Business Excellence and Management
Volume 3 Issue 2 / June 2013

A SHORT LITERATURE REVIEW IN INFORMATION SYSTEMS SECURITY MANAGEMENT APPROACHES

Ioannis KOSKOSAS
International Hellenic University, Thessaloniki – Moudania, Greece
ioanniskoskosas@yahoo.com

Abstract
This study provides a short literature review in information systems security (ISS) approaches either technical or non-technical in nature. Although, the benefits and uses of the technical information systems security approaches are valuable, there is still a need to investigate the alternative non-technical approaches or at least, to find a way to combine them in a more appropriate and thus, successful way. In doing so, this paper presents the available methods and techniques in information systems security in an attempt to shed some light into how these alternative approaches could be used in benefit of information systems security.

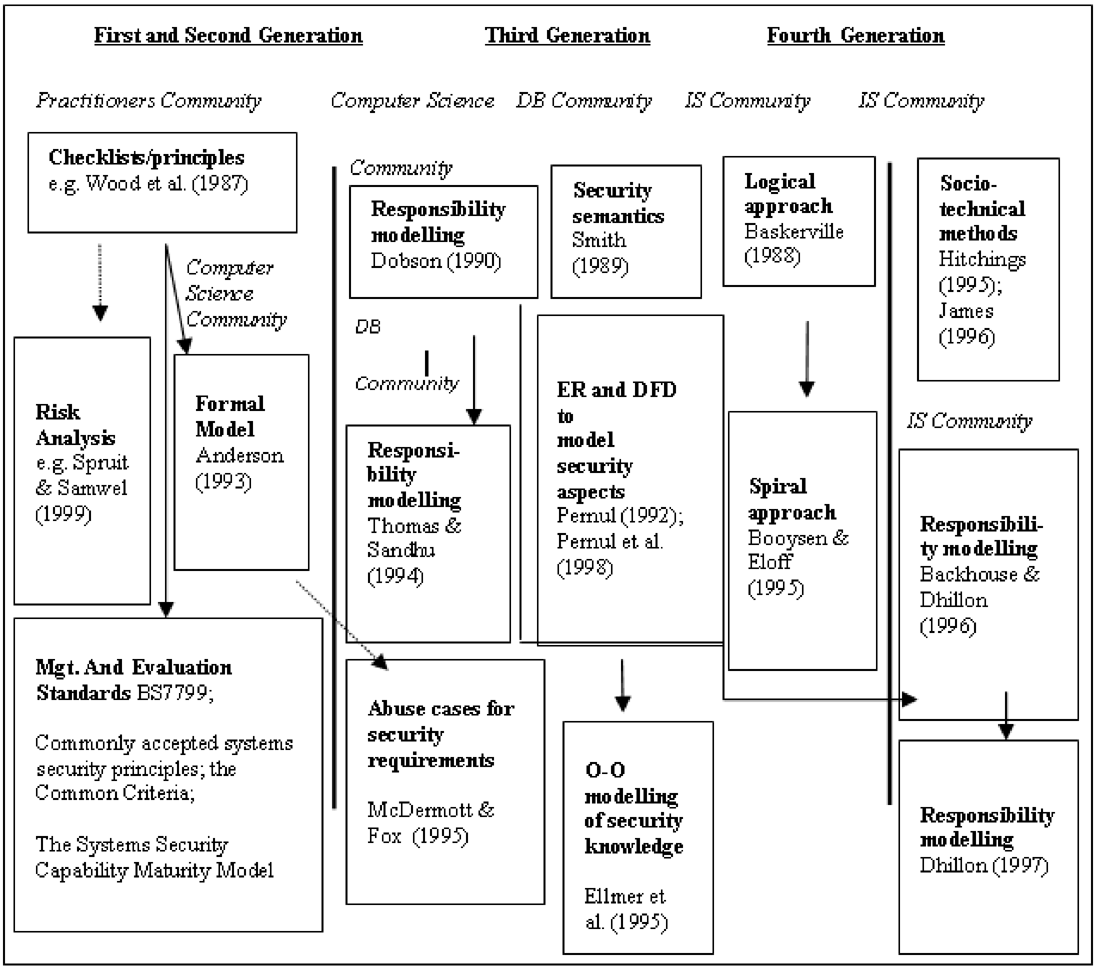
Keywords: Information systems security, Positivistic-interpretivist approaches, Case studies.

