

2006

Information security management and virtual collaboration: A Western Australian perspective

Rosanna Fanciulli
Edith Cowan University

Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western
Australia, 5th December, 2006

This Conference Proceeding is posted at Research Online.

<http://ro.ecu.edu.au/ism/73>

Information security management and virtual collaboration: A Western Australian perspective

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

Abstract

This paper presents an ongoing case study into stakeholder perceptions regarding information security management systems in emergent organisations operating in Western Australia. It takes a socio-political perspective on the problem of how to manage simultaneously virtual collaboration and information security management. A literature review introduces the context and history of the research. In light of this, it is proposed that social and political issues need to be researched and addressed before many of the existing technological strategies for information security will succeed. The research project is then outlined and the design and preliminary results presented. The results point to a lack of clarity and cohesion amongst stakeholders about how their information security management systems operate and who has ownership of the security function. This emerging trend is discussed and the plans for future research explained.

KEYWORDS

Information security management, virtual collaboration, adaptive organisations, emergent organisations, distributed work groups, soft systems methodology, critical systems

INTRODUCTION

To succeed in the highly competitive global business environment, enterprises have increasingly adopted flexible, distributed work practices. However, distributed work practices bring with them additional information security threats and risks. Whilst numerous national and international regulations have been put in place to address this growing problem, their implementation and enforcement have met with limited success. This paper proposes that a socio-political research perspective may provide insight into why these technical regulations have failed to stem the growth of corporate security breaches.

The background to these developments is reviewed and a closer look taken at how organisations conduct virtual collaboration. It notes the problems previous research has uncovered and considers the implications for information security regarding situations where workers seldom operate at a central site. This leads to a discussion of the research project's objective to investigate stakeholder perceptions regarding information security management systems in emergent organisations. The design and findings emerging from this study are then presented. Finally, the paper is discussed in the context of the larger and ongoing research project.

HISTORICAL CONTEXT - EMERGENT ORGANISATIONS

To meet the challenges of a global market, organisations have reengineered their operations to deliver more responsive and flexible services (Wognum & Faber, 2002; Harris, 1998). This strategy of redistributing the organisational workforce, geographically and temporally, has grown rapidly over the last decade. Driven by increasing environmental turbulence, global competition, shorter product life cycles, and faster product innovation, organisations have sought operating structures that are more accommodating. 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).

New organisational forms have emerged (Desouza & Evaristo, 2004; Jackson & Van Der Wielen, 1998; Garcia & Quek, 1996; Perin, 1998) as across the globe, strong external coalitions are transforming

traditional monolithic, centralised, and hierarchical organisations into loosely coupled organic networks (Dhillon, 2004; Dhillon & Backhouse, 2000). Often referred to as adaptive or emergent organisations, they are characterised by the ability to change their form in response to rapid shifts in the nature of their markets and their economic or political environment (Baskerville, 1996). Frequently the common unit of work is the virtual project group, characterised by cooperation instead of control.

These new structures involve intense sharing of information and a high level of interpersonal and inter-organisational connectivity (Davenport & Prusak, 1997; Perin, 1998). Consequently, organisations are no longer characterised by physical assets but by a network of individuals who create, process, hold, and distribute information, enabling them to be location and structure-independent (Garcia & Quek, 1996). To realise the full potential of these new structures, organisations need to create opportunities for dispersed employees to interact as meaningfully as they would in traditional face-to-face environments (Desouza & Evaristo, 2004; Dhillon & Backhouse, 2000).

Innovations in information technology have revolutionised the way organisations conduct business and facilitated the growth of the global market place. Even small to medium organisations can now operate with a dispersed workforce. Inevitably, information technology is fundamental to achieving these goals, with wide area networking, telecommunications, convergence technologies, and the Internet being increasingly adopted. Virtual collaboration takes place through telecommunications networks. Each node of which contains one or more people relying upon mediated, rather than face-to-face communication to produce an outcome (Wainfan, et. al., 2005). The primary facilitation methods for virtual collaboration include videoconferencing, audioconferencing, and computer-mediated communication. Interestingly however, there exists no agreed-upon model of virtual collaboration and mediated communication (Ibid., 2005).

