be engaged in courses of action that involve a higher level of uncertainty. To sum up, this is another side effect produced by the introduction of this kind of technology that significantly affects the level of security.

The objective of this digression is to throw light on the limits of risk analysis and risk evaluation for managing IS security. In this scenario, the above mentioned intractable problems emerge restricting the function of this analysis and evaluation: the lack of reliable empirical data regarding the frequency of losses, on the one hand, and the rarity of many kinds of these losses, on the other hand (Baskerville, 2005). In a context described by a phenomenon like drift, the rarity and even the uniqueness of security compromised events are no longer an exception, and the traditional instruments of risk analysis such as arithmetic probability becomes inadequate.

4 THE DUAL NATURE OF IS SECURITY

Straub and Welke (1998) maintain that the main objectives of IS security planning should be to deter, prevent, detect and pursue remedies and/or punishing offenders for abuses. These objectives should drive the selection of technical solutions in the design phase of an information security management system. From their perspective, computer incidents play a passive role in the research process, they are considered to be an undesired phenomenon and, in some sense, a fatality - a scenario that should not happen but sometimes can take place. Here incidents acquire a different meaning. They can be seen as an indicator of what effectively is occurring in an organization. A resource to understand how technology is employed which can then reconsider the functionality of these systems, which is a ray of sunlight in the obscure mechanisms that characterize the adoption of complex technical systems. Therefore, we can claim that computer incidents should be one of the main phenomena under investigation in the context of IS security research. In fact, this phenomenon is related both to the unpredictable behaviour of actors involved in the information system, and to the openness of technology.

From this perspective, new elements emerge. If users' unpredictable behaviours are examined, computer incidents in organizations can be considered strongly related to the subjective understanding of human actors interacting with a set of technical, formal and informal rules which are composed of the implemented Information Security Management System (ISMS) and the more general information

system. Losses in confidentiality, integrity and availability of data and communications, are at the centre of compromises in which organizational actors are the protagonists due to malicious or involuntary behaviours. One of the objectives of an ISMS is to reduce the risks that are represented by the notion of computer abuse and computer misuse. The former is intended as the malicious violation of formal or informal rules which regulate the use of technical systems in order to gain a personal tangible or intangible benefit. The latter is the violation of the same set of rules without the intentional consequences of the security of the information system. In our opinion, both kinds of computer incidents are extremely valuable for the IS researcher.

According to this understanding, a duality of IS security can be taken into consideration. On the one side, security has to face the incident issue. That is, those events that are produced by unpredictable users' behaviour due to both the nature of technology under examination, and the possibility of unforeseen practices. On the other side, security is constituted by a protection system against predictable threats. Breakdowns and other problems can be recurrent or identifiable.

5 COMBINING INTEPRETIVISM AND POSITIVISM: LEE'S INTEGRATED FRAMEWORK

The dual nature of security poses a problem for analysis. Is it possible to study a phenomenon so ambivalent to its method? Furthermore, which method simultaneously allows us to investigate the purely objective and recurrent threats, and which method allows us to investigate those unpredictable threats based on a specific situation? This twofold nature of IS security requires us to accept the existence of different levels of understanding when dealing with human behaviour.

In order to introduce a possible solution for demonstrating the feasibility of such a opinion, we present in this section an integrated framework proposed by Lee (1991) in the context of organisational research. We also apply the following three levels of understanding, defined in the framework, to concepts related to IS security:

- the subjective understanding, consists of everyday meanings and common sense notions in which observed human subjects see themselves and the organizational world around them;
- the interpretive understanding, consists of the organizational researcher's reading or interpretation of the subjective understanding, developed with the help of such methods as phenomenological sociology, hermeneutics, ethnography, and participant-observation;
- the positivist understanding, consists of theoretical propositions, manipulated according to the rules of formal logic and hypothetical-deductive logic, so that the resulting theory satisfies the requirements of falsifiability, logical consistency, relative explanatory power, survival. These theoretical propositions are not about people, but "puppets" which are supposed to think and act like the observed human subjects.

The cyclical relationships among these three levels of understanding is illustrated in the next figure.

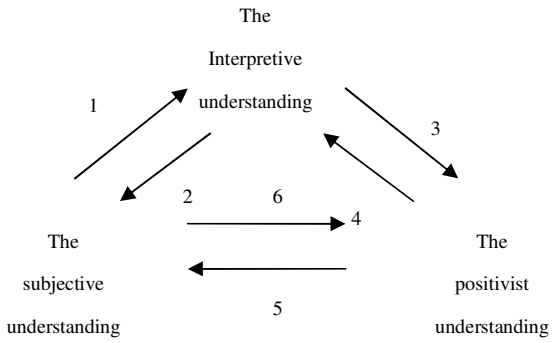

Figure 2. The integrated framework (Lee, 1991).

