INTEGRATING POSITIVIST AND INTERPRETIVE APPROACHES TO IS SECURITY RESEARCH

Paolo Spagnoletti
CeRSI Università Luiss Guido Carli
Roma, Italy
pspagnoletti@luiss.it
ABSTRACT

The use of a socio-organizational perspective for understanding information system security is still at a theory building stage. This is due in part to the slow progress of positivist research in a domain where is very often difficult to have access to empirical data for quantitative studies. However, even if interpretive research can be performed on a single case basis, this kind of studies are facing the lack of any prescriptive component and subsequently the lack of value to the security manager. In this paper the main positivist and interpretive concepts and assumptions will be introduced. Then, an integrated framework already proposed in the organizational literature will be presented and the possibility to apply this framework to the IS security domain will be investigated.
INTRODUCTION

With the objective of understanding the maturity of IS security research, some authors have identified a common trend between information systems security design methods and the more general information system development methods. Nevertheless, the results of such analysis see the use of socio-organizational perspective for understanding information system security at a theory building stage (Dhillon & Backhouse 2001). Moreover such methods are based on different approaches and paradigms. Burrel and Morgan (1979) suggested a framework classifying theories of organization in four paradigms: functionalist, interpretive, radical humanist and radical structuralist. In their view combination among paradigms are not possible. Orlikowski & Baroudi (1991) debate the merits and demerits of interpretive and positivist approaches. Furthermore some contribution advocates the integration of largely positivist and interpretive approaches (Lee 1991, Gable 1994, Ritzer 1992).

Referring to the more general field of IS, Björn & Carsten (2006) claim that the question of ‘paradigm incommensurability’ regarding positivism and interpretivism has to be seen as an open issue. Based on a variety of different arguments, Landry & Banville (1992) show how these paradigms can be seen as different but compatible views of the same research subject, but also as intrinsically contradictory. This twofold view depends on different definitions of positivism and interpretivism. The first viewpoint stands 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. From the second viewpoint, positivism and interpretivism neither share the epistemological nor the ontological assumption. Adopting this view, it is difficult to reconcile the two paradigms.

Sharing the first position and according with the suggestion of Lee (1991) in the context of organizational research, we claim that IS security researchers can simultaneously enjoy the benefits of both approaches.

In this paper the main positivist and interpretive concepts and assumptions will be introduced. Then Lee’s integrated framework (Lee 1991) will be presented and the
possibility to apply this framework to the IS security domain will be investigated. Finally we conceptually analyse some of the implications of using such an integrated positivist and interpretive research approach in the information system security domain with a brief discussion of possible advantages in terms of rigour and relevance. Our aim is to understand to what extent the three levels of understanding provided by the above mentioned framework can fit with the investigation of phenomena involved in IS security research.

AN INTEGRATED FRAMEWORK FOR POSITIVIST AND INTERPRETIVE APPROACHES

The positivist approach is characterized by a methodology of formulating hypotheses that are tested through controlled experiment or statistical analysis. Stated differently, the positivist tradition is based on the measurement and control of variables and on testing pre-specified hypotheses. This “natural-science model”, applied to social-science research, requires that social reality be captured in formal propositions, quantified and subjected to experimental controls. Despite the rigour of this approach, the application to social phenomena of positivist methods has been often criticized since the simplification and abstraction needed for good experimental design can remove enough features from the subject of study that only obvious results are possible (Kaplan & Duchon 1988). Moreover, in the particular context of IS security is very often difficult to have access to empirical data for quantitative studies. As a consequence, there is a negative effect on the progresses of positivist research in finding relevant and interesting results.

On the opposite, the interpretive approach is based on the assumption that people create and attach their own meanings to the world around them and to the behaviour that they manifest in that world. Therefore, the role of the social scientist is to observe and interpret this empirical reality in terms of what it means to the observed people. This means that facts and data about human behaviour collected in field research, represent also the subjective meaning this behaviour has for the human subjects themselves. In this case, data are used to both pose and resolve research questions. Thus, researchers increase their understanding of the perspective of those being studied through an iterative process. Starting without prior commitment to theoretical constructs or to hypothesis formulated before gathering any data, they test and modify their understanding through cycles of
additional data collection and analysis until coherent interpretation is reached (Kaplan & Duchon 1988).

In order to demonstrate the feasibility of integrating these two approaches often believed to be opposed and incompatible when performing organizational research, an integrated framework has been proposed by Lee (1991). The following description will draw heavily on the views of Lee. In his framework Lee defines three levels of understanding.

“They are:

1) the subjective understanding, which consists of the everyday meanings and everyday common sense with which the observed human subjects see themselves and the organizational world around them,

2) the interpretive understanding, which consists of the organizational researcher’s reading or interpretation of the subjective understanding, developed with the help of such methods as those of phenomenological sociology, hermeneutics, ethnography, and participant-observation, and

3) the positivist understanding, which consists of theoretical propositions, manipulated according to

- the rules of formal logic
- the rules of hypothetico-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 1: 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 starting from the subjective understanding.

