Current directions in IS security research: towards socio-organizational perspectives

Gurpreet Dhillon* & James Backhouse†

*College of Business, Box 456009, University of Nevada, Las Vegas, NV 89154, USA, email: dhillon@nevada.edu, and †Department of Information Systems, London School of Economics, London, UK, email: j.p.backhouse@lse.ac.uk

Abstract. *The purpose of this paper is to map the current territory of information systems and security research. It uses the Burrell and Morgan framework as an intellectual map to analyse the socio-philosophical concerns in various information systems and security approaches. The paper's contributions are in its analysis of trends in information systems and security research, the former in stressing the socio-organizational perspectives and the latter in criticizing the preponderance of technical solutions. The paper also sets an agenda for a future research emphasis.*

Keywords: interpretive perspective, IS security research, socio-organizational perspective, socio-philosophical concerns

INTRODUCTION

Until quite recently there has been reluctance within most organizations to tackle the issue of information systems security. Even in situations where companies are aware of specific security methods and approaches, the consequences have been rather disappointing. A clamorous case in point was Barings Bank, revealing the stress on narrow, technically oriented audit techniques and the inability of management to detect significant discrepancies (e.g. see Rawnsley, 1995). It is estimated that annual losses within the US alone may be anything between $500 million to $5 billion (Flanagan & McMenamin, 1992). A 1999 Computer Security Institute survey put the losses at $124 million among the surveyed companies. There have been voices of concern, in both the academic and practitioner world, that such losses are going to increase (e.g. Schwartz, 1990; Angell, 1995; Angell, 1996). To comment authoritatively on such issues of concern, it is therefore important to analyse the intellectual origins of the current approaches to managing information systems and security.

The scope of this paper is to review and assess the current body of knowledge in the subject of information systems security. The subject is broken down into two constituent disciplines of information systems and security. The paper is organized into five sections. After the introduction, section 2 presents a conceptual framework that is used to traverse the literature.

Section 3 surveys the trends in information systems and security research. The paradigmatic orientation of the respective literatures is identified as a way of establishing future research emphases in regards to current research. Section 4 discusses and summarizes the findings so far. Section 5 highlights the contribution of this paper.

THE CONCEPTUAL FRAMEWORK

In order to review the vast literature in information systems and security, we need a conceptual framework that helps us not only to classify the works but also to trace their intellectual origins. Theorists such as Burrell & Morgan (1979), Lane (1994) and Walsham (1993) assert that it is important to understand the theoretical concepts that form the basis of a methodological approach. Such understanding allows researchers to cut through the surface detail that overlays different approaches and hence indicate the philosophical assumptions of the approaches.

It is important to understand the conceptual basis of various security approaches if they are to be used in a systematic and appropriate manner. Often certain approaches are critiqued because of their intellectual origins but from a limited understanding of the context in which they are used. As most information system security approaches have traditionally been grounded in positivism, researchers associated with alternative paradigmatic thought may engage in 'positivist bashing'. Critics point to the futile search for the same type of knowledge as found in natural science, which can be characterized as analytical and value free and with only occasional efforts that consider the subjectivism of the applications. Clearly, there are positive and negative aspects of all approaches, and it is inappropriate merely to critique one against another solely on the basis of its intellectual provenance. The context in which an approach is used should be the key factor when critiquing methods. Non-positivist researchers have increasingly looked towards social sciences for a suitable theory of knowledge. Sociology, in particular, offers a wide array of theories which can provide interesting insight, and many information systems researchers have been informed by these theories. In fact many have argued that information systems are social systems (e.g. see Ulrich, 1984; Walsham *et al.*, 1990; Stamper, 1991; Lee & Liebenau, 1996). This line of argument draws credence from the work of those who equate an information system to an organization (e.g. Stamper, 1973), i.e. an organization is constituted of informal, formal and technical parts (e.g. Liebenau & Backhouse, 1990). And computer-based systems are but just a small part of the technical component (e.g. see Dhillon & Backhouse, 1996).

Burrell & Morgan (1979) organize various organizational theories along two axes and position them in the four emergent paradigms of sociology. Burrell & Morgan (1979) believe that all theories of organization rely upon a philosophy of science and a theory of society. Diagrammatically the researchers represent the assumptions about the nature of science to be located along the subjective–objective continuum, and assumptions related to the nature of society along the regulation–radical change continuum. The objective nature of social science

is usually described as 'sociological positivism'. It is characterized by the application of models and methods derived from natural science to study human affairs. The subjective dimension stands in complete opposition to this and denies the relevance of models and methods of natural science to studies in this realm. 'Regulation', according to Burrell & Morgan (1979), emphasizes the stability and cohesiveness of the society, whereas 'radical change' views, by contrast, emphasize societal conflict and domination. Using these two dimensions, four paradigms have been suggested: functionalist, interpretive, radical humanist and radical structuralist.

Functionalist paradigm

The functionalist paradigm represents a perspective that is firmly rooted in the 'sociology of regulation' and approaches the subject from an objectivist point of view, concerned with the 'regulation' and control of all organizational affairs. Researchers grounded in this paradigm tend to provide practical solutions to practical problems. In the tradition of Durkheim, functionalists assume the social world to be composed of concrete empirical artefacts. They assume that such artefacts and their relationships can be studied by deriving approaches from the natural sciences.

Interpretive paradigm

Arising from the work of Weber, interpretivism is grounded in the philosophy of phenomenology. It is concerned with the subjective understanding that individuals ascribe to their social situations. Although interpretivists agree with the regulative principles of the functionalists, they believe in a subjective analysis of the social world. Their fundamental concern is to study the world as it is. The intentional act figures as the core concept in interpretive sociology, and proponents emphasize the need to understand such acts and link them with the meaning of conduct. Consequently they consider social reality as 'a network of assumptions and intersubjectively shared meanings' (Burrell & Morgan, 1979; p. 28). Reality results as an emergent property of the actions of individuals.

Radical humanist paradigm

This paradigm opposes the regulation theories and espouses radical change. Viewing society as antihuman, radical humanists stress the emancipation of human beings so that they may realize their full potential. Structural conflicts and modes of domination are also explored. Underlying radical humanism rests the core notion 'that the consciousness of man is dominated by the ideological superstructures with which he interacts, and that these drive a cognitive wedge between himself and his true consciousness. This wedge is the wedge of 'alienation' or 'false consciousness', which inhibits or prevents true human fulfilment' (Burrell & Morgan, 1979; p. 32).

Radical structuralist paradigm

This paradigm also presents a viewpoint that opposes the regulation view of society. While advocating radical change, radical structuralists share the objectivist standpoint of the functionalists. The key notion of the radical structuralist is that 'change in society inevitably involves a transformation of structures which, even given favourable circumstances, do not fall or change of their own accord' (Burrell & Morgan, 1979; p. 358). Consequently, they consider the structures to change radically, thereby generating conflict and disruption in the status quo.

The four paradigms discussed above are defined by the meta-theoretical assumptions that form the frame of reference and the mode of theorizing (this definition of a paradigm differs somewhat from Kuhn's conception. A paradigm, according to Kuhn, is a universally recognized scientific achievement that for a time provides models, problems and solutions to a community of practitioners). Each paradigm emphasizes the commonality of perspective, although there may be much debate among those who adopt different standpoints. Burrell and Morgan maintain that theorists belonging to a particular paradigm may not even recognize the alternative views of reality that lie outside their boundaries. They also assert that the four paradigms are mutually exclusive and contradict each other and as a consequence no socio-theoretic viewpoint may belong to more than one paradigm at any given time.

The fourfold classification of organizational theories based on sociological paradigms as proposed by Burrell and Morgan, is not without its critics. Many sociologists have considered the classification to be overly simplistic (e.g. see Hopper & Powell, 1985; Chua, 1986). Others regard the two analytical dimensions to be synthetic and incapable of dealing with subtleties of social theories (e.g. see Gutting, 1980; Reason & Rowan, 1981). Burrell and Morgan, however, assert in respect of the philosophical issues discussed earlier that a paradigmatic orientation for understanding organizational theory is essential. They consider the four paradigms to be 'in essence distinct, internally coherent and self-sustaining' (Burrell & Morgan, 1979; p. 396). Jackson & Carter (1991) consider this paradigmatic apartheid to serve as a defence against 'scientific authoritarianism' hence avoiding emasculation and incorporation of approaches within the functionalist paradigm (Burrell & Morgan, 1979; p. 398).

The Burrell and Morgan framework has also come under attack because of the inherent notion of paradigm incommensurability. However, arguments both in favour and against paradigm incommensurability can be found in the literature (e.g. see Mathews *et al*., 1999 who examine the notion and the present state of theoretical diversity in organization theory). Despite the criticisms voiced concerning the classification proposed by Burrell and Morgan, it has nevertheless been widely used in the literature. Lane (1994), for example, uses it to trace the philosophical origins of operations research and system dynamics. Hirschheim & Klein (1989) have applied it to the area of information systems development. Schultze (1998) uses it to categorize research in knowledge management and identifies contradictions that emerge because of the enabling and constraining qualities of each paradigm. Works of Orlikowski & Baroudi (1991) and Jönsson & Macintosh (1997) have also compared and contrasted functionalist, interpretivist and critical perspectives. (These researchers have collapsed the radical humanist and radical structuralist paradigms into a *critical* perspective. One argument afforded

in support is that the Burrell and Morgan framework does not accommodate post-structural theories. This argument perhaps stems from the omission of Foucault's work.) Such varied application gives credibility to the Burrell and Morgan classification. Therefore, the use of the four paradigms as a means to classify the literature in information systems and security and to interpret the intellectual origins of the respective approaches appears both valid and legitimate.