1. A BROAD VIEW

Over the years, a number of security approaches have been developed that help in managing IS security and in limiting the chances of an IS security breach. A security breach is an act from outside an organization that bypasses or contravenes security policies, practices and procedures relative to information systems security. The majority of the approaches are presented in Table 1 below. The thick separated lines represent the different generations originally presented by Baskerville (1988). The arrows show influences or inspirations while the broken arrows mean that the approach is influenced by the deficiencies of a certain approach. Traditional approaches such as *Computer Science, Data Modelling, Practitioners Community and IS Community* under which other techniques have been developed are noted by *italics*. For example, responsibility modelling is developed in the Computer Science Community.

First and second generation methods aim at finding out what can be done and actually dominate the principles, checklists, and most standards for secure systems development. Third generation approaches include modelling and fourth generation emphasize socio-technical design. Siponen (2001) supports the view that there have been only a few isolated (less-well known) approaches to consider the socio-technical aspects of information systems security management. The majority of IS security methods entails checklists, risk analysis, and evaluation methods. Although these approaches help in managing security, Siponen (2001) supports the need for IS security approaches to provide a holistic modelling support which can be integrated into modern IS development approaches, and the lack of approaches which focus on socio-organizational roles of IS security.

TABLE 1 – AN OVERVIEW OF APPROACHES FOR SECURE IS DEVELOPMENT


First and Second Generation
Third Generation
Fourth Generation
Practitioners Community
Computer Science Community
DB Community
IS Community
IS Community
Checklists/principles e.g. Wood et al. (1987)
Computer Science Community
Risk Analysis e.g. Spruit & Samwel (1999)
Formal Model Anderson (1993)
Mgt. And Evaluation Standards BS7799;
Commonly accepted systems security principles; the Common Criteria;
The Systems Security Capability Maturity Model
Responsibility modelling Dobson (1990)
DB Community
Responsi-bility modelling Thomas & Sandhu (1994)
Abuse cases for security requirements
McDermott & Fox (1995)
Security semantics Smith (1989)
ER and DFD to model security aspects Pernul (1992); Pernul et al. (1998)
O-O modelling of security knowledge
Ellmer et al. (1995)
Logical approach Baskerville (1988)
Spiral approach Booysen & Eloff (1995)
Socio-technical methods Hitchings (1995); James (1996)
IS Community
Responsibili-ty modelling Backhouse & Dhillon (1996)
Responsibility modelling Dhillon (1997)

Source: Siponen, 2001

Hirschheim et al., (1995), Backhouse and Dhillon (1996), Hitchings (1996) and James (1996), suggest that although the value of most IS security methods, tools, and techniques is evident, their focus is on narrow, technically oriented solutions and they ignore the social aspects of risks and the informal structures of organizations (see also the arguments proposed by Baskerville, 1991; Willcocks and Margetts, 1994; Straub and Welke, 1998; Siponen, 2000). Dhillon and Backhouse (2001) have also analyzed existing approaches within the socio-philosophical framework of Burrell and Morgan (1979) and in so doing, they suggest that a socio-organizational perspective is the way forward if information systems security is to be achieved.

The social-philosophical framework of Burrell and Morgan has been widely used in the literature by other researchers as well despite its criticisms. For instance, Hassard (1991) used it as a model to produce four different accounts of work behaviour in the British Fire Service, Korukonda and Hunt (1991) used it to study leadership, while Rickards (1999) used the four paradigmatic positions to explore creativity and the management of change. Since these studies give credibility to the Burrell and Morgan classification framework, this study uses these four sociological paradigms to present a short literature review in information systems security.

2. A FRAMEWORK OF PARADIGMS

Based on Burrell and Morgan's framework there are four sociological paradigms, these are the functionalist, interpretivist, radical humanist and radical structuralist.

2.1. The Functionalist Framework

The functional paradigm approaches the subject from an objective point of view. In doing so, functionalist researchers adopt a more realistic approach, thus postulating that the outside world is made up from hard, tangible and immutable structures. According to Dhillon and Backhouse (2001), the research on the formal automated portion of information security has been investigated through a functional paradigm point of view. These include checklists, risk analysis and evaluation methods.
Checklist is a handout type of a utility for the user that can be referenced to ensure that all the tasks the user has to accomplish are done and noted. In the context of information systems security, the task is to ensure the security of information flow through the systems. The underlying notion of using checklists is to ensure the ideal system solution by studying the entire range of system elements (Baskeville, 1993). In the functional paradigm, checklists provide a way of choosing the best means in order to achieve specified ends (Hirschheim and Klein, 1989). Although checklists are widely used in information systems security, their focus is on observable events and not in the social nature of systems' security.

