2005

An investigation into the paradox of organisational flexibility versus security: A research project

Rosanna Fanciulli

An investigation into the paradox of organisational flexibility versus security: A research project overview

Rosanna Fanciulli
School of Computer and Information Science
Edith Cowan University
r.fanciulli@ecu.edu.au

Abstract

The trend towards utilising geographically and temporally dispersed personnel has grown quickly over the past decade; enabled by swift advances in computing, telecommunications, and networking technologies. The impact of these developments on corporate strategies and forms has manifested itself in a move to de-legitimise the rigid structure of a traditional bureaucracy and move towards one that is more flexible. These new technologies and organisational structures, however, also bring with them Information Security threats and risks. It is critical that managers become informed and equipped to deal with these issues. This paper presents an ongoing study designed to determine the major Information Security Management issues in implementing Distributed Work Groups, compared to those found in other organisational structures. It considers how best to manage these issues through the development of an ideal model, using a Soft Systems Methodology (SSM) approach.

Keywords

Information security management, interpretivism, soft systems methodology, organisational management

INTRODUCTION

Enterprises are facing a security paradox. On one hand, competitive pressure is driving organisations to adopt increasingly flexible structures, requiring them to open up their networks to a distributed range of users. On the other hand, this strategy simultaneously exposes them to greater information security risks, potentially threatening their competitive position. Ironically, information security controls by their very nature may limit worker flexibility, organisational adaptability, and hence competitive stance. It is critical that managers become informed and equipped to deal with these issues.

This paper outlines an ongoing project designed to determine the major Information Security Management issues in implementing Distributed Work Groups, compared to those found in other organisational structures. It provides an account of how the SSM method is applied, the research structured and the thesis progressed.

THE PROBLEM

The strategy of using geographically and temporally dispersed personnel has grown rapidly over the last decade, such that, today Distributed Work Groups (DWGs) and virtual project groups are a major part of organisational operations (Desouza & Evaristo 2004). This reaction to the increasing pressure to deliver more responsive and flexible operations (Assimakopoulos & Macdonald 2002; Harris 1998; Wognum & Faber 2002) has been enabled by the simultaneously rapid advance in computing, telecommunications and networking technologies (Wognum & Faber 2002).

Driven by increasing environmental turbulence, global competition, shorter product life cycles and pressure to speed up product innovation, organisations have sought more accommodating operating structures. The impact on corporate strategies and forms has manifested itself in a move to de-legitimise the rigid structure of a traditional bureaucracy and move towards one that is more flexible or adaptable. The result is dispersed or *virtual* organisational structures designed to be innovative, adaptive and to overcome time-and-place constraints associated with rigid bureaucratic structures (Hassard et al. 1999).

Inevitably, information technology is fundamental to achieving these goals. In fact, many organisations rely upon information technology to the extent that it would be impossible to manage without it (Brooks et al. 2002). As a result, it is imperative that businesses be able to secure the availability, integrity and confidentiality of information (Price Waterhouse Coopers 2004). However, security breaches within

organisations continue to rise, with significant cost to businesses (ibid.) as billions of dollars are lost to computer theft, fraud and abuse (Whitman 2003, 2004). The increase in interconnectivity, whilst providing the much needed flexibility, has also aggravated this problem by further exposing organisations and their information networks to more numerous and diverse threats and vulnerabilities (OECD 2002).

A number of principles for managing information security have been developed to address this situation (Brooks et al. 2002). Realistically however, financial and operational constraints often exist which influence and restrict the implementation of these recommendations (Price et al. 2004). This scenario often results in Information Security issues being neglected, exposing organisations to unnecessary risk (CSI/FBI 2004). The difficulty lies in trying to achieve balance between quality of service '*flexibility'* and level of security '*control*' (Baskerville 1996). That is, how does one identify appropriate levels of expenditure while managing threats to organisations (Khalfan 2004; Whitman 2004)? From this perspective, it is clear that this is more than just a technical or economic issue (Dhillon & Backhouse 2000). It is also inherently socio-political in nature as different stakeholders vie for solutions that will assist them meet their individual deliverables. Consequently, there is indication that social research may provide important insight to this area (Clarke & Drake 2003; Dhillon 2004; Eloff & Eloff 2003; OECD 2002).

THE SOLUTION – A SOFT APPROACH

Research Purpose

This paper describes a project investigating the issues involved with achieving balance between flexibility (using distributed work groups to achieve quality of service) and control *(*managing to achieve security of information*)*. It does this by grounding the research process in the hermeneutic philosophy, providing opportunity for new socio-political insight to an area that has largely been addressed from a technical perspective.