RESEARCH IN INFORMATION SYSTEMS AND SECURITY

This section classifies research in information systems and security. It identifies the key characteristics of particular research efforts and systematically places them within the socio-philosophical framework of Burrell and Morgan.

Research orientations in the functionalist paradigm

Burrell and Morgan contend that research grounded in functionalism focuses on investigating the causal laws and hence takes a rationalistic view of phenomena under investigation. Furthermore, they suggest that functionalist research tends to express the objective and expert viewpoint of management.

Information systems literature

Alongside numerous other approaches, contingency theory research belongs to the functionalist paradigm. Contingency theory, as introduced by Woodward (1965), explored the relationship between organizational structures and technical systems. She revealed that organizational effectiveness was the consequence of a match between a situation and a structure. Information systems researchers have used contingency theory concepts to establish matches between the organization and its environment. Ives *et al*. (1983), for example, used the approach to determine information system success by reference to user satisfaction. The majority of the earlier literature on identifying user requirements is also based on contingency theory (e.g. Bailey & Pearson, 1983; Davis & Olson, 1984; Baroudi *et al*., 1986).

Many information systems researchers have continued to use concepts rooted in contingency theory, although the core research concepts have increasingly been criticized as simplistic because human beings and organizations are far more complex than implied by this theory. Such criticisms are especially relevant in the context of changing organizational structures – from relatively stable hierarchical structures to loosely coupled arrangements (see Orton & Weick, 1990). The socio-technical designs of Mumford & Weir (1979), though not strictly functionalist in nature, are subjected to criticism on similar grounds. This is because they do not consider organizations as loose couplings where conflict, politics and power dominate. Taking user satisfaction as an indicator of system success has also come under severe criticism (e.g. Melone, 1990), because there is an attempt to quantify the variables without

understanding the relationships. An abstract concept such as user participation cannot be understood in terms of any single organizational activity and, thus, poses complex problems of quantification.

Although the 'bureaucratic phenomena' of Weber (1947) and 'scientific management' of Taylor (1911) have had a profound impact on researching organizations, within the domain of organization studies such concepts have been increasingly critiqued. Much of the criticism questions the relevance of the machine metaphor as an adequate representation of modern day organization, especially in view of advances in information and communication technologies (see reviews by Walsham, 1991; Kendall & Kendall, 1993; Kendall & Kendall, 1994). A thorough review and critique of structuring of organizations can be found in Orton (1994) and Orton & Weick (1990).

Mechanistic orientation also has had a significant influence on the development of information systems within organizations. Kling (1987) terms these engineering conceptions as 'discrete-entity' models. He considers that the focus of mechanistic models is squarely on the economic, physical and information processing aspects of technology. As a result such models ignore the context of complex social actions in which information technology develops. Locked in the mechanistic viewpoint of organizations, many information systems professionals may neglect the socio-political facet of information systems, with inevitable knock-on effects of inflexibility, rejection and failure.

Likewise similar debates have reverberated in the organizational strategy literature. Such debates have focused on the merits and demerits of rationally planned and emergent strategies (a summary can be found in Quinn *et al*., 1988). Interestingly, with respect to information systems strategy formulation and implementation, many information systems researchers and practitioners have tilted in favour of rationalistic approaches. In particular, the competitive strategy of Porter (1980) and the value chain of Porter & Millar (1985) have significantly influenced strategic thinking within the information systems domain. This has resulted in strategy researchers being more concerned with overall business performance than with the organizational information handling activities. Many other strategists have developed variants of Porter's conceptions. Notable among them are the Strategic Option Generator (Wiseman, 1985), Strategic Opportunity Matrix (Benjamin *et al*., 1984) and the Strategic Grid (McFarlan *et al*., 1983). Mainstream strategy research has also critiqued the options and alternatives generating research, so common for the rationally planned approaches and has instead highlighted the relevance of the more emergent 'value focused thinking' (e.g. refer to the arguments proposed by Keeney, 1992).

Connoisseurs of functionalist thinking need look no further than popular systems analysis tools and techniques. A classic case would be in DeMarco (1978; p. 13), for example, where he expounds that 'political problems aren't going to go away and they won't be 'solved'. The most we can hope for is to limit the effect of disruption due to politics. Structured analysis approaches this objective by making analysis procedures more formal'. With respect to requirement assessment for designing databases, McMenamin & Palmer (1984) assert that there should be one reality and it should be the same for everyone. Only if the system requirements meet this criteria, will these be termed as 'true requirements'. Therefore, developers

are urged to develop systems that model this reality (Griethuysen, 1982). Naturally when implementing such systems, professionals may choose from an equally high proportion of functionalist strategies. Most of the planned change literature falls into this category and prominent among these are the implementation (Lucas, 1981; Alter, 1992), counterimplementation and counter-counterimplementation strategies (Bardach, 1977; Keen, 1981). Experience shows, however, that the social and political aspects of organizations appear to have a significant impact on the manner in which information technology systems are conceived, designed and implemented. Information technology failures such as the baggage handling systems at Denver International Airport and Chek Lap Kok airport in Hong Kong are cases in point.

Recent emphasis on social considerations when designing, implementing and managing information systems has resulted in functionalist approaches being criticized for two basic assumptions. First, that there is an objective empirical reality and that positivist methods are the best way to make sense. Second, that the social world is best conceived in terms of an integrated order and hence system and organizational objectives are legitimate and have been agreed upon (this synthesis is based on the arguments presented by Burrell & Morgan (1979: pp. 118–220) while discussing functionalist organization theory). Because of these assumptions, the behaviour, intentions and domination patterns of people have largely been ignored. Many authors now agree that the positivism espoused by functionalist thinkers is inappropriate for the study of information systems (see, for example, Boland, 1985; Klein & Lyytinen, 1985; Walsham, 1995). This is because it fails to provide a 'rich picture' of the complex interplay between the technological structures and the behavioural patterns. Various organizational theorists, particularly those grounded in functionalism, have also realized the limitations and problems with a positivist mode of inquiry. Notable among these is the work of Silverman & Jones (1973) and Silverman & Jones (1976), which, in contrast to the position articulated in *The Theory of Organizations* (Silverman, 1970), adopts an alternative paradigmatic view.

Security literature

The focus of most research in information systems security is concerned with the formal automated part of an information system. Traditionally, this has been studied under the banner of 'Computer Security'. This subsection reviews the security literature under three subheadings: checklists, risk analysis and evaluation.

Checklists

One of the most prominent methods for addressing the security of technical systems has been checklists. Checklists help in identifying every conceivable control that may be implemented. The underlying idea is to ask the question: 'what can be done rather than what needs to be done' (Baskerville, 1993). In the functionalist tradition, checklists tend to concentrate on means not ends (Hirschheim & Klein, 1989). Many of the prevailing security checklists were constructed initially as evaluation guidelines, enabling an analyst to check the computer-based

system and determine the necessity of existing controls and the possibility of implementing new ones. Typical examples in this category are IBM's 88-point security assessment questionnaire (IBM, 1972), the SAFE *Checklist* (Krauss, 1972; Krauss, 1980) and the *Computer Security Handbook* (Hoyt, 1973; Hutt *et al*., 1988). The *AFIPS Checklist for Computer Center Self-Audits* (Browne, 1979) while addressing similar issues of disaster planning, encryption, off-site backup and physical security, marks a slight departure in its approach from the other checklists. Rather than providing a simple taxonomy of threats, it develops a kernel style framework of threats and the related defences (Baskerville, 1993). The AFIPS and the SAFE checklists are in general oriented towards computer centre audits.

The checklist approaches, although still widely used, carry less conviction when searching for theoretical foundations in security. They indicate where exclusive attention has been given just to the observable events without considering the social nature of the problems. Checklists inevitably draw concern onto the detail of procedure without addressing the key task of understanding what the substantive questions are. Procedures are constantly changing and for this reason offer little in the way of analytical stability.

Risk analysis

Most risk analysis approaches grounded in the functionalist paradigm draw mechanical and biological analogies (e.g. Van Der Veen *et al*., 1994). Prominent work in risk analysis and security evaluation methods takes this orientation and consequently adopts a prescriptive and normative mode. The methods suggest that negative events can be prevented and information systems can be made secure if countermeasures are developed and implemented in a logical sequential manner. Most risk analysis approaches (e.g. Parker, 1981; Fisher, 1984; Birch & McEvoy, 1992; Kailay & Jarratt, 1994) prescribe methodologically discrete steps. Such approaches can be considered to have developed linearly and controlled 'scientifically'. The Structured Risk Analysis methodology of Birch & McEvoy (1992), for example, views an information system in terms of data structures, data processing and events in a system. The fundamental principle in evaluating risk is to see the correspondence between threat and vulnerability. The approach is grounded in systems theory concepts. Other risk analysis and evaluation approaches also have similar philosophical underpinnings (e.g. Parker, 1981; Fisher, 1984; Zyl *et al*., 1994).