Arrows 3 and 4 represent the formulation of theoretical propositions (3) and 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 confirmation or the disconfirmation 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.

This integrated approach allows 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.

IMPLICATION FOR THE IS SECURITY RESEARCH DOMAIN

Despite the trend in IS security research is moving away from a narrow technical viewpoint, the socio-organizational perspective in dealing with security issues is still at an early stage. Several efforts in the direction of interpretive studies are facing the lack of any prescriptive component and subsequently the lack of value to the security manager. Furthermore more structured and mechanistic
approaches, such as risk management techniques, have shown their limits in predicting computer incidents, especially those depending on the behaviour of internal actors.

Straub and Welke (1998) maintain that the main objectives of IS security planning should be deterring, preventing, detecting and pursuing 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. In their perspective, computer incidents play a passive role in the research process, being considered as the undesired phenomenon to reduce. We partially disagree with this view, claiming that computer incidents should be the main phenomenon under investigation, playing a central role in the context of IS security research. We consider this phenomenon as a particular form of “drift”. Using the words of Ciborra (2000) drift is the “outcome of tactics, ruses and improvisations” and is “related on the unpredictable behaviour of actors involved and on the openness of technology”. From this perspective, computer incidents in organizations can be considered as strongly related to the subjective understanding of human actors interacting with the set of technical, formal and informal rules which compose the implemented information security management system and the more general information system (Spagnoletti, 2006). One of the objectives of an information security management system is the reduction of risks due to losses in confidentiality, integrity and availability of data and communications. Apart from external attacks and natural disasters, these losses can be determined by malicious or involuntary behaviour of organizational actors, leading to computer abuses or misuses respectively.

In this paper, a computer abuse 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. While a computer misuse is the violation of the same set of rules without intentional consequences on the security of the information system.

In our view, both kind of computer incidents are really valuable for the IS researcher. In fact, from a socio-organizational perspective, the researcher is not only interested in the purely objective, publicly observable aspects of human behaviour (which is the incident itself), but also in the subjective meaning this
behaviour has for the human subjects themselves (the offender perspective). Therefore, performing an in-depth analysis of computer incidents using qualitative methods based on the interpretive approach, researchers will be able to develop and test the coherence of an interpretive understanding. The results of this process will constitute the premises for the formulation of new theories and hypothesis related to the context in which the incident happen and will increase the relevance of research results. Then the construction of the third level of understanding, using the rules of formal and hypothetico-deductive logic, will be performed with a positivist approach. The rigour of final results will be assured by the application of empirical quantitative methods.

In other words we claim that focusing on the interpretation of the subjective understanding of actors involved in a computer incident, is possible to achieve a deeper understanding of the observed phenomenon. Moreover, by applying the above mentioned framework, the interpretive understanding, achieved and tested through interpretive qualitative methods, can be then formalized in order to develop a positivist understanding. Finally the formal propositions defined through this process, will be empirically verified with traditional quantitative methods.

Implication for the information security manager

Recent studies on information system security show a totally different approach. Several surveys concentrate on the classification of the different types of computer incidents. The aim of this kind of studies is to suggest to security managers the implementation of countermeasures, which are very often technological solutions, with the objective of reducing the number of incidents. However, professionals involved in the management of IS security need not only technical tools and skills to detect computer incidents but also the capability to react with short-term and long-term actions. While the short-term actions are aimed pursuing remedies and/or punishing offenders for abuses, the aim of long-term actions is to prevent new forms of incidents and to improve the overall information system. In order to perform all these tasks, a continuous monitoring of human actions and a deep understanding of the subjective meaning they attach to their actions is necessary. Therefore, the proposed framework, while used in this context, should contribute by helping both the management and the researcher. The first will take advantage of the researcher cooperation during computer
incident investigations (action research), the last will benefit of these results in building new theories about human-technology interaction.

CONCLUSION

This paper is methodological in nature and no empirical data are mentioned in order to validate the integrated framework. However the aim of the paper is to stimulate discussion about the debated topic of integrating such apparently opposite research approaches.

The author is envisaging the possibility to adopt this approach as the underpinning assumption for an action research project where the role of security managers in the improvement of the overall information system is under investigation. In fact, the pervasive nature of information technologies in organizations and the different context and organizational cultures in which they are implemented, make computer incidents an effect of the interaction among human actors and the whole information system. Therefore, this approach should make possible to better understand the interaction between technology and organization with benefits for the security practitioners and the researchers.
REFERENCES


Kaplan B. & Duchon D., 1988, Combining qualitative methods in information systems research: A case study. MIS Quarterly, 12(4), 571-586

Lee, A. "Integrating positivist and interpretivist approaches to organizational research," Organization Science (2) 1991, pp 342-365