The purpose of this research is to investigate what major Information Security management issues may be involved with implementing these DWGs. It aims to ascertain if in fact the implementation of DWGs do present different Information Security implications for management than those pertaining to other organisational structures such as co-located or rigidly bureaucratic structures. Using Soft Systems Methodology, it will then consider how these issues can best be managed through the development of a systems model for the Information Security Management of DWGs.

Why Soft Systems Methodology?

In order to address the complex socio-political issues discussed above, it was deemed necessary to use a flexible and evolving problem solving strategy. Soft Systems Methodology, with steps designed to be adapted or modified to suit the particular problem situation under study, proved the most suitable choice. Originally, it was thought that this project would see the researcher immerse themselves in selected organisations. However, the dynamic political environments of these organisations threatened the viability of the project. Within the timeframe of a PhD study, not only was it possible that the DWG could be disbanded, it was also possible that the business unit or organisation themselves would be dismantled, jeopardising research in progress. These problems rendered the action research, case study, grounded research and ethnographic research methods problematic and inappropriate to this study. The harder end of Soft Systems Methodology was deemed more applicable and feasible. Importantly, it was found to hold the flexibility required to deal with the sensitive, political and volatile environments under investigation. Developed by Peter Checkland (1981), this approach provides for organised intervention and purposeful action, which recognises and builds on the multiple realities perceived by different stakeholders (Walsham 1993).

Philosophy guiding the way: Interpretivism and Constructionism

The interpretative qualitative approach discussed above is generally committed to the broad philosophy of social construction and hermeneutics. It views social reality as a constructed world built in and through meaningful interpretations (Denzin & Lincoln 2000; Schwandt 2000). This approach finds truth "in the potential of language (conversation, dialogue) to disclose meaning and truth" (Schwandt 2000 p.198). Therefore, the researcher starts out with the assumption that access to reality (given or socially constructed) is through social constructions such as language, consciousness and shared meanings (Prasad & Prasad 2002).

Boland, in the 1980s was one of the first to apply these theoretical ideas specifically to the study of information systems. This paper proposes to apply them to the study of Information Security Management. Drawing on Gadamer's (1975) work, Boland adopted the argument that language is fundamental to our being-in-the-world, that one's daily social experiences are hermeneutic; and that daily one encounters a text of meanings already made and in the act of being made (Walsham 1993). Therefore, every reading and hearing of a text can be considered a hermeneutic act; as it gives meaning to it through interpretation. This researcher finds that the argument also holds true for the human activity systems that are related to information security management. As such, a hermeneutic approach, as adopted here, has the potential to provide new socio-political insight to an area that has largely been addressed from a technical perspective.

RESEARCH METHOD

Research Status

A review of the status of this project finds the proposal to undertake this research has been submitted and approved. An extensive literature review has commenced, and will continue to be updated and informed throughout the course of the project. The interview schedule has been developed and the trial completed. Negotiations have been undertaken with major organisations to participate in the study and interviews are underway.

Research Structure

Soft Systems Methodology sees different individuals and groups as constructing interpretations of the world, the interpretations having no absolute or universal status. Consistent with the research objectives, the purpose of the intervention is to reconcile these views sufficiently to achieve organised action (Daellenback 1994). In Soft Systems Methodology, a special feature is the use of conceptual models of the area of interest known as holons or human activity systems. These are based on a root definition representing a particular view of the core purpose of the activity system. These holons when compared to the real world as epistemological devices can initiate interpretive debate between the organisational participants (Checkland 1981).

In this case, the views of the participants are interpreted, collated and pictorially represented. The models are then presented back to the participants for comment, enabling refinements and modifications to be made in keeping with the research design represented below in Figure 1. Recognising the limitations of SSM, Critical Systems Heuristics (CSH) is used as a front end tool to address political issues in the investigatory and analytical phases.