Risk analysis has indeed become the watchword of modern security management, and has enabled organizations to cost justify new information systems security and avoid the implementation of unnecessary and expensive controls. Practically all researchers of information systems security use risk analysis in one form or another (Baskerville, 1991). Risk analysis techniques provide a means of forecasting critically the financial benefits *vis-à-vis* the initial investments. Such management science principles laid the foundation for techniques that were proposed by researchers such as Courtney (1977) and Wong (1977). For instance, Courtney defines risk (R) in terms of the probability (P) of an exposure in a year and the cost (C) – or loss – associated with the exposure. Therefore, risk is calculated as: $R = P \times C$. The US Department of Commerce declared risk analysis based on Courtney's technique as govern-

ment standard (US Department of Commerce, 1979). Consequently this technique has been widely used and forms the basis of a number of proprietary variants (e.g. Badenhorst & Eloff, 1990).

Paper-based approaches have given way to automated risk analysis methodologies, such as CRAMM (CCTA Risk Analysis And Management Methodology), used to conduct risk analysis and other related management reviews. Another example of a once widely used automated security risk analysis tool is RISKPAC (Computer Security Consultants, 1988). Besides seeking to provide a balance between quantitative and qualitative risk analysis, RISKPAC also calculates annualized loss expectancy, thereby adhering to Courtney's conventional risk analysis.

Risk analysis has also been a subject of interest to researchers. Merten *et al*. (1982) look at the technique from a managerial perspective whereas Boockholdt (1987) cites its importance in establishing security and integrity controls. Anderson *et al*. (1993) outline risk data repository for a 'dynamic risk evaluation'. Krueger (1993) proposes a 'functional control matrix' for risk assessment, which is based on the work carried out at The World Bank. Saltmarsh & Browne (1983) and Gallegos *et al*. (1987) differentiate between risk analysis and risk assessment, the former the process of identification, the latter the degree of exposure. Using this differentiation, Gallegos *et al*. (1987) comment on the usefulness of risk analysis in establishing monetary value of the risks.

Risk analysis has had an influence on a number of other approaches. Examples among the earlier work include Parker's programme (Parker, 1981) and Fisher's methodology (Fisher, 1984). Both approaches use risk analysis as a means to design controls. However, Parker introduces a different kind of analysis, the 'exposure analysis', which supposedly eliminates the elements of guesswork and consensus determination. He also proposes an alternative threat model. Loch *et al*. (1992) have gone further to develop a four-dimensional model of IS security focusing on threat identification. Von Solms *et al*. (1993) apply risk analysis approaches to develop a 'process approach' to information security management.

Baskerville (1988) in contrast attempts to minimize the importance attributed to risk analysis by embedding controls in the logical model of an information system. Baskerville feels that the 'best approach to the development of security analysis and design methodology, both for office use and for field practice in general, would essentially be to nest it as a component part of an existing, established, successful overall information systems analysis and design methodology' (p. 88). He suggests that structured security analysis and design can be carried out in much the same way as a structured systems analysis. He chooses DeMarco's structured systems analysis and specification approach and implements controls, by developing formal heuristics, in its logical design phase.

Criticism of the use of risk analysis as a basis for developing secure systems has always been strong. Clements (1977) regarded classical probability theory to be inappropriate for assessing security risks because threats are invariably random in nature, offering instead a methodology based on the theory of fuzzy sets for evaluation of data processing installations.

Whatever the claim of one risk analysis method compared with another, very little difference appears in the basic theoretical assumptions. A careful consideration of most risk analy-

sis approaches suggests that the boundaries between different classes of risk analysis are uncertain. Despite the diversity reflected in the literature, the issues that separate the different classes are of minor rather than major significance. As Burrell and Morgan note, 'the real big issues are rarely discussed, lying hidden beneath the commonality of perspective which induces organization theorists to get together and talk with each other in the first place' (p. 120).

Evaluation

Another category of research in computer security is in evaluation methods, whose rationale stems from the need to measure security (Longley, 1991). Although it is often difficult to place a value on the level of security, a number of techniques exist which help in grading the security of systems. Early work on establishing such levels of assurance was sponsored by the US Department of Defense. The emphasis was to prevent 'unauthorized disclosure of information'. Among the various models of secure systems, the *Bell La Padula Model* (Bell & La Padula, 1976) was the most prominent. The model deals with mandatory and discretionary access control with the primary objective of preventing illegal disclosure of information.

In 1983, the National Computer Security Center in USA published the Trusted Computer Systems Evaluation Criteria, targeted at Automatic Data Processing systems. These provided computer vendors with an evaluation procedure to develop trusted computer systems. Today these criteria form an integral part of the US Department of Defense security procedures. Recently, research has been carried out to improve and supplement these evaluation criteria. Chokhani (1992), for example, expands upon these criteria and proposes an Information Security (INFOSEC) approach to such an evaluation. However, the improved evaluation method takes a discrete event-oriented approach. This creates a narrow technical conception about security, which delimits it from the organizational context.

Hoffman *et al*. (1978) adopted a different basis for security evaluation. They proposed an automated tool, SECURATE, which is a design and selection process. The system automates the security analysis process and provides detailed ratings of a system security profile. SECURATE calculates the security ratings on the basis of fuzzy set theory and ultimately outlines the strengths and weaknesses in system design. Critics have, however, contested the statistical validity of fuzzy metrics.

Besides the US, evaluation criteria have been established in other countries as well. In the UK, for example, the Department of Trade and Industry and the Government Communications Headquarters produced a series of 'Green Books'. These were specifically intended for the Commercial Computer Security Centre. Other countries have also been quite active in this area. In an attempt to harmonize the work on information security standards in Europe, France, Germany, The Netherlands and the United Kingdom decided to combine the best features of each of the national initiatives. As a consequence, in May 1990, the first draft of the Information Technology Security Evaluation Criteria was issued. The text is referred to as the 'White Book'. Evaluation criteria, while having found public approval, still fail to provide answers to

many important questions and are unacceptable to a body of researchers in the area (e.g. McLeen, 1990). Again the main criticisms centre on the technical nature of the approaches. The national level initiatives tend to focus on 'The One Best Way', typically grounded in the 'organization as a machine' metaphor and scientific management as advocated by Taylor. The White Book, for example, stresses but fails to take a holistic view of the organization and hence is extremely static. Because of such an orientation, an over-emphasis on the explanation of status quo results.

BS7799, the British Standard for information security management, has emerged as a phenomenally successful vehicle for addressing security management issues in organizations, with take-up across the globe from Australia to Sweden. However, the problem of using the standard as a basis for evaluation remains a hard nut to crack. In the UK the *c:cure* scheme was launched by the Department of Trade and Industry to allow 'accredited certification', by approved auditors, of security management in organizations. But the certification was qualified strongly by the UK Trade and Industry Minister Michael Wills at the 1999 Infosec conference: '*. . .* of course c:cure cannot provide absolute guarantees. Rather it is a business enabler. It does show that certificated organizations are committed to information security'. Such an admission testifies to the limited scope of evaluations of security of this kind.

The research carried out on security has indeed enriched the field of information systems. It has been possible to implement legislative measures, especially in relation to a variety of technological crimes and privacy related issues (Turn, 1982; Bequai, 1987). These have also helped in implementing operational security, making it possible to establish management control by setting objectives and guidelines for accountability, surveillance and authority (Hsiao *et al*., 1979; Norman, 1983; Weber, 1988). Threats and risks can also be identified with a reasonable amount of precision. As users now have greater access to computer-based information systems than before, identification and authentication methods have been well researched. However, the focus of attention has shifted and in particular database access control has received much attention (Highland, 1985). Database access control mechanisms often have a legislative bearing, and this has led to relating access control issues to those of privacy (Garfinkel, 2000).

In spite of some basic benefits accruing from the evaluation methods, there is limited long-term usefulness. The security evaluation approaches run into serious problems because they tend to provide essentially rational explanations of social affairs. The traditional approaches, developed for military use, have now been translated for commercial use. Because the social world of a defence environment is significantly different from a commercial setting, there are compatibility and coherence concerns.

To summarize, the main characteristics of the risk analysis and security evaluation approaches can be enumerated as follows:

1 Organizations and the information systems are considered in terms of strict boundaries which differentiates them from each other and the environment.
2 Information systems and security management are conceptualized as being processual in nature and hence focus on the input, throughput, output and feedback mechanisms.

3 Organizations and their information systems are considered secure if the needs of models (subsystems) are satisfied (i.e. by having secure subsystems, we can have a secure organization).
4 Different models that help in securing parts of an information system are mutually interdependent.
5 Overall security can be achieved by analysing the behaviour of constituent elements of the system.

Indeed these characteristics of the prevailing approaches offer a very narrow conceptual framework with which to address information system security issues. Although the sections below present different orientations in information systems and security research that lend support to the above conclusion, further research is necessary to provide empirical evidence to lend support or refute the above statements.

Research orientations in the interpretive paradigm

An alternative view to functionalism is that of interpretivism. While most of the current and past research in information systems and security is confined to the functionalist paradigm, researchers have begun gradually to consider the philosophical aspects of interpretive sociology. This trend towards providing explanations within the realm of individual consciousness and subjectivity is more prominent among mainstream information systems literature than in security research.

Information systems literature

The common theme in most research efforts is to appreciate the social implications of computer-based information systems. Consequently there is an increased awareness of the cultural and informal aspects of information handling. Research in this paradigm does not take the 'what is' approach of the functionalists. Rather the organization and social world is studied 'as it is'. The social world therefore is viewed as an emergent process, created by the individuals concerned.