Arrows 1 and 2 represent the construction (1) and test (2) of the interpretive understanding performed by researchers through qualitative methods (i.e. phenomenological sociology, hermeneutics, and ethnography). The objective here is to reach an interpretive understanding and to test the coherence of the interpretation given to the subjective understanding of actors involved in computer incidents. In this phase the interpretive approach underlies an in depth analysis of computer incidents and contextual elements, based on data gathered from people, documents and computer systems (i.e. logs, files, etc.). The positivist understanding can then be developed on the basis of the results of the interpretive understanding and theoretical propositions are formulated in order to explain human behaviour. It is at this point that, Lee utilizes the Schultz' concept of "puppets" (1973), in order to adapt the positivist understanding to the social reality under investigation. This is carried out by the researcher who constructs puppets which are capable of thinking and acting like the observed human subjects. According to this aim, the researcher "endows the puppets with certain internally held values, specifies the variety of external opportunities and constraints that the puppets may encounter in their environment, and specifies the actions (the publicly observable behaviours), with which the puppets given their internally held values, may respond to the externally encountered opportunities and constraints". Arrows 3 and 4 refer to the formulation of theoretical proposition (3), using the rules of formal and hypothetico-deductive logic, and to the comparison (4) between the subjective meanings attached by human subjects to their actions and the subjective meanings assigned by researchers to the actions of the puppets. Finally, arrows 5 and 6 represent the predictions (5) and the confirmation/disconfirmation (6) of theoretical propositions through controlled empirical testing. Thus, human behaviours are predicted from the theory (5) and are tested (6) against actual behaviours, arising from the subjective understanding.

The above mentioned framework belongs to the body of contributions which advocate the integration of largely positivist and interpretive approaches (Lee 1991, Gable 1994). In a recent work and referring to the more general field of IS, Björn & Carsten (2006) claim that the question of 'paradigm incommensurability' regarding positivism and interpretivism must be seen as an open issue. Based on a variety of different arguments, Landry & Banville (1992) demonstrate how these paradigms can be seen as different but compatible views on the same research subject, but also as intrinsically contradictory. The twofold perspective depends on different definitions of positivism and interpretivism. The first viewpoint states that positivism and interpretivism feature distinct epistemological assumptions, but share the (ontological) 'real world' assumption. As a consequence of this perspective, interpretivism and positivism do not lead to different paradigmatic views on IS, but they do analyze IS differently. Also Orlikowski & Baroudi (1991) claim that "from the viewpoint of weak constructionism, interpretive research is understood to complement positivist research, that is, by generating hypothesis for further investigation, by filling in the positivist knowledge gaps the positivist research cannot attend to, such as the contextual exigencies, the meaning systems, and the

interaction of various components of a systems". From Lee's perspective, this integrated approach allows us to test both the validity of the positivist understanding, and of the interpretive understanding in a mutually supportive collaboration. Furthermore, this mutually supportive collaboration can also be conducted by different researchers across different studies.

6 PREDICTABLE AND UNPREDICTABLE THREATS: REVISITING LEE'S INTEGRATED FRAMEWORK

The fact that the Lee's approach tries to integrate the subjective understanding, the interpretative understanding and the positivist understanding can be of some help to us to investigate the IS security phenomenon according to its dual perspective. The reason for this is based on the fact that the question of security, which is related to the incident issue, tends to fall into the sphere of the subjective and interpretative understanding for its interpretation whilst the question of security against predictable threats tends to fall into the sphere of the positivist understanding. Indeed, the motivation is intuitive. Considering the nature of ICT, the permeating role played by enterprise systems or information infrastructures and the possible reformulation of procedures and practices employed by users, incidents can be considered as emerging phenomena which are context related and unpredictable in nature. Therefore, the analysis of these phenomena requires a theoretical approach which is able to examine the specifics of each incident, and only a subjective and interpretative understanding permits such an analysis. This differs from the analysis and survey of predictable threats which requires a different instrument of examination. In this case, the positivist understanding is more fruitful, because of the recurrence of these events, the rules of formal logic and the rules of hypothetical-deductive logic seem more appropriate for their analysis.

As it was mentioned above, Lee's approach consists of a cycle in which subjective and interpretative understanding are, in some sense, the engines of the positivist understanding. It is crucial to have a solid base on which to build theories that acquire their validity identifying regularities through, for example, statistical instruments. Furthermore, the analysis of incidents can effectively contribute to the development of a positivist understanding, and this aspect is not neglected in this analysis. Risk assessment, for example, is based on this presupposition. Therefore, a determinate range of events becomes determinable (see figure n. 3 "clear side").