VIRTUAL COLLABORATION - SECURITY IMPLICATIONS

Information Assets

These virtual collaborations find geographically dispersed people working together interdependently in their tasks and sharing responsibility for outcomes. The implications for information security management are important. Outcomes from virtual collaboration form fundamental contributions to corporate information and knowledge assets. These outcomes can include developing a shared understanding, evaluation, strategy, recommendation, decision, action plan, or other product (Wainfan & Davis, 2005). Distributed work operations also deal with operational issues and involve information pertaining to corporate strategy, operating principles, client details, personnel records and so forth. It is critical that these information assets are protected.

Information Security

A number of principles for managing information security have been developed. Predominantly, these have been technically oriented solutions (Brooks et al, 2002; Stacy, 2000). However, security breaches within organisations continue to rise with significant cost to businesses. Billions of dollars a year are lost to computer theft, fraud and abuse (Whitman 2003, 2004). Given cyber-crime continues to be a significant threat to organisations it is becoming increasingly clear that these solutions alone may not hold the answer. As discussed throughout this paper many researchers, in recognition of the changing nature of organisational work units, have recommended that social research be conducted into information security management (Clarke & Drake, 2003; Dhillon, 2004; Eloff & Eloff, 2003; OECD, 2002). This call has been taken up by this research project.

Truex et.al. (1999) describe the features and processes in emergent organisations as constantly undergoing social negotiation and consensus building. They are never fully formed. Thereby a mismatch occurs between the requirements of modern organisations and the aims of traditional information systems development strategies that assume long periods of stable operation. The dynamics involved with emergent organisations raise critical questions about closure and stability within them (Ibid., 1999). This leads to the question raised in this paper: how do organisations simultaneously manage virtual collaborations and information security?

In order to understand how IT can promote (and protect) organisational emergence, Truex et. al. (1999) suggest it is necessary to understand some of the forces behind it. They put forward the concept of three “levers of encouragement” that are known to stimulate emergent organisations: shared reality construction; self-reference and organisational identity; and, the dialectics of organisational autopoiesis. This paper holds that these socio-political issues also need to be better understood in the context of information security management systems, if they are to successfully promote and protect emergent organisations.

SOCIAL AND POLITICAL ISSUES AFFECTING INFORMATION OPERATIONS

Perspective, Power and Status

Wainfan & Davis (2005) found outcomes from virtual collaboration depend on many factors: communication medium (or media), task type, context, group characteristics, and individual characteristics. They found a number of valid conclusions arose consistently across different experimental conditions. In particular, all media to some extent changed the context of the communication, generally reducing cues used to (1) regulate and understand conversation, (2) indicate participants' perspective, power, and status, and (3) move the group toward agreement (Wainfan & Davis, 2005).

They also found that in videoconferencing, audio-conferencing and computer-mediated communication, participants tend to cooperate less with those at other nodes and more often shift their opinions toward extreme or risky options than they do in face-to-face collaboration. In videoconferencing and audioconferencing collaboration, local coalitions can form in which participants tend to agree more with those in the same room than those on the other end of the line. There is also a tendency in audioconferencing to disagree with those on the other end of the communication link. Computer-mediated communication was found to affect efficiency (as measured in time to solution), status, domination, participation, and consensus.

Whilst, virtual collaboration has been shown to be useful in broadening the range of inputs and ideas; it was also shown to increase polarisation, deindividuation, and disinhibition. That is, it was found that individuals might become more extreme in their thinking, less sensitive to interpersonal aspects of their messages, and more honest and candid. This clearly would hold concerns for those responsible for the quality and safety of corporate intelligence and decision-making processes. It indicates that socio-political issues in virtual collaboration are affecting outcomes, including the integrity, availability and confidentiality of information. The implications of these findings are important for information security management and very important for this research project.

Commitment, Loyalty and Organisational Identity

Other researchers have noted additional problems that may occur where workers seldom operate at a central site. For instance, issues of commitment, loyalty and organisational identity can become important. Research shows that some of the problems stem from psychological effects associated with the communication medium. This can include the emergence of animosities (or in-group/out-group effects) among participants, in-effective discussion, and the adoption of options that are riskier and perhaps less well-considered than those that would have emerged from face-to-face discussion (Wainfan & Davis, 2005). The potential of these findings for corporate intelligence and information operations is grave. It not only suggests that virtual collaborations may be at risk of deliberate sabotage attempts, but also subconscious attempts as relationships between stakeholders affect information, outcomes and information security management.