The main proponents of interpretive research have been Orlikowski & Baroudi (1991) and Walsham (1993). They have used Giddens (1984) structuration theory to study information systems use within organizations. With concepts rooted in structuration theory, Walsham (1993) has developed a synthesized framework for interpreting information systems within organizations. This framework pays particular attention to the content, social context and social processes. Walsham attempts to address the matter by analysing the connection between context and process. In order to study the context (in the domain of information systems) Walsham draws on the 'web models' of Kling & Scacchi (1982) and Kling (1987). The web models study the social context of information systems by considering the social relations of the participants, the infrastructure of the available support and the history of previous developments. Walsham studies processes in terms of the culture and politics that prevail in an

environment. The process model so generated draws heavily from work by Boland & Day (1989), Zuboff (1988) and Markus (1983). In the final synthesis he establishes a link between the context and the process.

Walsham's research also draws on the contextualist analysis of Pettigrew (1985) which inspired many researchers in both management (e.g. Fincham, 1992) and information systems (e.g. Madon, 1991; Symons, 1991). The essence of the approach is in unfolding the interaction between structure and process. It views change as an outcome of the interplay between the historical, processual and contextual aspects of an enterprise (Whipp & Pettigrew, 1992). Criticism of contextualism has come from Murray (1989), who argues that although contextualist research provides an insight into the trends and events in historical, cultural and political terms, it does not explain why the events take place.

Information system research has seen another trend. Recognizing the shortcomings of previous descriptions, many researchers have extended and modified frameworks developed in the past. Galliers & Sutherland (1991) for instance have revised Nolan's (1979) Stages of Growth Model. Although Nolan's theoretical basis came under criticism (Benbasat *et al*., 1984), his ideas provide a useful foundation for strategic planning. A similar trend is also seen in the work of (Ward & Griffiths, 1996). They have developed the portfolio model for information systems strategic planning based on the generic strategies of Parsons (1983). Ward & Griffiths (1996) consider organizational reality to be meaningfully constructed from the point of view of actors directly involved. Such conceptions in developing frameworks suggest a trend towards a more interpretive rather than a causal explanation.

A shifting emphasis of researchers towards the social considerations in information systems research led to importance being given to power and politics in organizations. Some pioneering work was carried out by Keen (1981) on organizational change and by Markus (1983) on the power and politics of information system implementation. This has given rise to a variety of approaches, which consider emergent forms of organizations as a consequence of social interactions. In examining the influence of information systems on organizational structure in particular, many researchers acknowledge the importance of social phenomena such as power, authority and responsibility (Buchanan & Linowes, 1980; Bloomfield & Coombs, 1992; Fincham, 1992; Roach, 1992). Some theorists have even regarded designing information systems as similar to designing power systems (Boland, 1986). Others have viewed computer-based information systems as social resources having little influence on power systems (Kling, 1980; Wynne & Otway, 1982; Kling, 1991). Mintzberg (1983), writing on the theory of management policy, highlights the concept of power in relation to influence, authority and control. He regards power to be central to all management activities. While he discusses the various issues related to this social phenomenon, he does not comment upon the manner in which the structures of power, authority, influence, control and responsibility can be identified.

Other research directions in information systems attempt to bridge a gap between man and machine, whole and part, the unique and the repetitive. Semantics, the study of relationships between signs and what they refer to, has been used in the study of information systems (e.g. Andersen, 1990; Backhouse, 1991). The inherent argument in this strand of research is that symbols have meanings that are socially determined and that culture mediates between the

formal systems and reality. Liebenau & Backhouse (1990) stress that in analysing and developing an information system, consideration should be given to the assumptions, beliefs and expectations of agents involved. A related study by Lehtinen & Lyytinen (1986) considers information systems as formal language-based systems whose use can be studied as linguistic processes. Lyytinen & Klein (1985) have used these concepts as a basis for a theory of information systems. Dobson *et al*. (1991) use speech act theory for evaluating conversation structures when determining requirements for computer-supported co-operative work. In a similar spirit Wand & Weber (1990) adopt an ontological approach in addressing issues concerned with the semantics of information systems. Leifer *et al*. (1994) stress the importance of 'deep structure information' in eliciting requirements for an information system. They propose a 'focus group' technique in conducting such an exercise. These studies take a processual mode of inquiry and attempt to interpret social actions over a period of time.

In recent years, the interpretive approaches have also been a subject of much debate and criticism. Orlikowski & Baroudi (1991), for example, debate the relative merits and demerits of interpretive and positivist approaches. Lee (1991) and Gable (1994) have explored the possibility of combining largely positivist and interpretive approaches. In the Burrell and Morgan tradition such combinations and meta-theorizing is not possible, although more recent research in sociological theory is sympathetic to such trends. Ritzer (1992), in particular, is a strong advocate of developing integrated sociological paradigms.

Security literature

Given the pace of evolution in modern organizations, an increasing number of information systems researchers have begun adopting socio-organizational perspectives for the design of systems. However, approaches to managing information security still seem to dwell on the 'organization as a machine' metaphor (see Walsham, 1991) and fail to consider stakeholder interests, using designs rooted in the instrumental interpretation of events.

Siponen (2001) classifies such approaches into first, second and third generation methods, with most emerging from the computer science and database management communities. Siponen argues that there have been but a few isolated endeavours to consider the socio-technical aspects of information system security management (e.g. Backhouse & Dhillon, 1996; Hitchings, 1996; James, 1996). Among this group is also the work by Willcocks & Margetts (1994) to assess information system risks using Pettigrew's contextualism. The conceptual framework developed by Willcocks and Margetts highlights the value of historical, context-oriented, processual analysis and underlines the importance of social and qualitative aspects of information systems security.

The technique of risk analysis has been a subject of debate among many researchers. Beck (1992) and Baskerville (1991), for example, believe that over-reliance on risk analysis as a technique in the design of secure information systems has negative consequences with few benefits in using the technique for predictive modelling. Recognizing the value of the technique for establishing information systems controls, Baskerville (1991) feels that its predictiveness is of less value while its real usefulness lies in it being an effective communication

tool, especially between security and management professionals. Interestingly, Baskerville's earlier work in designing information systems security was highly structured and mechanistic (see Baskerville, 1988). In recent years he has shown an increased tendency towards interpretivism, especially in the area of risk analysis. More recently, Straub & Welke (1998) adopt an interpretive research mode to develop managerial guidelines for coping with system risks. Although Straub & Welke (1998) recommend the use of an earlier generation of tools and techniques such as Courtney's (1977) risk assessment, they position their use within the broad scope of an organization and suggest merging the earlier approaches with the 'threat tree analysis'. Rather than focus on exact probabilities, the threat tree analysis looks for semantic matches of terms specifying degrees of risk.

Other research directions have considered the usefulness of traditional interpretive social theories in understanding the security issues. Examples are found in the work of Dobson (1991) and Strens & Dobson (1993). Their main concern is to provide explanations in terms of roles (of people), actions, goals and policies. In doing so they have used Searle's (1969) speech act theory to specify organizational security requirements. Backhouse & Dhillon (1996) have also considered information systems security from an interpretivist viewpoint. They correlate security concerns with organizational communication and intentional acts of agents involved, and security is regarded as an outcome of communication breakdowns. They draw upon semiotics, the theory of signs, to interpret the security implications of organizational actions. Researchers in other fields have also begun to consider organizations as social forms with patterned, ritualized and conventionalized interactions (e.g. Manning, 1992).

An interpretivist understanding of information systems security concerns certainly offers advantages, furnishing a holistic view of the problem domain, especially within the scope of networked organizational forms, instead of the simplistic, one-dimensional, explanation, more suitable for hierarchically structured organizations. At the same time interpretive approaches lack any prescriptive component and therefore offer value to a security manager. Moreover the explanations come enshrouded in complexity, largely because of the sophisticated sociological and philosophical bases, and as a result the audience for such security approaches remains just a small group of academic researchers.

Research orientations in the radical humanist paradigm

Information systems and security researchers within the radical humanist paradigm aspire to the liberation of managerial consciousness from cognitive domination. Radical humanists believe that the primary goal should be to divert management away from developing hierarchical and technological superstructures and towards harnessing the competence of people. Hence approaches within this paradigm focus neither on technology nor on rational models, but on an emancipated body corporate.

Information systems literature

Traditionally the notions of emancipation and of computer-based systems have been at odds with each other. Computer-based systems are usually considered as a means of managerial

and social control (Huber, 1982). They increase the domination of instrumental reason and, therefore, are deemed to create a social 'iron cage'. Emancipation, by contrast, aims to free the human being from all sorts of restraints (legal, social, political, intellectual or moral).

Within the radical humanist paradigm, researches are few and far between. A mere handful of authors (e.g. Lyytinen & Hirschheim, 1989; Nissen, 1989; Ngwenyama & Lee, 1997) have used concepts rooted in this paradigm. Lyytinen & Hirschheim (1989) adopt Habermas' social action theory to understand and describe information systems. Accordingly 'information system development and use is seen as manifestations of social action, and are always socially determined and conditioned' (p. 117). They conclude that computer-based systems and emancipation are not necessarily antithetical, only paradoxical. In fact Lyytinen & Hirschheim (1989) assert that computer-based systems can promote physical and organizational emancipation by establishing new discursive processes. They can, moreover, promote physical, psychological and organizational emancipation by debating all system related changes.

A slightly different stance is taken by Nissen (1989). Using Habermas's concepts he focuses on developing responsible human action. The basic premise of this work posits that any computer-based system 'intends to influence how people act' (p. 99). And 'whoever wants to work with information systems development and to act responsibly has to develop information systems which encourage and facilitate responsible human action by all the people affected' (p. 99).