The focus of risk analysis is on helping people and managers specifically to make informal decisions about investments and to develop risk management and information security policies. Generally speaking, risk analysis has been the cornerstone of security management and it has proven very useful in allowing organizations to justify the cost of new information systems security while avoiding the implementation of unnecessary controls. Risk analysis methods suggest that if countermeasures are developed and implemented in a logical sequential way then, negative risk events can be prevented while information systems can be made more secure. In similar terms, risk analysis techniques allow the definition of financial benefits versus the initial costs of an investment.

The popularity of risk analysis methods is well noticed through the work of various researchers such as Parker (1981), Fisher (1984), Birch and McEvoy (1992), Kailay and Jarratt (1994) although Courtney (1977), Wong (1977), and Fitzgerald (1978) were among the first. Moreover, Merten (1982) look at risk analysis from a managerial viewpoint whereas Anderson et al. (1993) outline risk data repository for a 'dynamic risk evaluation'. Boockholdt (1987) argues that risk analysis is important in establishing security and integrity controls while Saltmarsh and Browne (1993) and Gallegos et al. (1987) differentiate between risk analysis and risk assessment, the former as a process of identification, and risk assessment as the degree of exposure. Based on this differentiation then, Gallegos et al. (1987) support that risk analysis is useful in establishing the monetary value of risks.

Similarly, Lichtenstein (1996) suggests that in the development of information systems, risk assessment is a two-stage process. The first stage defines the scope of risk assessment, which allows the identification of the information resources and then prioritises risks in respect of those resources. The second stage provides useful information in the context of risk-controls, which in turn can be used to make decisions such as whether to transfer risk by implementing safeguards. Moreover, even though organizations use different risk assessment methods at the initiation stage of information systems development the majority of these methods are based on economic or statistical criteria (Lichtenstein, 1996). The main characteristics of such criteria are based on qualitative measures such as usability, complexity, credibility, completeness, adaptability, and validity, with the exception of costs, which are defined by quantitative means.

Evaluation methods is another category of the functional paradigm, where these methods are used by managers in order to measure their own security. An example is, the National Computer Security Center that published in 1983 the Trusted Computer Systems Evaluation Criteria (TCSEC), also known as the Orange Book. TCSEC evaluates technical features of products that are taken "off the shelf", providing managers with a means of deploying a trusted computer system (Dhillon and Backhouse, 2001; Von Solms, 1998). Other evaluation methods and techniques include but are not limited to, the ISO 17799, the German IT Baseline Protection Manual, the Australian and the New Zealand Standard 4444 (Von Solms, 1998; BSI, 2000).

2.2. The Interpretivist Framework

The interpretivist paradigm approaches do not approach their studies from an objective point of view but they are more concerned with the subjective meaning that people attribute to their social situations (Hirschheim and Klein, 1989). Particularly, they look the world through "nominalism", assuming the world is constructed from names, concepts and labels that are used to structure reality. Thus, this reality is better understood by being involved in the behaviour and activities that are examined. In doing so, interpretive researchers believe that people are mainly autonomous and free willed, thus taking an idiographic approach to social sciences.

Interpretive research within the tradition of phenomenology is concerned with the description (Galliers, 1987) and analysis of everyday life (Beynon-Davies, 1997). It provides the identification of themes and social meanings related to the phenomena of interest by concentrating on the aspect of individual experiences (Moreno, 2001). Its actual claim is that knowledge is not the physical but the 'realm of pure thought' (Mingers, 2001). Similarly, phenomenology is based on the 'intuitive grasping of essences of phenomena' whereas the essences are more concerned with issues of *how* and *why* rather than *which* and *what* (Hirschheim, 1992), while a phenomenological disposition involves giving up the natural science attitude and its assumptions (Mingers, 2001).

In the context of interpretive information systems security research, Siponen (2001) suggests that there is much less research undertaken on the social-technical aspects of information security while most approaches are undertaken from a positivist point of view. Dobson (1991) used an interpretive social theory based on Searle's (1969) speech act theory, in order to explain security issues in terms of human roles, actions, goals and policies. Koskosas and Paul (2003) adopted a socio-organizational perspective to investigate information systems security management by focusing on the interrelationship between trust, culture and risk communication.

An interpretivist framework has also been used to business processing and information security models. Backhouse and Dhillon (1996) developed a model of information security for viewing organizations' patterns of behavior while Kokolakis et al (2000) combined organizational and risk analysis in a framework for information security.

2.3. The radical humanist framework

The radical humanist point of view advocates sociology of radical change through a subjective perspective seeking to understand the basis of change within social and organizational settings. Thus, through this perspective radical researchers believe that technology and security controls could violate and isolate people within organizations.