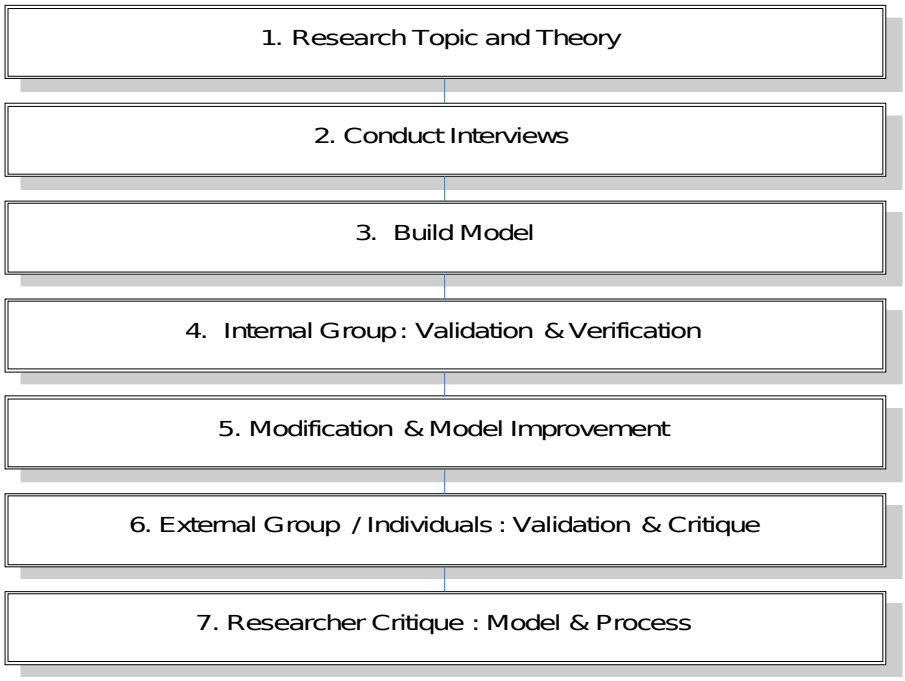

FIGURE 1 Diagram of the research design

In keeping with the interpretive methodology, the SSM process is able to provide for reflexivity, reiteration and flexibility (Hicks 1991). In fact, the researcher may begin at any stage; move freely between stages; or work on different stages concurrently. The research design and sampling strategy, however, have remained purposive (Mason 2002), consistent with the position of the interpretivist paradigm within the rationalist epistemology (Klein 2000).

The interpretivist approach adopted here, views knowledge (Miles & Huberman 1994 p.4) as a social and historical product and that "facts" come to us laden with theory. The research design acknowledges that to get to the construct we need to see different instances of it, at different moments, in different places and with different people. Therefore, the objective is to find an individual, or a social process, a mechanism, or a structure at the core of events that can be captured to provide a causal description of the forces at work. Thus, the sampling process is strategic and organic rather than random, driven by theory, not representativeness.

The primary concern is to investigate the conditions under which the construct / theory operates, not with the generalisation of the findings to other settings (Miles & Huberman 1994). Consequently, it is acknowledged that the findings may not hold where local circumstances are different - or even in some sites that show similar characteristics. This follows Weisberg's classification (1989), which recognises that in this type of non-probability sampling procedure, results may be seen as estimations only. To test and ramify claims and to establish their analytic generality, several case examples with similar and contrasting characteristics are being investigated (Miles & Huberman 1994). The aim of this procedure is to not only strengthen the conceptual validity of the study, but also help determine the conditions where the findings hold.

Sample Population

Consistent with a qualitative approach, the sample involves a small number of people deeply nested in the context under investigation (Miles & Huberman 1994). Thirty participants across 6 organisations are studied in some depth. Unlike quantitative researchers who aim for larger numbers of context-stripped cases and seek statistical significance, this approach tends to be *purposive* and *theory driven* rather than random. This is partly because the initial definition of the universe is more limited. It is also because social processes have a unique logic and coherence that random sampling may fail to represent rationally (Miles & Huberman 1994).

The sample population consists of a range of stakeholders that belong to organisations employing DWGs and actively engaging computer, telecommunications and Internet technologies to facilitate this. They vary in economic reach, level of centralisation, industry, technology adoption and such factors. Some organisations are providers of information technology products and services. The organisations predominantly operate in the private sector; are medium and large sized; and may have state, national and international operations. All are aware of the need for Information Security but vary in their approach and their level of adoption. All the participating organisations have delocalised their activities rendering their production process; supply of their services; or, relations with customers and staff more flexible. Importantly, the target sample ranges across preferred management styles from controlled to flexible management approaches. It is expected that this variation will provide further insight into the second order security dilemma, as it illuminates the relationship between Information Security Management and organisational structure.

Research Instruments

Research instruments have been selected in keeping with the view that social explanations and arguments can be constructed by laying emphasis on depth, nuance, complexity and roundedness in data. Questionnaires and broad surveys may provide a broad understanding of surface patterns (Mason 2002) and many have provided an important insight into the background of this research project. However, they will not deliver the depth and rounded understanding of Information Security Management required here. As such, qualitative / semi-structured interviews have been selected as the primary data collection method. To help ensure reliability, secondary data sources are also used, primarily consisting of associated corporate and public documentation. This will include formal documents such as policies, regulations, organisational charts and annual reports, as well as more informal documents such as operating instructions, staff memos or email.