A synthesis of emancipatory approaches for analysis, design and management of information systems is provided by Hirschheim & Klein (1989) who contend that if computer-based systems development proceeds in a radical humanist tradition, then there would be three knowledge interests in mind:

> Systems would have features to support the technical knowledge interest and these would be similar to those developed under the functionalist influence. Other features would support the creation of shared meanings and reflect the knowledge interest in mutual understanding. This is similar to systems inspired by social relativism. Finally there would be a comprehensive set of features to support emancipatory discourse. This means that information systems are developed that facilitate the widest possible debate of organizational problems such that truly shared objectives could be agreed upon as policies for achieving them (p. 1208).

Security literature

As with mainstream information systems research, few security approaches espouse radical humanist principles. Prominent among them are the ideas forcefully expounded by Angell (1994; 2000), who, discussing the impact of globalization on today's businesses, takes a radical stance on the implications for the security of information systems. He criticizes the functionalist perspective on the grounds that logic, rationality and technology are the vehicles of cognitive dominance that lead to the alienation of humans, which in turn becomes a barrier

to the achievement of full humanity. He criticizes the functionalist approaches to security on the basis of 'sheer complexity', 'profound uncertainty' and 'linear thinking', especially on the part of security managers (Angell, 1993; 1996). Underpinning this criticism is his concern with the 'pathology of consciousness', in which humans see themselves trapped within a mode of social organization that is created and supported in their everyday lives. Angell appears to be influenced by anarchism. Sociologists have classified such viewpoints as 'anarchistic individualism'. Anarchistic individualism is not a unified intellectual movement. It represents a perspective that advocates total individual freedom without any restrictions of external or internal regulation.

Webler *et al*. (1992) may also be categorized as radical humanist in nature. They use critical theory concepts to locate the activities of risk identification and risk assessment in the context of a social theory and offer normative guidance for correcting the deficiencies inherently associated with these activities. Webler *et al*. (1992) adopt Habermas's concepts of 'communicative rationality' and the 'ideal speech situation' and argue that these have 'immediate ramifications of risk communication' (p. 23).

On the one hand, it seems that the emancipatory approach to developing information systems and managing security hold great promise. On the other hand, an emancipated employee of an organization may lose interest in the core business, introducing significant risks. Thus, although the cognitive domination aspects of radical humanism are appreciated, the implementation strategies largely remain vague and unclear.

Research orientations in the radical structuralist paradigm

Radical structuralists believe that the business environment, social organization and computer-based superstructures are locked into a dynamic process of dialectical materialism. Organizations are seen not as monolithic structures with singularity of purpose and direction, but instead as loosely coupled coalitions with conflicting interest groups. It is assumed that the various groups are in discordance with each other, but order can be restored through negotiation.

Information systems literature

In developing systems grounded in the radical structuralist paradigm, designers tend to take sides with the end users in the organization. They presume a conflict of interest between the top management and the users and that system development can intervene in order to resolve discordance. The conflicts may centre around prestige, power or resources. Therefore, the system development process is seen as a catalyst in resolving problems primarily through participation – biased towards the end users. Systems developed with such an emphasis promote enhancement of craftsmanship and the working conditions.

Pioneering work by Ciborra on the contractual view of information systems falls into this paradigm. His focus is on interaction or bargaining between individuals both within an organization and within the environment (Ciborra, 1987). Ciborra therefore believes that conflicts

in organizations can be exposed and then negotiated and those affected by the situation can be actively involved. As a consequence, competitive advantage with respect to computer-based systems can be achieved not by developing top-level policies and strategies, but by 'tinkering at the grassroots of the organization' (Ciborra, 1991; 1994).

There are a number of success stories that support the radical structuralist viewpoint. Typical examples are the ECONOMOST (Clemons & Row, 1991) and SABRE (Hopper, 1990) systems. In both cases competitive advantage was created by the end users, not by top management. Counter to popular management theories, systems such as these were derived from experimentation at the bottom rungs of the organization (Clemons & Row, 1988; Hopper, 1990; Venkataraman & Short, 1990).

In spite of success stories grounded in the radical structuralist viewpoints, much criticism exists about the basic assumptions. One could argue that not all problem situations may be viewed as potential conflicts: in many instances the core ideal may be co-operation. Others have noted that new technology creates demarcation disputes among different stakeholders (see for example Ehn, 1988), and this runs counter to the basic premise of radical structuralists.

Security literature

Information systems security researchers have rarely exploited concepts from the radical structuralists, although earlier work carried out by Lane (1985) shows some inclination towards this paradigm. This resemblance is merely superficial, as Lane's work represents an assemblage of loosely coupled ideas. Different facets of his work bear comparison not only with the work of radical structuralists, but also with that of interpretivists and functionalists as well.

It is, however, interesting to note that Lane's work was primarily inspired by risk analysis. Lane considers the behaviour of people to be a major factor in security. He argues that not only should it be the first factor to receive attention, but also be a key component of the risk-analysis process. He proposes that in an organization, staff with special risk responsibility should be designated, in order to reduce risks in computer-based systems. Further he suggests the division of responsibility and the division of knowledge about the system amongst many personnel. Lane's concepts show a slight departure from the underlying principles of other approaches but he has been unable to show how his 'psychological model of human action' can perceive 'social causality'.

SUMMARY AND DISCUSSION

This section synthesizes the discussion so far. The preconceptions and dispositions of researchers are considered with respect to information systems and security. The paradigmatic orientation and preponderance of particular kinds of research is identified. Finally

comments are made about the systematic position of future research in light of the Burrell and Morgan framework.

With respect to information systems researchers, there is a growing disillusionment with the formal, rational and overly mechanical conception in the analysis and design of information systems. Although this narrow technical viewpoint, common to most functionalist thinking, may have been necessary when computer service provision was confined to a single function and when organizations were predominantly organized as a hierarchy, with the move towards a more networked form and with computers permeating all aspects of business, the importance of social aspects of systems analysis and design is being recognized. There is also increasing realization that computer-based systems dynamically interact with the formal and informal environments in which they are used. Hence an understanding of human interactions, patterns of behaviour and meanings associated with the actions of individuals becomes important. In recent years, the narrow conceptions of traditional functionalism have been a subject of debate and there have been efforts within sociological theory to expand its scope – in particular the emergence of neofunctionalism (for a fuller discussion see Alexander, 1985). Trends can also be observed in other information systems related areas, where more consideration is being given to the 'softer' issues. A harbinger of things to come could be the emergence of 'soft OR' (see Forrester, 1994; Lane, 1994) which has shifted operations research away from its traditional engineering preconceptions.

By contrast to mainstream information systems work, the majority of the information systems security research tends to focus on formalized rule structures in designing security. Although important, exclusive reliance on formalized structures is not sufficient when designing security. The earliest risk analysis (e.g. Courtney, 1977) and security evaluation approaches (e.g. Bell & La Padula, 1976) and the more recent security evaluation and design methods are founded on functionalist conceptions, most being influenced by systems theory. The emphasis has been to apply 'valid and complete' models to the commercial environment. While the value of such methods, tools and techniques is evident, their focus is rather limited, restricting security to an extremely narrow perspective – predominantly as managing access control. But as Dhillon (2001) notes about the Bell and La Padula models 'validity exists not because of completeness of their internal workings and their derivations through axioms, but because the reality they are modelling is well defined, i.e. the military organization'. The concern, therefore, has been on maintaining a security perimeter around information processing activities. Although such concepts work well when organizational structures are hierarchical and information processing largely centralized, problems arise when organizational structures become flatter and more organism-like in their nature. When this happens, a broader vision for addressing security concerns is needed which address social groupings and the behaviour of people.

Along with recognizing the significance of social issues, an increasing number of researchers have begun to explore alternative philosophical viewpoints. The review of various approaches in the previous sections has identified information systems and security research associated with the interpretive, radical humanist and radical structuralist paradigms. In terms of the use

Table 1. Summary of information systems and security research

Paradigm	Theories used	Information systems methods and seminal work	Security methods and seminal work
Functionalist	System theory; Contingency theory	IS success (Ives *et al*., 1983); Requirement identification (Bailey & Pearson, 1983; Davis & Olson, 1984; Baroudi *et al*., 1986), Systems development (DeMarco, 1978)	Traditional risk analysis approaches (Courtney, 1977; Parker, 1981; Fisher, 1984); Security evaluation methods (Bell & La Padula, 1976; Van Der Veen *et al*., 1994)
Interpretive	Structuration theory; Phenomenology and Hermeneutics; Semiotics; Contextualism	Information systems strategy, system design and implementation (Boland, 1985; Walsham, 1993) Use of signs in system specification (Liebenau & Backhouse, 1990)	Risk analysis and the communicative content (Baskerville, 1991); Speech act theory and security development (Dobson, 1991); Pragmatic considerations and security (Backhouse & Dhillon, 1996)
Radical Humanist	Critical theory; Anarchistic individualism	Theory of information systems and system specification (Lyytinen & Klein, 1985)	Strategic options for security as described by Angell (1994); Critical theoretic considerations in risk analysis (Webler *et al*., 1992)
Radical Structuralist	Conflict theory	Contractual view of information systems (Ciborra, 1987)	Not found (except some resemblance of Lane's 1985 work)

of social theories, there has been an extensive reliance on phenomenology, hermeneutics, critical theory and conflict theory. Table 1 summarizes the literature in information systems and security in terms of paradigmatic orientation, relevant theory and seminal work.