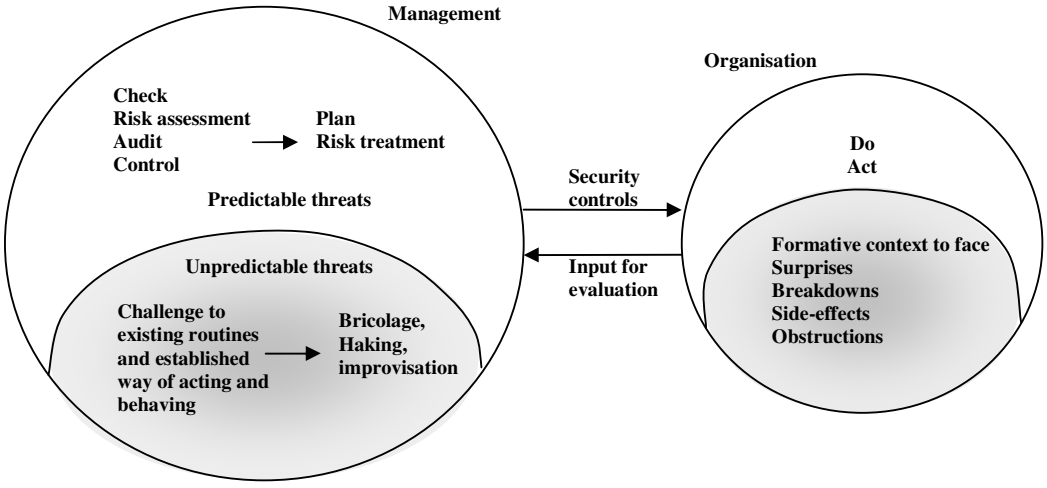

Figure 3. The duality of IS security

If the statistical incident analysis can be a source and identification of predictable threats, in some cases this could not happen. Following Baskerville (2005), it is possible to face intractable problems when the very nature of incidents is rare or even unique. Users' re-inventions and unforeseeable technical interdependences can determine short circuits, which are unpredictable and based on fortuitous events and pure coincidences.

In this case, Lee's integrating approach is no longer viable. The cycle that sees the subjective understanding, the interpretative and the positivist understanding supporting each other in order to provide a comprehensive theoretical approach has limitations, as a positivist understanding of these phenomena is impractical. Nevertheless, the same approach suggests that this is in the circle of subjective and interpretative understanding and that an analysis of these kinds of incidents should take place.

7 MANAGING UNPREDICTABLE THREATS: BRICOLAGE, HACKING AND IMPROVISATION

In some parts of this analysis, it has been suggested that incidents are context related. This means that these events, at least as far as it concerns the human actors perspective, can originate from specific dynamics of a determinate sphere. All of this suggests that the focus of analysis should move, and in some cases the organizational level, used so far, is not appropriate. Authors like Suchman (1987) and Lave and Wenger (1991) have introduced the concept of situational action and the community of practice respectively. These concepts define an environment that is less loose in respect to that one identified by the term organization. They underline a series of characteristics that adhere to a stricter social entity because of the social learning processes, identity, and shared preconceptions etc. In this understanding the concept of formative context is going to be introduced.

However, now, this concept will not be taken into consideration in order to investigate the reasons that cause a specific incident, but will focus on how these incidents can be prevented and managed. That is, what kind of interventions can be adopted, in this case, in order to reduce damages? Which organizational measures should be taken in advance for managing critical situations? Unger (1987) was the first to introduce this concept but this paper will seek to examine this concept's interpretation according to Ciborra and Lanzara (1994). The subjective and the interpretative understanding of the formative context is based on a twofold analysis that considers structural aspects and cognitive aspects as well. In other words, by formative context we mean the institutional instruments and mechanisms, and the cognitive images and presuppositions associated with them, that the actors bring to the organization and that they habitually use in action situations. For example, if the hierarchy is the formative context, it can be assumed, on the one hand, that there exists a specific division of labour inside a typical hierarchical organizational chart in which any member holds an established role (institutional arrangements), and on the other hand, it can also be seen as a way of reasoning, of solving problems and of executing tasks imbued with the hierarchy (cognitive frames), often without questioning the legitimacy of these actions. This means that the combination of institutional and cognitive aspects allows us to investigate the background, which often occurs without questioning the legitimacy of such an action, that influence both the individual subjects' interpretation of the different organizational dynamics and the routines and forms of coordination that characterize those dynamics.