Implications for Further Research

In relating these research findings to information security management, there is good reason for concern. After all, it is well documented that much of the damage to security comes from perpetrators within organisations themselves. In most cases, ethical standards remain unclear and there is a lack of general awareness across the organisation (Whitman, 2003, 2004). In short, whilst the benefits of virtual collaboration are numerous, the problems that accompany them are also numerous. It is now widely

acknowledged that it is imperative that businesses be able to secure the availability, integrity and confidentiality of information (Price Waterhouse Coopers, 2004).

However, achieving consensus regarding safeguards for an information system, among different stakeholders in an organisation, has often become more difficult than solving many technical problems that might arise (Dhillon & Backhouse, 2000). This has led many researchers to note that the integration of dispersed activities into traditional business structures requires new forms of co-operation, co-ordination and control (Baskerville, 1996; Gallivan, 2001; Handy, 1995; Jarvenpaa et al., 1998; Orlikowski et al. 1996). It has also led to the call for more social research into the issue of information security management (OECD, 2002; Clarke et al, 2003; Eloff, 2003).

RESEARCH PROJECT

In light of the research outcomes discussed above, strategy formulation for information security management of distributed work groups needs to incorporate a balanced appreciation of many diverse internal and external factors. It is more than just a technical or economic issue. The theory explored and developed in this research project is that the information security management is also a socio-political issue. This is because the human element is a component of all threats. These socio-political issues, intentionally or unintentionally, can affect the implementation of technical and regulatory solutions. Therefore, the complexity of the social and political obstacles undermining these technical solutions must be addressed before many of them will succeed. With this in mind, it is expected that a new socio-political perspective will hold value for information security management.

Using a socio-political approach, this research project investigates the issue of finding balance between competitive advantage and information security in virtual collaborations. The interdependence of these corporate priorities is acknowledged; and, the role they play in fostering organisational health is respected. With this in mind, the research aims to shed light on the issue of how organisations may use virtual collaboration techniques whilst simultaneously managing a secure information system.

Generalisation

It is important to note that the intent behind this research is to develop concepts, generate theory, draw implications, and provide rich insight into the issue of information security management systems of distributed work groups (Walsham, 1993). The objective is not to test theory in a simple or direct manner, as with positivist case study research. Rather, the aim is to relate theoretical abstractions and generalisations carefully back to the field study details as they were experienced by the researcher, to illustrate how their arguments were developed. The philosophical basis for this approach to abstraction and generalisation in interpretive field studies is well documented by .

Research Design

The methodological approach for this ongoing study is aimed at investigating the multi-level contextual nature of information security management, and the process of organisational change with which information security is interdependent. In particular, it focuses on organisational structural and cultural change in the form of adopting, implementing and managing distributed workgroups. The research design was structured to explore and develop a potential ideal model for managing information security within distributed workgroups. The case study strategy was employed to investigate a range of corporate examples. Soft System Methodology was the primary research method adopted to facilitate the investigation. Critical System Heuristics was used to complement this approach by providing opportunity and means to address issues of power.

Given the premise, that information security management in adaptive organisations is essentially a socio-technical situation, it was decided that a means was needed by which to make sense of its inherent political nature. Political issues by nature are never explicit, and can be very elusive, which often predisposes us to ignore them (Checkland, 1993). To assist in collecting and understanding this socio-political data, Critical Systems Heuristics was employed as a front end tool to guide the development of the survey questions and assist in the investigatory and analytical phases. Combined with Soft Systems Methodology, the research design provides for different individuals' and groups' interpretations of the problem situation. It

acknowledges that people see the world through different eyes and may view a particular situation differently.

A range of research participants were asked to share their perceptions and ideas on the problem situation as it currently occurs in their organisation. They were also asked how they think the situation should operate in an ideal system. Eventually, these views will be reconciled sufficiently to develop illustrations that represent the current and ideal situation (Daellenback, 1994). Comparison of the two will be used to initiate interpretive discussion and debate (Checkland, 1990). The models can then be refined and presented back to the participants for validation. This is discussed further in the section on Future Research.