The point of undertaking an extensive review of information systems and security literature is to identify gaps and problematic areas with respect to information systems security theories and approaches. This establishes the systematic position for future research. In taking forward the theory building exercise, we adopt the viewpoint and process recommended by Burrell & Morgan (1979):

> Theorists who wish to develop ideas . . . cannot afford to take a short cut. There is a real need for them to ground their perspective in the philosophical traditions from which it derives; to start from first principles; to have the philosophical and sociological concerns by which the paradigm is defined at the forefront of their analysis; to develop a systematic and coherent perspective within the guidelines which each paradigm offers, rather than taking the tenets of a competing paradigm as critical points of reference. Each paradigm needs to be developed in its own terms (p. 397).

In essence, our aim is not to build on criticisms of research grounded in other paradigms and thereby be involved in 'academic demolition': we appreciate the usefulness of many of

the approaches, but retain the right to qualify it. For example, risk analysis, rooted in the functionalist paradigm, is extremely useful for evaluating security, but it cannot form the basis of an entire security strategy. Likewise traditional evaluation methods can be useful in assessing the extent of security, but a corporate strategy to prevent the occurrence of negative events cannot be based on the highly structured security evaluation criteria.

This review of literature and the related discussions presented in the previous sections suggests that a socio-organizational perspective is the way forward if security of information systems is to be achieved. This perspective is grounded in the interpretive paradigm as defined by Burrell and Morgan and can be justified in terms of the ontological status of the subject being studied and the nature of the models used as a basis of analysis.

With respect to the ontological status of security, it is worth reflecting on the underlying beliefs presented in the sections so far. Most security research has been classified under the functionalist paradigm and the theorists have treated security as something tangible and concrete. This may have been appropriate in the context of a strict hierarchy or military organization. As the context of use for traditional security measures has evolved, it is rather difficult to develop objective views of reality and be able to consider information systems and organizations as concrete entities. However, if information system security continues to be viewed in a mechanistic manner, the inter- and intraorganizational social relationships would be considered as incidental. Clearly, as has been suggested in the previous sections, understanding human-centred controls is an important component for maintaining information system security (also see Hitchings, 1994; 1996 and Dhillon, 2001). It, therefore, follows that security should not be seen as a means of protecting something tangible and hard. Indeed a majority of the negative events, for which reason security exists, cannot be viewed as discrete events. The prevention of such events therefore means more than just 'locks and keys' and must relate to the social groupings and behaviour.

When considering the nature of models used for review and analysis of information security, the primary problem relates to the context of use. As noted, most current models and frameworks have been developed for either the military organization or hierarchically structured enterprises. The US Department of Defense, for example, has been using the Trusted Computer System Evaluation Criteria for years. The criteria are certainly valid and complete when the context of use is the military organization. Similarly, the Bell La Padula and Denning Models of confidentiality and access control are valid and complete for the domains they were developed for. One of the major assumptions in these models, and the military to a large extent, is the predominant culture of trust among its members and a system of clear roles and responsibilities. The review of approaches presented earlier in this paper positions most security models and frameworks within the functionalist paradigm. Perhaps it was an adequate means to design security using these models when applications were often in the military sector. However, in the current information age, there is clearly a challenge in managing security using the conventional approaches. An understanding and review of such challenges will define the scope of future research.

CONCLUSION

The contribution of this paper is twofold. First, it presents the current research directions in studying information systems and security. It identifies a trend in information systems research moving away from a narrow technical viewpoint. With respect to information systems security, the literature review identifies the dominance of technical and functionalist preconceptions, essentially because most methods have been grounded in a particular well-defined reality, i.e. that of the military. There have only been a few isolated attempts to break away from this focused vision. The critique of the current approaches lays the foundation for a socio-organizational perspective in dealing with security issues and in setting an agenda for future work. This standpoint is systematically classified to be within the interpretive paradigm of Burrell and Morgan.

Second, the concepts presented in this paper are justified by recognizing that the use of a socio-organizational perspective for understanding information systems security is still at a theory-building stage. Save Straub & Welke's (1998) action research to develop risk management guidelines, the literature search for this research found few examples of a socio-organizational perspective for evaluating information systems security, pointing to a greater need for more empirical research to develop key principles for the prevention of negative events and therefore to help in the management of security. In a nutshell, here lies the nature and scope of our future research emphasis.

REFERENCES

Adam, N.R. & Wortmann, J.C. (1989) Security-control methods for statistical databases: a comparative study. *ACM Computing Surveys*, **21**, 4.

Alexander, J., ed. (1985) *Neofunctionlism*. Sage Publications. Beverly Hills, CA.

Alter, S. (1992) Why persist with DSS when the real issue is improving decision making? In: *Decision Support Systems: Experiences and Expectations*, Jelassi, T. *et al*. (eds), pp. 1–11. Elsevier Science Publishers, Amsterdam.

Andersen, P.B. (1990) A semiotic approach to construction and assessment of computer systems. *Proceedings of the IFIP TC8/WG8.2 Conference on Information Systems Research Arena of the 90s*. Copenhagen, Denmark, pp. 465–514.

Anderson, A.M. *et al*. (1993) The risk data repository: a novel approach to security risk modeling. *Proceedings of the Ninth IFIP International Symposium on Computer Security, IFIP/Sec '93, Deerhurst*. Ontario, Canada, pp. 179–188.

Angell, I.O. (1993) Computer security in these uncertain times: the need for a new approach. *Proceedings of the Tenth World Conference on Computer Security, Audit and Control, COMPSEC*. London, UK, pp. 382–388.

Angell, I.O. (1994) The impact of globalization on today's business, and why Information System Security is strategic, *Proceedings of The 1994 Annual Congress of the European Security Forum*, Cologne, Germany.

Angell, I.O. (1995) Winners and losers in the information age. *LSE Magazine*, **7**, 10–12.

Angell, I.O. (1996) Economic crime: beyond good and evil. *Journal of Financial Regulation and Compliance*, **4**, 1.

Angell, I.O. (2000) *The New Barbarian Manifesto: How to Survive the Information Age?* Kogan Page, London.

Backhouse, J. (1991) The use of semantic analysis in the development of information systems. Unpublished PhD, London School of Economics, University of London, London.

Backhouse, J. & Dhillon, G. (1996) Structures of responsibility and security of information systems. *European Journal of Information Systems*, **5**, 2–9.

Badenhorst, K. & Eloff, J. (1990) Computer security methodology: risk analysis and project definition. *Computers and Security*, **9**, 339–346.

Bailey, J. & Pearson, S. (1983) Development of a tool for measuring and analyzing computer user satisfaction. *Management Science*, **29**, 530–545.

Bardach, E. (1977) *The Implementation Game*. MIT Press, Cambridge, MA.

Baroudi, J.J. *et al*. (1986) An empirical study of the impact of user involvement on system usage and information satisfaction. *Communications of the ACM*, **29**, 3.

Baskerville, R. (1988) *Designing Information Systems Security*. John Wiley & Sons, New York.

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

Baskerville, R. (1993) Information systems security design methods: implications for information systems development. *ACM Computing Surveys*, **25**, 375–414.

Beck, U. (1992) *Risk Society*. Sage Publications, London.

Bell, D. & La Padula. (1976) *Secure Computer Systems: Unified Exposition and Multics Interpretation*. MITRE Corp., Bedford, UK.

Benbasat, I. *et al*. (1984) A critique of the stage hypothesis: theory and empirical evidence. *Communications of the ACM*, **May**, 467–485.

Benjamin, R.I. *et al*. (1984) Information technology: a strategic opportunity. *Sloan Management Review*, **Spring**.

Bequai, A. (1987) *Technocrimes – the Computerization of Crime and Terrorism*. Lexington Books, Cambridge, MA.

Birch, D. & McEvoy, N. (1992) Risk analysis for information systems. *Journal of Information Technology*, **7**, 44–53.

Bloomfield, B. & Coombs, R. (1992) Information technology, control and power: the centralization and decentralization debate revisited. *Journal of Management Studies*, **29**, 459–484.

Boland, R.J.J. (1985) Phenomenology: a preferred approach to research on information systems. In: *Research Methods in Information Systems*, Mumford, E., *et al*. (eds), pp. 193–201. Elsevier Science Publishers, Amsterdam.

Boland, R. (1986) Fantasies of information. *Advances in Public Interest Accounting*, **1**, 49–65.

Boland, R.J. & Day, W.F. (1989) The experience of system design: a hermeneutic of organizational action. *Scandinavian Journal of Management*, **5**, 87–104.

Boockholdt, J.L. (1987) Security and integrity controls for microcomputers: a summary analysis. *Information and Management*, **13**, 33–41.

Browne, P. (1979) *Security: Checklist for Computer Center Self Audits*. AFIPS Press, Arlington, VA.

Buchanan, J. & Linowes, R. (1980) Understanding distributed data processing. *Harvard Business Review*, **July/Aug.**, 143–153.

Burrell, G. & Morgan, G. (1979) *Sociological Paradigms and Organizational Analysis*. Heinemann, London.

Chokhani, S. (1992) Trusted products evaluation. *Communications of ACM*, **35**, 66–76.

Chua, W. (1986) Radical developments in accounting thought. *Accounting Review*, **61**, 601–632.

Ciborra, C.U. (1987) Research agenda for a transaction cost approach to information systems. In: *Critical Issues in Information Systems Research*, Boland, R.J. & Hirschheim, R.A. (eds). John Wiley & Sons, Chichester, UK.

Ciborra, C. (1991) From thinking to tinkering: the grass roots of strategic information systems. *Proceedings of the Twelfth International Conference on Information Systems*, New York.