Although there are only few researchers under the radical humanist framework, one of them, Nissen (1989) supports that it would be pointless to demand responsible human action unless managers allow some freedom of action amongst their employees. Angel (2000) suggests that the difference between the criminal and the security officer is a total of social values and that managers make the security process too complicated, uncertain and without imagination. Moreover, he argues that lack of freedom between employees results into a social trap within their organization.

Webler et al (1992) used Haberma's communicative rational theory to explore technical risk analysis and in doing so, they suggest that if social, psychological and cultural variables are excluded from risk identification, assessment and management, the results cannot be as effective as if these variables had been incorporated. They also found that this type of communication helped participants to form a basis of understanding.

2.4. The radical structuralist framework

The radical structuralist framework tries to develop a sociology of radical change through an objective point of view, while emphasizing the need to overcome barriers and limitations placed on existing social and organizational activities. In doing so, the radical structuralist researchers believe that even in positive circumstances, these barriers will never be raised or change in anyway (Burrell and Morgan, 1979). The radical structuralist framework focuses on the analysis of economic power, conflict and disruption (Hirschheim and Klein, 1989).

Similarly, in the context of information systems security, the radical sturcturalist researchers emphasize the need for security designers to take sides with the end-users; that is, the customers, the employees and the suppliers (Dhillon and Backhouse, 2001). McBride and Wood-Harper (2002) have used an end-user perspective by advocating a movement of resources, responsibility and authority away from IT to end-user departments because such departments tend to develop processes for standardising, limiting and controlling the use of technology that results too often to problem solutions from end-user computing activities. However, the problem with moving responsibility to end-uders, may be that managers may see their cost control being affected and their departments feel a loss of control and authority.

Baskerville and Siponen (2002) have proposed the use of meta-policies for emergent organizations because they change and negotiate on a continuous basis. The researchers through the structuralist framework assume that all characteristics and relationships that explain and describe the social world within an emergent organization are developed in fundamental opposites. In doing so, the need to understand these opposites is considered the cause of continuous change and negotiation within the organization (Bresser and Bishop, 1983). Thus, there is a need for security meta-policies that facilitate continuous change and development of control strategies.

However, if the employees find the use of security meta-policies inconvenient and not well presented, the organizations' business objectives will not be efficiently matched with its information technologies. In effect, conflict may arise between managers and employees, in implementing such polices with a subsequent effect a new round of negotiations (Baskerville and Siponen, 2002).

3. DISCUSSION AND FUTURE RESEARCH

The functionalist researchers approach the subject from an objective point of view and in the context of information systems security they believe that information security is based on a good information security policy (Parker, 1981). A meta-policy will allow an organization to be flexible when it makes and maintains its security policies although there has been little research on the need for meta-policies and their use within organizations.

Interpretivist researchers examine information systems security from a contextual and human perspective and they view organizations in terms of their stable underlying patterns of behaviour. In doing so, it is feasible to capture into a model the interactions that are necessary to achieve synchronized, cooperative action (Backhouse and Dhillon, 1996). Up to date, most of the research literature on information systems security has focused on the technical characteristics of information security such as software design, or hardware performance and there is an equal need to integrate these technical issues into a social context, considering organizations' norms, purpose and interpretation of information.

Radical humanist researchers focus on human's dependence from the structures which limit its potential for development. Future research can focus on the notion of change occurring through managerial decisions on information security. For instance, what happens when the implemented security level is too narrow or complex?

The radical structuralist researchers suggest that information systems security imposed by senior managers can result in tension with employees because security measures may have an impact on perceived trust and may affect negatively work cohesion (Koskosas, 2011). Radical structuralism considers social reality as deemed to be a 'fact', so the social world is made up of contradictions and intrinsic tensions whereas, the result would be radical change in the social systems as a whole. Future research within the structuralist framework should focus on information systems security planning and the contradictions that may result.

4. CONCLUSIONS

There is an equal need to undertake research within the social – organizational context of information systems security in order to integrate them with the technical characteristics of information security. In doing so, information systems security planning, development and management can be achieved more effectively than ever before since senior managers and the IT staff involved, will have a broader view of the issue under concern either from a technical or non-technical perspective.

For example, if organizational values, beliefs and exemplars are not widely shared there may be a misinterpretation of the intended information systems security plan. The stronger these values and beliefs are commonly shared among the IT staff, the better and clearer the information security vision to be achieved in accordance to overall business goals.