Research – A Political Process

Politics, in the sense that it is used in this paper, refers to the process by which interested parties reach some sort of mutual accommodation or compromise, including all the manoeuvring and intrigue this entails. Attempting to unravel the politics of the situation is critical. Checkland suggests that human problem situations are a historical product and their history affects people's perceptions, judgments, and standards of the problem situation. The researcher needs to be cognisant of this to uncover the basis of power and understand how situations have come about.

Importantly, in this study it was able to forewarn the researcher of the difficulties ahead in collecting data including possible resistance to, or support for, the research. This was critical in this project where participants were asked to discuss their organisational information security management system, potentially a very sensitive area. The research process is ongoing and it is necessary to acknowledge that the very presence of the researcher can affect the situation, simply by focussing attention on the issue at hand. It was viewed suspiciously by some that it might have the potential to be a political act in itself, such that they declined or withdrew participation. Was someone trying to catch them out? The issue was addressed through vigilant ethical behaviour. Inevitably, however these social and political dimensions will affect what is culturally feasible for the research project.

Sampling Strategy

Subsequently, sampling is driven by theory, not representativeness. The primary concern is the investigation of the conditions under which the construct operates. It is not with the generalisation of the findings to other settings. This strategic approach tends to be purposive while remaining organic. This is partly because the initial definition of the universe is limited. It is also because social processes have a unique logic and coherence that random sampling may fail to represent rationally (Miles & Huberman, 1994).

This approach provided for the researcher to seek the best opportunities to collect pertinent data. Organisations were carefully chosen according to their level of participation in these new virtual structures and their willingness to participate in the study. Individual participants were specifically chosen according to their stakeholder status within this context. A champion or informant was nominated in each organisation to provide insight into the organisation and to initiate strategic selection of appropriate participants. These participants were then able to provide intelligence as to the pertinence of other stakeholders. Thus, the sample was able to grow organically.

Consequently, it is acknowledged that the findings may not hold where local circumstances are different - or even in some sites that show similar characteristics. They are estimations only (Weisberg's, 1989). As the sample is not statistically relevant and participants were chosen because of their diversity of opinion, findings are not presented numerically and each participant's observations are given equal consideration. To test and ramify claims and to establish their analytic generality (Miles & Huberman, 1994), several case examples with similar and contrasting characteristics have been investigated. The aim behind this was twofold: to strengthen the conceptual validity of the study and help determine the conditions where the findings hold.

Case Studies

Three case studies are presented, collectively as one unit, in this paper. The first case study is a medium sized firm with operations throughout Asia. Its head office is based in Perth, Western Australia. The

second case study is a large organisation with operations distributed across metropolitan and regional Western Australia, as well as international offices. The third case study is a cross industry unit, involving participants from across five organisations with operations in metropolitan and regional Western Australia, Australia and other countries.

Case Participants

The sample selected involves a small number of people deeply nested in the context under investigation. At this stage of the research project, twenty participants across three case studies have been interviewed and studied in some depth. The final stage will see 40 participants interviewed across four case studies. The sample population covers a range of stakeholders that include management, user, technical and information security representatives.

Case Organisations

The organisations employ distributed work groups, use virtual collaboration methods, and actively engage computer, telecommunications and Internet technologies to facilitate this. They vary in economic reach, level of centralisation, industry, technology selection 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 or 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. The target sample ranges across preferred management styles from controlled to more flexible management approaches.

Virtual collaboration is fundamental to the operations of all the case study organisations in this project. Distributed work groups are used to facilitate broadening reach, responsiveness, adaptiveness, corporate intelligence, and economies in time and money. Consistent with the study by Wainfan & Davis (2005), they use videoconferencing, audioconferencing and computer mediated communications. In using videoconferencing, participants are able to face a video image of other members or multiple images of other members. Common graphics can be viewed, using techniques such as shared briefing or a shared whiteboard. Notably they use audio-conferencing, whereby participants are on the telephone with one or a number of other people. Frequently, face-to-face subgroups meet simultaneously in the same room during these virtual collaborations. Computer displays are used to see shared briefings or whiteboards. Most frequently, virtual collaboration incorporates computer-mediated communication. This is typically text-based, but also includes drawings, photos, emoticons and other images. This is either synchronous (such as instant messaging) or asynchronous (such as e-mail, discussion boards, application-specific groupware, or shared databases) (Ibid., 2005).