In keeping with the interpretivist intent of SSM, the research aims to explore people's individual and collective understandings, reasoning processes and other significant factors. Nevertheless, given the multi-textured and chaotic environment within which the research project is undertaken, some prior

preparation was deemed a necessity (Stacey 2000). As a result, the interview schedule is consistent, thematic, topic-centred and semi-structured with questions based on the theory and philosophy earlier discussed. It also readily reflects the influence of critical systems heuristics (CSH), employed as a front-end investigation tool to address the socio-political issues. It has been designed in this manner to minimise potential bias through the application of common instruments, including the interview schedule and supporting corporate documents. Comparable interviews are expected to help build theory, improve explanations and in turn contribute to recommendations and better practice (Miles & Huberman 1994). Having noted this rationalist approach, the researcher also acknowledges the need to retain fluidity of the interview process to allow the interviewee to discuss pertinent themes in a suitable manner (Fontana & Frey 2000).

Data Analysis

While most research materials are written, they initially present in a variety of formats. Once deemed sound, they are transformed into a common written format to enable them to be readily sorted and organised for analytical purposes (Mason 2002). Ultimately, data is translated into diagrams, a highly effective communication method fundamental to the Soft Systems Methodology.

Data is read interpretively, literally and reflexively (Mason 2002), the former being the dominant method consistent with the hermeneutic philosophy. This includes documenting what it is thought the data may represent, or what can be inferred from them. Of prime interest are the interviewees' interpretations, understandings, and accounts of how they make sense of the social phenomena. Importantly given the interpretivist nature of the study, data are also read reflexively, recognising the impact of the researcher's own historicity (Gadamer 1975) and the constant evolution of the situation under review (Walsham 1993).

Validity and Reliability

Discussing the issues of validity and reliability in interpretivist research is often contentious, within traditionally positivistic domains. Much headway has been made in clarifying the differences between the two (Myers 2004). The perspective adopted here is that there is no fixed point to reality, as it is constantly evolving. It is understood that information systems are contextually and historically specific; and, that the information system itself is not static, neither in a physical nor in a social sense. The researcher acknowledges that there are numerous ways to view the one situation, more like a crystal than a triangle (Miles & Huberman 1994). Rather than trying to use different methods to pinpoint the exact same position, it is necessary to support a finding by showing that independent measures of it agree with it or, at least, do not contradict it. With this as the priority, triangulation sources have been selected for their different biases, different strengths and capacity to complement each other.

Therefore, a variety of data types, sources, participants, events, places, theories and methods, as discussed throughout this paper, are incorporated into the study. Additionally, to ensure memories are accurate and perceptions valid, the researcher's interpretations are systematically recorded and reflexively reviewed. This includes making transparent the researcher's own assumptions on what is recorded, heard, observed or read (Mason 2002). Misrepresentation is further avoided by respecting the partial nature of the interview transcripts, audio recordings and written texts, treating data as retrievals not variables. In turn, the researcher's interpretations, selection, and coding decisions will be validated via inter-related reliability, a comparative researcher method. The results then will be verified and validated by seeking feedback from both internal and external study participants. Finally, the model will be presented to selected external organisations for comment and validation as represented in Figure 4.1 above.

Klein and Myers (1999) principles have been adopted, as appropriate, to guide the researcher in evaluating reliability and validity in this interpretive project. The principles are consistent with a considerable part of the philosophical base of literature on interpretivism. Importantly they help reduce the risk of judgement against positivist or otherwise inappropriate criteria. Their seven principles are adhered to throughout the research process to ensure the issues of reliability and validity are consistently addressed. This includes respecting the meta-principle of the hermeneutic circle as the researcher's focus moves continually between the whole and its parts. Attention is also paid to the principles of contextualisation, interaction between researchers and subjects, abstraction and generalisation, dialogical reasoning, multiple interpretations, suspicion, and their interdependence.

CONCLUSION

The trend towards utilising geographically and temporally dispersed personnel has grown quickly over the past decade, enabled by swift advances in computing, telecommunications, and networking technologies. Pressure to improve worker productivity, supply chain efficiencies and global competitive position has affected corporate strategies, resulting in the adoption of more flexible operating structures. These new technological and organisational practices, however, also bring with them additional Information Security threats and risks. Managers must become informed and equipped to deal with them. The literature reviewed in this paper indicates that socio-political issues need to be addressed and that appropriate methodologies are needed to do this. Accordingly, a research proposal to use SSM to address this problem is presented. An account is provided of the ongoing study designed to determine the major Information Security Management issues in implementing Distributed Work Groups, compared to those found in other organisational structures. It considers how best to manage these issues through the development of an ideal model, using an SSM approach.