Ciborra, C. (1994) The grass roots of IT and strategy. In: *Strategic Information Systems. A European Perspective*, Ciborra C. & Jelassi, T. (eds), pp. 3–24. John Wiley, Chichester, UK.

Clements, D.P. (1977) Fuzzy ratings for computer security evaluation. Unpublished PhD Thesis, University of California, Berkeley.

Clemons, E. & Row, M. (1988) A strategic information system: McKesson drug company's ECONOMOST. *Planning Review*, **16**, 14–19.

Clemons, E.K. & Row, M.C. (1991) McKesson Drug Company: a case of ECONOMOST, a strategic information system. *Journal of Management Information Systems*, **5**, 36–50.

Computer Security Consultants (1988) *Using Decision Analysis to Estimate Computer Security Risk*. Computer Security Consultants, Ridgefield, CI.

Courtney, R. (1977) Security risk analysis in electronic data processing. *Proceedings of the AFIPS Conference Proceedings NCC*. pp. 97–104.

Davis, G.B. & Olson, M.H. (1984) *Management Information Systems: Conceptual Foundations, Structures and Development*. McGraw-Hill, New York.

DeMarco, T. (1978) *Structured Analysis and System Specification*. Yourdon Press, New York.

Dhillon, G. (2001) Challenges in managing information security in the new millennium. In: *Information Security Management: Global Challenges in the New Millennium*, Dhillon, G. (ed.). Idea Group, Hershey.

Dhillon, G. & Backhouse, J. (1996) Risks in the use of information technology within organizations. *International Journal of Information Management*, **16**, 65–74.

Dobson, J. (1991) A methodology for analyzing human and computer-related issues in secure systems. In: *Computer Security and Information Integrity*, Dittrich, K., *et al*. (eds), pp. 151–170. Elsevier Science Publishers. Amsterdam,.

Dobson, J.E. *et al*. (1991) Determining requirements for CSCW: the ORDIT approach. In: *Collaborative Work, Social Communications and Information Systems*, Stamper, R.K., *et al*. (eds), pp. 333–353. Elsevier Science Publishers, Amsterdam.

Ehn, P. (1988) *Work Oriented Design of Computer Artifacts*. Arbetslivs-centrum, Stockholm.

Fincham, R. (1992) Perspectives on power: processual, institutional and 'internal' forms of organizational power. *Journal of Management Studies*, **29**, 741–759.

Fisher, R. (1984) *Information Systems Security*. Prentice Hall, Englewood Cliffs, NJ.

Flanagan, W.G. & McMenamin, B. (1992) The playground bullies are learning how to type. *Forbes*, **Feb.**, 184–189.

Forrester, J.W. (1994) System dynamics, systems thinking, and soft OR. *System Dynamics Review*, **10**, 245–256.

Gable, G.G. (1994) Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems*, **3**, 112–126.

Gallegos, F. *et al*. (1987) *Audit and Control of Information Systems*. South-Western, Cincinnati.

Galliers, R. & Sutherland, A. (1991) Information systems management and strategy formulation: 'the stages of growth' model revisited. *Journal of Information Systems*, **1**, 89–114.

Garfinkel, S. (2000) *Database Nation: The Death of Privacy in the 21st Century*. O'Reily & Associates.

Giddens, A. (1984) *The Constitution of Society*. Polity Press. Cambridge, UK.

Griethuysen, V., ed. (1982) *Concepts and Terminology of the Conceptual Schema and the Information Base*, ISO Report No ISO TC97 SC5 N695.

Gutting, G., ed. (1980) *Paradigms and Revolutions*. University of Notre Dame Press, South Bend.

Highland, H. (1985) Microcomputer security: data protection techniques. *Computers and Security*, **4**, 517–531.

Hirschheim, R. & Klein, H.K. (1989) Four paradigms of information systems development. *Communications of the ACM*, **32**, 1199–1215.

Hitchings, J. (1994) The need for a new approach to information security. *Proceedings of the 10th International Conference on Information Security (IFIP Sec '94)*, Curacao, NA.

Hitchings, J. (1996) A practical solution to the complex human issues of information security design. In: *Information Systems Security: Facing the Information Society of the 21st Century*. Katsikas S.K. & Gritzalis, D. (eds), pp. 3–12. Chapman & Hall, London.

Hoffman, J. *et al*. (1978) SECURATE – Security evaluation and analysis using fuzzy metrics. *Proceedings of the AFIPS National Conference Proceedings*, pp. 531–540.

Hopper, M. (1990) Rattling SABRE – new ways to compete on information. *Harvard Business Review*, **68**, 118–125.

Hopper, T. & Powell, A. (1985) Making sense of research into the organizational and social aspects of management accounting: a review of its underlying assumptions. *Journal of Management Studies*, **22**, 429–465.

Hoyt, D. (1973) *Computer Security Handbook*. Macmillan, New York.

Hsiao, D. *et al*. (1979) *Computer Security*. Academic Press, New York.

Huber, G.P. (1982) Organizational information systems: determinants of their performance and behavior. *Management Science*, **28**, 567–577.

Hutt, A. *et al*., eds (1988) *Computer Security Handbook,* 2nd edn. Macmillan, New York.

IBM. (1972) *Secure automated facilities environment study 3, Part 2*. IBM, Armonk, NY.

Ives, B. *et al*. (1983) The measurement of user information satisfaction. *Communications of the ACM*, **26**, 785–793.

Jackson, N. & Carter, P. (1991) In defense of paradigm incommensurability. *Organization Studies*, **12**, 109.

James, H. (1996) Managing information systems security: a soft approach. *Proceedings of the Information Systems Conference of New Zealand.*

Jönsson, S. & Macintosh, N.B. (1997) CATS, RATS, and EARS: making the case for ethnographic accounting research. *Accounting, Organizations and Society*, **22**, 367–386.

Kailay, M. & Jarratt, P. (1994) RAMeX: a prototype expert system for computer security risk analysis and management. *Proceedings of the Tenth IFIP International Symposium on Computer Security, IFIP Sec 94*.

Keen, P.G. (1981) Information systems and organizational change. *Communications of the ACM*, **24**, 24–33.

Keeney, R.L. (1992) *Value-Focused Thinking*. Harvard University Press, Cambridge, MA.

Kendall, J.E. & Kendall, K.E. (1993) Metaphors and methodologies: living beyond the systems machine. *MIS Quarterly*, **17**, 149–171.

Kendall, J.E. & Kendall, K.E. (1994) Metaphors and their meaning for information systems development. *European Journal of Information Systems*, **3**, 37–47.

Klein, H., Lyytinen, K. (1985) The poverty of scientism in information systems. In: *Research Methods in Information Systems*, Mumford, E., *et al*. (eds), pp. 131–161. Elsevier Science Publishers, Amsterdam,

Kling, R. (1980) Social analysis of computing: theoretical perspectives in recent empirical research. *ACM Computing Surveys*, **12**, 61–110.

Kling, R. (1987) Defining the boundaries of computing across complex organizations. In: *Critical Issues in Information Systems Research*, Boland, R.J. & Hirschheim, R.A. (eds). John Wiley & Sons, New York.

Kling, R. (1991) Computerization and social transformation. *Science, Technology and Human Values*, **16**, 342–367.

Kling, R. & Scacchi, W. (1982) The web of computing: computer technology as social organization. *Advances in Computers*, **21**, 1–90.

Krauss, L. (1972) *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems*. Amacon, New York.

Krauss, L. (1980) *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems*, Revised ed., Amacon, New York.

Krueger, K.H. (1993) Internal controls by objectives: the functional control by objectives. *Proceedings of the IFIP/Sec "93, Computer Security: Discovering Tomorrow, Deerhurst*. Ontario, Canada, pp. 151–164.

Lane, V.P. (1985) *Security of Computer Based Information Systems*. Macmillan, London.

Lane, D.C. (1994) With a little help from our friends: how system dynamics and soft OR can learn from each other. *System Dynamics Review*, **10**, 101–134.

Lee, A.S. (1991) Integrating positivist and interpretive approaches to organizational research. *Organization Science*, **2**, 342–365.

Lee, H. & Liebenau, J. (1996) In what way are information systems social systems? A critique from sociology. *Proceedings of the First UK Academy for Information Systems Conference,* Cranfield School of Management, Cranfield, Bedford.

Lehtinen, E. & Lyytinen, K. (1986) Action based model of information system. *Information Systems*, **11**, 299–317.

Leifer, R. *et al*. (1994) Deep structures: real information requirements determination. *Information and Management*, **27**, 275–285.

Liebenau, J. & Backhouse, J. (1990) *Understanding Information*. Macmillan, London.

Loch, K.D. *et al*. (1992) Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, **June**, 173–186.

Longley, D. (1991) Formal methods of secure systems. In: *Information Security Handbook*, Caelli, W., *et al*. (eds), pp. 707–798. Stockton Press, New York.

Lucas, H. (1981) *Implementation: the Key to Successful Information Systems*. Columbia University Press, New York.

Lyytinen, K.J. & Klein, H.K. (1985) The critical theory of Jurgen Habermas as a basis for a theory of information systems. *Proceedings of the Research Methods in Information Systems,* Amsterdam, pp. 219–236.

Lyytinen, K. & Hirschheim, R. (1989) Information systems and emancipation. Promise or threat. In: *Systems Development for Human Progress*, Klein H.K. & Kumar, K. (eds), pp. 115–139. Elsevier Science Publishers B.V., Amsterdam.

Madon, S. (1991) The impact of computer-based information systems on rural development: a case study in India. Unpublished PhD, University of London, London.