RESEARCH INSTRUMENTS

Research instruments were designed to emphasise the depth, nuance, complexity and roundedness in data. This approach was chosen to best facilitate the construction of social explanations and arguments. When reviewed, questionnaires and broad surveys were found to provide a broad understanding of surface patterns (Mason, 2002). However, depth and rounded understanding of information security management was required for this research project. As such, qualitative / semi-structured interviews were selected as the primary data collection method. Interviews were undertaken in person, via telephone or email. To help ensure reliability, secondary data sources were also used, primarily consisting of associated corporate and public documentation.

There is a heavy emphasis on contextuality and historicity in this type of research. It was important to be able to review the data in its original form. The computer assisted data management tool, NVivo, proved valuable in enabling data to be efficiently managed while facilitating its treatment as retrievals and not variables.

FINDINGS

It was found that financial and operational constraints influence and restrict the practicality of many technical, security recommendations. This is in keeping with the CSI/FBI 2004 survey and Brooks et. al. (2002). The larger and more affluent corporations used more sophisticated behavioural and technical information security measures. The smaller and less affluent corporations took more simplified and ad hoc measures, potentially exposing them to unnecessary risk.

However, the findings from this research project indicate that the issue is more complex than this. It was found that the decision-making process regarding corporate resources is inherently a socio-political activity. Different stakeholders vie for limited resources that will assist them to meet their specific deliverables. Elevating an individual's issue or deliverable to the top of the corporate agenda was often a highly competitive and political process. For example, the priorities of the manager of sales has been found to well differ from those managing information security. In instances where this occurred, finding balance between the two was problematic. Furthermore, corporate decision-making capabilities and information security management measures were found to be less effectual where organisational politics led to passive/aggressive or intentional/unintentional sabotage of the system. In some instances, this included controlling the communication medium itself as an expression of power.

On the question of whether information security management differs between co-located work groups and distributed work groups, it was found that participants do believe information security management is different for distributed work groups. On the question of whether participants thought their organisation's information security management system was ideal, the response was negative. No participant thought their current system was ideal. Even those participants that were generally happy with their current system, pointed to weaknesses in it when dealing with the greater organisational construct and collaborative work groups. Whilst some participants acknowledged weaknesses in their internal networks, universally they are aware of fundamental flaws when dealing with external networks.

Having said this, many of the participants were hesitant and unsure about their own ability to participate in the study. This raised issues about their understanding of the function of an information security management system. The interviews confirmed many participants' uncertainty about what actually is their organisation's information security management system and their uncertainty about their particular role in it. Those participants that presented as more confident tended to perceive information security management as a largely technical function. Interestingly, those that presented as less confident were still clearly able to indicate information security issues that were providing obstacles to their work performance or work place harmony.

This was an indicator for an emerging trend. A review of the results showed a common pattern. There is a lack of clarity and cohesion amongst stakeholders about how their information security management systems operate and who has ownership of the security function within their organisations. There are also indications that the social and political environment affects stakeholder relationships and corporate communications. This, in turn, influences the corporation's information security function. Not surprisingly, prevalent socio-political issues, pertaining to stakeholders, also affected the research process.

The data analysed to this point, primarily relates to the beneficiaries and outcomes of the systems. It relates information relevant to participants' perceptions of their current information security management systems and participants' ideas on what would be present in an ideal information security management system for distributed work groups. It appears, at this point, that there is a discrepancy between what is currently considered the client of the system and whom interview participants believe should be a client of the system. Most noticeably, employees in the current system are not acknowledged as clients. However, in the ideal system employees feature prominently as clients.

Additionally, participants stressed that information security management is critical to efficient and effective distributed organisational operations. This appears to indicate an important inconsistency between the current and the ideal systems. Participants tended to believe that the current system is impeding their performance and creating operational inefficiencies with distributed work groups. In particular, they questioned the rationale behind restrictions placed on access to information they deemed necessary to do their job. This appears to impact organisational morale. Research participants also noted a lack of clarity, consistency and awareness of information security permeating through the organisation. Some indicated this was a leadership issue. Emphatically participants pointed to the provision of accessible / useable information as a primary purpose in an ideal system. They also clearly emphasised the protection of

information for individuals and the organisation. This supports the finding that stakeholders do not consider their current system to be optimal.