The objective, now, is to see if the concept of formative context can be of some help to face rare or unique incidents. In other words, which institutional arrangements and cognitive frames allows us to face, in some way, those incidents that, because of their very nature, are not predictable? Which countermeasures can be adopted in order to manage situations characterized by breakdowns, surprises and side-effects? Following Ciborra's work (1992), a formative context capable of managing these situations should characterize itself because of cognitive and institutional structures that challenge existing routines, and established ways of acting and behaving. A context where learning and innovation are favoured in respect to monitoring and control, where deviations and mismatches are seen as raw material for outlining new practices and where bricolage, improvisation, and hacking

rather than formalization and pre-planned ways describe the mode of operation (see figure n. 3 “dark side”).

Particularly, the terms bricolage, improvisation, and hacking may describe some characteristics of this formative context. Bricolage represents the capacity to tinker with the resources available. A group of elements are combined according to the needs of a specific context contributing to new ways of acting where technology and practices can be re-interpreted. Improvisation underlines the vision, the quick glance in which the situation appears, all of a sudden, under control and propitious for acting. Extemporaneity, suddenness and unpredictability characterize improvised human interventions. Hacking has acquired a negative meaning. However, in this case, it is not take on a negative connotation. Hacking can be considered as the ability to implement a specific programme of a common function in a creative and unusual way. What is considered important to underline about hacking is the fact that these interventions fit with the larger application environment even though technology is used according to improper modalities. If the term bricolage is more apt for outlining the intervention of organizational procedures, for example, hacking concerns the field of software engineering. Software programs are reinterpreted and used in an unorthodox way leading to new solutions. Moreover, hacking activities tend to develop in a different community from the environment in which software engineering is built up, where a clear division of labour between analysts, and application programmers etc. exists.

The hacker community introduces a characteristic of formative contexts that support bricolage, improvisation and hacking. Institutional arrangements and cognitive frames, in this case, are highly situated and shared by a minority that acts within the parameters of organizational systems. Only in this environment do interventions acquire the sense of timing and touch of the connoisseur. This does not mean that this community should be impervious to its surrounding environment. On the contrary, its contamination with new cultures and ideas, collaborations and cooperative undertaking can give rise to learning and other related innovations.

To sum up, bricolage, improvisation, and hacking may, in a paradoxical way, represent some countermeasures against unpredictable incidents. The development of a formative context that support these activities can constitute a significant part of IS security management.

8 DISCUSSION

The question of the management of predictable and unpredictable threats has already been investigated by Baskerville (2005) in his work “Information Warfare”. Specifically, he underlines that fundamental assumptions and premises distinguish the thinking not only in the business environment, but also in the information warfare environment. In fact, he proposes both a business and warfare paradigm. The former assumes that risks are predictable, measurable and persistent and they should be managed on the basis of the probability theory, quality improvement and an exploitation type of organizational learning rather than an exploration one (March, 1991). On the other hand, the latter assumes that risks are both unpredictable (not measurable) and transient and managed on the basis of the possibility theory, the agility theory and an exploration type of organizational learning rather than an exploitation one.

The perspective proposed in this paper is not dissimilar from Baskerville’s one. However, in this case, rather than outlining of a paradigm related to information systems security in the business environment and in the information warfare environment, an epistemological issue emerges. That is, a research activity based on positivist approaches seems more apt for investigating instruments to manage predictable threats and a research activity based on interpretive approaches seems more apt for investigating instruments to manage unpredictable threats. This means that the diverse nature of threats seems to require a diverse epistemological approach. To sum up, whereas Baskerville’s perspective focuses on the construction of a paradigm on the basis of the different environment in which the security issue emerges, here, the crucial point is the nature of the threats, which are

indifferent from the environment in which they take place and the adoption of an appropriate epistemological approach for their management.

9 CONLUSIONS

This paper provides a discussion on the duality of information systems security, where the main issue for the management has been identified in facing both a set of predictable threats and a set of emerging and context related intractable problems. In the first case, a number of methods and techniques are available with the objective of reducing risks through the selection of appropriate countermeasures at a technical and procedural level. For the second class of problems, the adoption of a new approach has been envisaged, based on the development of a subjective and interpretive understanding of actions surrounding human behaviour. According to its aims, the concepts of formative context have been presented and new elements such as bricolage, improvisation and hacking have been added to the traditional ISMS model. These elements should provide additional capabilities to management in respect to the well structured and formalized techniques based on monitoring and control. The assumption is that, in order to manage situations characterized by breakdowns, surprises and side-effects, it is impossible to evaluate the risks and to define an effective action plan. In this context, the ability to develop a formative context where learning and innovation are favoured, can force management to establish a more secure environment in their organizations.