Manning, P. (1992) *Organizational Communication*. Aldine de Gruyter, New York.

Markus, M.L. (1983) Power, politics and MIS implementation. *Communications of the ACM*, **26**, 430–444.

Mathews, K.M. *et al*. (1999) The problem of prediction and control in theoretical diversity and the promise of the complexity sciences. *Journal of Management Inquiry*, **8**, 17–31.

McFarlan, F. *et al*. (1983) The information archipelago – plotting a course. *Harvard Business Review*, **83**, 145–156.

McLeen, J. (1990) Specification and modeling of computer security. *Computer*, **23**, 9–16.

McMenamin, S. & Palmer, J. (1984) *Essential System Analysis*. Yourdon Press, New York.

Melone, N.P. (1990) A theoretical assessment of the user-satisfaction construct in information systems research. *Management Science*, **36**, 76–91.

Merten, A. *et al*. (1982) Putting information assets on a balance sheet. *Risk Management*, **Jan**.

Mintzberg, H. (1983) *Structures in Fives: Designing Effective Organizations*. Prentice Hall, Englewood Cliffs, NJ.

Mumford, E. & Weir, M. (1979) *Computer Systems in Work Design: the ETHICS Method*. John Wiley & Sons, New York.

Murray, F. (1989) The organizational politics of information technology: studies from the UK financial services industry. *Technology Analysis and Strategic Management*, **1**, 285–298.

Ngwenyama, O.K. & Lee, A.S. (1997) Communication richness in electronic mail: Critical Social Theory and contextuality of meaning. *MIS Quarterly*, **21**, 145–167.

Nissen, H.-E. (1989) Information systems development for responsible human action. In: *Systems Development for Human Progress*, Klein H.K. & Kumar, K. (eds), pp. 99–255. Elsevier Science Publishers B.V., Amsterdam.

Nolan, R. (1979) Managing the crises in data processing. *Harvard Business Review*, **57**, 115–126.

Norman, A. (1983). *Computer Insecurity*. Chapman & Hall, London.

Orlikowski, W.J. & Baroudi, J.J. (1991) Studying information technology in organisations: research approaches and assumptions. *Information Systems Research*, **2**, 1–28.

Orton, J.D. (1994) Reorganizing: an analysis of the 1976 reorganization of the US intelligence community. Unpublished PhD, University of Michigan, Ann Arbor.

Orton, J.D. & Weick, K.E. (1990) Loosely coupled systems: a reconceptualization. *Academy of Management Review*, **15**, 203–223.

Parker, D. (1981) *Computer Security Management*. Reston Publishing, Reston.

Parsons, G.L. (1983) *Fitting information systems technology to the corporate needs: the linking strategy* (Teaching Notes 9-183-176). Harvard Business School, Harvard.

Pettigrew, A.M. (1985) Contextualist research and the study of organizational change processes. *Proceedings of the Research Methods in Information Systems*, Manchester, UK.

Porter, M. (1980) *Competitive Strategy*. Free Press, New York.

Porter, M. & Millar, V. (1985) How information gives you competitive advantage. *Harvard Business Review*, **63**, 149–161.

Quinn, B. *et al*. (1988) *The Strategy Process – Concepts, Contexts and Cases*. Prentice Hall, Englewood Cliffs, NJ.

Rawnsley, J. (1995) *Going for broke: Nick Leeson and the collapse of Barings Bank*. Harper Collins.

Reason, P. & Rowan, J. (1981) *Human Inquiry: a Sourcebook of New Paradigm Research*. Wiley, Chichester.

Ritzer, G. (1992) *Sociological Theory*. McGraw-Hill, New York.

Roach, T.W. (1992) Effective systems development in complex organizations: a field study of systems development and use in the United States Army Medical Department (Army Medical Department). Unpublished PhD, University of Texas at Austin, Austin, TX.

Saltmarsh, T. & Browne, P. (1983) Data processing – risk assessment. In: *Advances in Computer Security Management, Vol. 2*, Wofsey, M. (ed.), pp. 93–116. John Wiley & Sons, Chichester.

Schultze, U. (1998) Investigating the contradictions in Knowledge Management. *Proceedings of the IFIP WG8.2 & WG8.6 Joint Working Conference on Information Systems: Current Issues and Future Changes*. Helsinki, Finland, pp. 155–174.

Schwartz, M. (1990) Computer security: planning to protect corporate assets. *Journal of Business Strategy*, **11**, 38–41.

Searle, J.R. (1969) *Speech Acts: an Essay in the Philosophy of Language*. Cambridge University Press, New York.

Silverman, D. (1970) *The Theory of Organizations*. Heinemann, London.

Silverman, D. & Jones, J. (1973) Getting in: the managed accomplishments of 'correct" selection outcomes. In: *Man and Organization*, Child, J. (ed.). George Allen & Unwin, London.

Silverman, D. & Jones, J. (1976) *Organizational Work: the Language of Grading/the Grading of Language*. Collier/Macmillan, London.

Siponen, M.T. (2001) An analysis of the recent IS security development approaches: descriptive and prescriptive implications, In: *Information Security Management: Global Challenges in the New Millennium*, Dhillon, G. (ed.). Idea Group Publishing, Hershey.

Stamper, R.K. (1973) *Information in Business and Administrative Systems*. John Wiley & Sons, New York.

Stamper, R. (1991) The semiotic framework for information systems research. *Proceedings of the IFIP TC8/WG8.2 Conference on Information Systems Research Arena of the 90s*. Copenhagen, Denmark, pp. 515–527.

Straub, D.W. & Welke, R.J. (1998) Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, **22**, 441–469.

Strens, R. & Dobson, J. (1993) How responsibility modeling leads to security requirements. *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD, pp. 398–408.

Symons, V.J. (1991) A review of information systems evaluation: content, context and process. *European Journal of Information Systems*, **1**, 205–212.

Taylor, F.W. (1911) *Principles of Scientific Management*. Harper & Row, New York.

Turn, R. (1982) Privacy protection in the 80s. *Proceedings of the IEEE Symposium in Security and Privacy*. Silver Springs, MD.

Ulrich, H. (1984) Management – a misunderstood societal function. In: *Self-Organization and Management of*

Social Systems, Ulrich H. & Probst, G.J.B. (eds), pp. 80–93. Springer-Verlag, Berlin.

US Department of Commerce (1979) *Guideline for Automatic Data Processing Risk Analysis (Federal Information Processing Standards Publication FIPS 65)*. US Department of Commerce, National Bureau of Standards, Washington, DC.

Van Der Veen, A.M. *et al*. (1994) SMART: structured multidimensional approach to risk taking for operational information systems. *Proceedings of the Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*.

Venkataraman, N. & Short, J. (1990) Strategies for electronic integration: from order entry to value added partnerships at Baxter, *Sloan School Working Paper*.

Von Solms, R. *et al*. (1993) A process approach to information security management. *Proceedings of the Proceedings of the Ninth IFIP International Symposium on Computer Security, IFIP/Sec '93, Deerhurst*. Ontario, Canada, pp. 365–379.

Walsham, G. (1991) Organizational metaphors and information systems research. *European Journal of Information Systems*, **1**, 83–94.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*. John Wiley & Sons, Chichester, UK.

Walsham, G. (1995) Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, **4**, 74–81.

Walsham, G. *et al*. (1990) Information systems as social systems: implications for developing countries. In: *Information Technology in Developing Countries*, Bhatnagar, S. & Bjorn-Andersen, N. (eds), pp. 51–61. Elsevier Science Publishers B.V., Amsterdam.

Wand, Y. & Weber, R. (1990) Toward a theory of deep structure of information systems. *Proceedings of the International Conference on Information Systems*. Copenhagen, Denmark, pp. 61–71.

Ward, J. & Griffiths, P. (1996) *Strategic Planning for Information Systems*. Wiley, Chichester, UK.

Weber, M. (1947) *The Theory of Social and Economic Organization*. Free Press, Glencoe, Ill.

Weber, R. (1988) *EDP Auditing: Conceptual Foundations and Practice*, 2nd edn. McGraw-Hill, New York.

Webler, T. *et al*. (1992) A critical theoretic look at technical risk analysis. *Industrial Crisis Quarterly*, **6**, 23–38.

Whipp, R. & Pettigrew, A. (1992) Managing change for competitive success: bridging the strategic and the operational. *Industrial and Corporate Change*, **1**, 205–233.

Willcocks, L. & Margetts, H. (1994) Risk assessment and information systems. *European Journal of Information Systems*, **3**, 127–139.

Wiseman, C. (1985) *Strategic Information Systems*. Irwin, Homewood.

Wong, K. (1977) *Risk Analysis and Control*. National Computing Centre, Manchester.

Woodward, J. (1965) *Industrial Organization: Theory and Practice*. Oxford University Press, London.

Wynne, B. & Otway, H.J. (1982) *Information Technology, Power and Managers*. Elsevier Science Publishers, Amsterdam.

Zuboff, S. (1988) *In the Age of the Smart Machine*. Basic Books, New York.

Zyl, P.W.J.V. *et al*. (1994) MOSS II – a model for open system security. *Proceedings of the Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*.

Biographies

Gurpreet Dhillon is currently an assistant professor of MIS at the University of Nevada Las Vegas. His research focuses on the socio-organizational aspects of information use and IS security within organizations. He is a graduate of the London School of Economics.

James Backhouse is a Senior Lecturer of Information Systems and Director of Computer Security Research Centre at the London School of Economics. His research focuses on semantic aspects of information use and IS security.