REFERENCES

Assimakopoulos, D., & Macdonald, S. (2002). A dual approach to understanding information networks *International Journal of Networking and Virtual Organisations, 1*(1), 1-16.

Baskerville, R. (1996). The Second Order Security Dilemma. In W. J. Orlikowski, G. Walsham, M. R. Jones & J. I. De Gross (Eds.), *Information Technology and Changes in Organizational Work: Proceedings of the IFIP WG8.2 Working Conference on Information Technology and Changes in Organizational Work, December 1995* (pp. 239-249). London: Chapman & Hall.

Brooks, W. J., Warren, M., & Hutchinson, W. (2002). A security evaluation criteria. *Logistics Information Management, 15*(5/6), 377-385.

Clarke, S., & Drake, P. (2003). A social perspective on information security: theoretically grounding the domain. In S. Clarke, E. Coakes, M. G. Hunter & A. Wenn (Eds.), *Socio-Technical and Human Cognition Elements of Information Systems* (pp. 249-265). London: Information Science Publishing.

CSI/FBI. (2004). *Computer Crime and Security Survey 2004*. Retrieved 29 November, 2004, from http://www.crime-research.org/news/11.06.2004/423/

Daellenback, H. G. (1994). *Systems and Decision Making: A Management Science Approach*. New York: Wiley.

Denzin, N. K., & Lincoln, Y. S. (2000). Introduction: The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 1-29). Thousand Oaks: Sage Publications.

Desouza, K. C., & Evaristo, J. R. (2004). Managing knowledge in distributed projects. *Communications of the ACM, 47*(4), 87-91.

Dhillon, G. (2004). Guest editorial: The challenge of managing information security. *International Journal of Information Management, 24*(1), 3-4.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Eloff, J., & Eloff, M. (2003, September). *Information Security Management - A New Paradigm*. Paper presented at the SAICSIT South African Institute for Computer Scientists and Information Technologists, South Africa.

Fontana, A., & Frey, J. H. (2000). The interview: from structured questions to negotiated text. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (2nd ed., pp. 645-672). Thousand Oaks: Sage Publications.

Gadamer, H.-G. (1975). *Truth and Method*. London: Sheed & Ward.

Harris, M. (1998). Rethinking the virtual organisation. In P. J. Jackson & J. Van Der Wielen (Eds.), *Teleworking International Perspectives: From Telecommuting to the Virtual Organisation* (pp. 74-92). London: Routledge.

Hassard, J., Law, J., & Lee, N. (1999). Themed section Actor-Network Theory and managerialism: Preface. *Organization, 6*(3), 387-390.

Hicks, M. J. (1991). Soft system thinking. In *Problem Solving in Business and Management* (pp. 226-255). London: Chapman & Hall.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management, 24*(1), 29-42.

Klein, & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67-93.

Mason, J. (2002). *Qualitative Researching* (2nd ed.). London: Sage.

Miles, M. B. & Huberman, A. M. (1994), *Qualitiative Data Analysis*. CA:Sage

Myers, M. D. (2004). *Qualitative Research in Information Systems: The Living Version*. Retrieved 8 September, 2004, from http://www.qual.auckland.ac.nz/

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Paris: OECD.

Prasad, A., & Prasad, P. (2002). The coming age of interpretive organizational research. *Organizational Research Methods, 5*(1), 4-11.

Price, Waterhouse, & Coopers. (2004, April 2004). *Information Security Breaches Survey 2004*. Retrieved 29 November, 2004, from http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Exec_Summ.pdf

Schwandt, T. (2000). Three epistemological stances for qualitative inquiry: Interpretivism, hermeneutics, and social constructionism. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (2nd ed., pp. 189-213). Thousand Oaks: Sage Publications.

Stacey, R. D. (2000). *Strategic Management and Organisational Dynamics: The Challenge of Complexity* (3rd ed.). Harlow: Financial Times.

Walsham, G. (1993). *Interpreting information systems in organizations*. Chichester: Wiley.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95.

Whitman, M. E. (2004). In defense of the realm. *International Journal of Information Management, 24* (1), 43-57.

Wognum, P. M., & Faber, E. (2002). Infrastructures for collaboration in virtual organisations. *International Journal of Networking and Virtual Organisations, 1*(1), 32-54.

COPYRIGHT