This work also has implication for the IS researcher, in fact computer incidents reveal themselves to be an interesting phenomenon to focus on. Therefore, the development of a body of knowledge in which computer incidents are thoroughly investigated, for instance, through action research projects can dramatically increase the understanding of social phenomena and lead to the definition of new interpretative frameworks.

References

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

Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, ACM Computing Surveys, 25 (4)

Baskerville, R. (2005). Best Practices in IT Risk Management: Buying safeguards, designing security architecture, or managing information risk? Cutter Benchmark Review, 5(12), 5-12.

Baskerville, R. (2005) Information Warfare: a comparative framework for Business Information Security, Journal of Information System Security, 1 (1) pp. 23-50

Björn, N., Carsten, S.B., Criticality, epistemology, and behaviour vs. Design – information systems research across different sets of paradigms ECIS 2006 Proceedings.

COBIT (2005). COBIT 4.0 Control Objectives, Management Guidelines, Maturity Models. Retrieved 21 December 2005, from www.isaca.org/cobit.htm

Chae, B. and Lanzara G.F. (2006) Self-destructive Dynamics in Large-Scale Technochange and some Ways of Counteracting it, Information Technology & People, 19 (1), 74-97

Ciborra, C. (1992) From Thinking to Tinkering: the Grassroots of Strategic Information Systems, Information Society, 8, 297-309.

Ciborra C. (2002) The Labyrinths of Information, Oxford University Press, London

Ciborra C. (2004) Digital Technologies and the Duality of Risk, Discussion Paper n. 27, Centre for Analysis of Risks and Regulations at the London School of Economics and Political Science, London

Ciborra C. and Hanseth, O. (2000) Introduction: From Control to Drift in Ciborra C. and Associates (edit by) From control to drift: the dynamics of corporate information infastructures, Oxford University Press, London.

Ciborra, C.and Lanzara G.F. (1994). Formative Contexts and Information Technology: Understanding the Dynamics of Innovation in Organisations, Journal of Accounting, Management and Information Technology, 4 (2) 61-86.
Deming W. E. (1986) Out of the Crisis. Massachusetts Institute of Technology Center for Advanced Engineering, Cambridge MA, USA.
Dhillon, G. and Backhouse J. (2001) Current Directions in IS Security Research: Toward Socio-Organisational Perspectives. Information Systems Journal 11(2): 127-153
ENISA 2006 Inventory of Risk Management/Risk Assessment methods and tools. Retrieved 16 November 2006 http://www.enisa.europa.eu/rmra/rm_home.html
Gable, G. (1994) Integrating Case Study and Survey Research Methods: An Example in Information Systems, European Journal of Information Systems, Volume 3, Number 2, pp. 112-126.
Gosain, S. (2004) Enterprise Information Systems as Objects and Carriers of Institutional Forces: the New Iron Cage? Journal of the Association of Information Systems, 5 (4), 151-182.
ISO/IEC. (2005). ISO/IEC 27001: Information technology - Security techniques – Information Security Management Systems - Requirements
Kaplan B. & Duchon D., 1988, Combining qualitative methods in information systems research: A case study. MIS Quarterly, 12(4), 571-586
Landry, M., and Banville, C. "A Disciplined Methodological Pluralism for MIS Research," Accounting, Management & Information Technology (2:2) 1992, pp 77 – 92
Lave, J. and Wenger, E. (1991) Situated Learning: Legitimate Peripheral Participation, Cambridge University Press, Cambridge
Lee, A. (1991) Integrating positivist and interpretive approaches to organizational research, Organization Science (2), pp 342-365
March, J. G. (1991), Exploration and Exploitation in Organizational Learning, Organization Science, 2 (1), pp. 71-87.
OECD (2002) Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris, OECD, July 2002. www.oecd.org
Orlikowski, W.J., and Baroudi, J. (1991) Studying information technology in organizations: research approaches and assumptions, Information Systems Research (2:1), pp 1-28
Schultz, A. (1973), Concepts and Theoty Formation in the Social Sciences, in Maurice Notanson (Ed.), Collected papers, 1, The Hague,; Martinus Nijhoff, pp. 48-66
Suchman, L. A. (1987). Plans and Situated Actions: The Problem of Human-Machine Communications, Cambridge University Press, Cambridge.
Straub, D. and R. J. Welke (1998) Coping with Systems Risk: Security Planning Models for Management Decision-Making." MIS Quarterly 22(4): 441-469.
Unger, R. (1987) False Necessity, Cambridge University Press, Cambridge