Validity and Reliability

The interpretivist approach adopted here, views knowledge as a social and historical product (Miles & Huberman 1994 p.4). In other words, facts do not come to us in a vacuum. They are laden with theory and preconception. 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. In this project, the focus is on the multi-level contextual nature and the interdependent network of ideas, machines and people that impacts information security management of distributed work groups. The research was designed to get to the construct by seeing different instances of it, at different moments, in different places and with different people. As such, a variety of data types, sources, participants, events, places, theories and methods are incorporated into the study.

The researcher's data collection and subsequent interpretations have been systematically recorded and reflexively reviewed. This included acknowledging the researcher's own assumptions on what has been observed (Ibid., 2002). Importantly, the partial nature of the interview transcripts, audio recordings and written texts was respected so as to avoid misrepresentation of data out of context.

FUTURE RESEARCH

Research Objectives

The ongoing primary objective of this study is to investigate the major information security management issues involved with implementing distributed work groups. The end objective of the research is to identify how the issues could be better managed through the development of an ideal systems model.

Research Methods

As discussed earlier, the basic structure finds four discrete case studies being researched, each self contained and evaluated. The first three are described above. The fourth is a very large firm, with international interests, that predominantly operates throughout Australia and has a strong presence in Western Australia. Research participants have been nominated and interviews have commenced.

The primary data collection method is in depth, interpretive interviews on participants perceptions of the problem situation. Field studies are also being conducted. Secondary data will include a wide range of public and corporate documents. The data collected will then be analysed using Soft Systems Methodology to develop current and ideal models of information security management of distributed work groups.

The different stages in Soft Systems Methodology, as used in this study, include considering the problem situation unstructured. Data will be collated and represented in diagrams, called rich pictures. These rich pictures will be used to identify relevant systems including primary tasks and issues of concern. Root definitions will then be developed for them. Based on the root definitions, conceptual models known as holons or human activity systems, will be developed representing a particular view of the core purpose of the activity system. These holons can then be compared to the real world as epistemological devices, providing opportunity for organisational participants to further reflect and comment on the problem situation (Checkland 1981).

The research process will remain highly flexible, reiterative and reflexive (Hicks 1991), in keeping with an interpretive, constructionist paradigm. Throughout the project, there is free movement between the different research stages and work on different stages is undertaken concurrently. This flexibility has proven very important to this point, when dealing with the large number of interviewees and the complex problem situation in this study. The researcher's interpretations, selection, and coding decisions will be later validated via inter-rater reliability, a comparative researcher method. The results then will be verified and validated by seeking feedback from both internal and external study participants.

Model Production

This research approach enables participants to determine collectively what the problem situation is and how it looks. Participants also determine and illustrate how the problem situation would look in a perfect world. The models developed will then be presented back to the participants for comment, enabling refinements, verification and validation. Thereby they collectively devise an ideal model (Checkland & Scholes, 1990) using the researcher as a facilitator to collate perceptions and provide opportunity for collaboration. Thus, the project utilises Soft Systems Methodology as a collaborative tool whereby the views of the participants are collected, interpreted, collated and pictorially represented.

This will make it possible to compare how information security management systems for distributed workgroups currently operate, with how the participants think they should operate. Reflection on how to address the gap between the two will result in a series of recommendations. These may assist the development of a future course of action for implementing improvements and change. Additionally, representatives across the organisational spectrum were able to contribute to the design of the system and take ownership for its outcomes. As a result, informed participants have the potential to act as a dissemination mechanism.

CONCLUSION

This paper notes the growing trend towards more adaptive, emergent organisational structures in response to global market pressure. Enabled by swift technological advances, organisations are distributing staff across geographical and temporal zones, so that they may capitalize on market opportunities wherever they may be presented. These new technological and organisational practices, however, also bring with them additional information security threats and risks, costing industry billions of dollars yearly in lost income. A socio-political perspective on managing information security management is expected to give new insight to the problem. This paper outlines a current research project, using case studies and soft systems methodology, to investigate the issues within the Western Australian context.

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), *Qualitative 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.
- Truex, D., Baskerville, R., & Klein, H. (1999). Growing systems in emergent organizations. *Communications of the ACM*, 42(8), 117-123.
- Wainfan, L. & Davis, P. K. (2005). *Challenges in virtual collaboration: Videoconferencing, audioconferencing, and computer-mediated communications*. RAND:National Defense Research Institute

- 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

Rosanna Fanciulli © 2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.