Since most of the organizations deploy information systems into almost any aspect of business, information security needs to be explored through human interaction, patterns of behaviors, contradictions and meanings associated with security activities and integrate all of them with the technical characteristics of information security.

Although each of the four frameworks-paradigms has its own strengths and weaknesses (Hirschheim and Klein, 1989), they can be used as a basis for future research directions in information security planning, development and management. Or better yet, to understand why there will always be a need to integrate technical and socio-organizational characteristics of information security in order to deploy persistent systems.

REFERENCES

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 1993, Deerhurst, Ontario, Canada, pp.179-188.

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

Backhouse, J. and Dhillon, G. (1996), Structures of Responsibility and Security of Information Systems, *European Journal of Information Systems*, 5(1), pp.2-9.

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

Baskerville, R. (1991), Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, *European Journal of Information Systems*, 1(2), pp.121-130.

Baskerville, R. (1993), Information Systems Security Design Methods: implications for information systems development*, ACM Computing Surveys*, 25(4), pp.375- 414.

Baskerville, R. and Siponen, M. (2002), An Information Security Meta-Policy for Emergent Organizations, *Logistics Information Management*, 15(5/6), pp. 337- 346.

Beynon-Davies, P. (1997), Ethnographic and Information Systems Development: Ethnography of, for and within IS Development*, Information and Software Technology*, 39(8), pp. 531-540.

Birch, D. and McEvoy, N. (1992), Risk Analysis for Information Systems, *Journal of Information Technology*, 7, pp. 44-53.

Boockholdt, J.L. (1987), Security and Integrity Controls for Microcomputers: A Summary Analysis, *Information and Management*, 13(2), pp.33-41.

BSI (2000), British Standards Institution, *Annual Reports 2000*.

Burrell, G. and Morgan, G. (1979*), Sociological Paradigms and Organizational Analysis*, London: Heinman.

Bresser R. K. and Bishop R. C (1983), Dysfunctional Effects of Formal Planning: Two Theoritical Explanations, *Academy of Management Review*, 8(2), pp.588 – 599.

Courtney, R. (1977), Security Risk Analysis in Electronic Data Processing. *Proceedings of the AFIPS Conference*, National Computer Conference (R.R.Korfhage), Vol. 46, AFIPS Press, pp.97-104.

Dhillon, G. & Backhouse, J. (2001), Current directions in IS security research: towards socio-organisational perspectives, *Information Systems Journal*, 11, pp. 127-153.

Dobson, J. (1991), A Methodology for Analysing Human and Computer-Related Issues in Secure Systems, In*: IFIP International Conference in Computer Security and Information Integrity*, Amsterdam, pp.151-170.

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

Fitzgerald, J. (1978), EDP Risk Analysis for Contingency Planning*, EDP Audit Control and Security Newsletter*, 6(2), pp.1-8.

Gallegos, F., Dana, R.R., and Borthick, A.F. (1987), *Audit and Control of Information Systems*, Cincinnati, OH: South- Western Publishing Co.

Galliers, R.D. (1987), Information Systems Planning in the United Kingdom and Australia: A Comparison of Current Practice, In: *Oxford Surveys in Information Technology*, Vol.4, P.I. Zorkoczy (ed.), pp.223-255.

Hassard, J. (1991), Multiple Paradigms and Organizational Analysis: A Case Study, *Organization Studies*, 12(2), pp. 275-299.

Hirschheim, R., Klein, H.K. (1989), Four Paradigms of Information Systems *Development, Communications of the ACM*, 32(10), pp. 1199-1215.

Hirschheim, R. (1992), Information Systems Epistemology: An Historical Perspective, In: *Information Systems Research: Issues, Methods, and Practical Guidelines*, R. Galliers, (eds.) Blackwell Scientific Publications, Oxford, pp. 28-60.

Hirschheim, R., Klein, H.K. and Lyytinen, K. (1995), *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*, Cambridge: Cambridge University Press, UK.

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*. Gritzalis, D. (eds), pp. 3-12, London: Chapman and Hall.

James, H. (1996), Managing Information Systems Security: A Soft Approach, *Proceedings of the Information Systems Conference in New Zealand*, Editor: Phillip Sallis, October 30-31, Palmerston North, New Zealand.

Kailay, M. and Jarratt, P. (1995), RAMeX: a Prototype Expert System for Computer Security Risk Analysis and Management, *Computer and Security,* 14(5), pp. 449- 463.

Kokolakis, S.A., Demopoulos, A.J. and Kiountouzis, E.A. (2000), The Use of Business Process Modelling in Information Systems Security Analysis and Design, *Information Management and Computer Security*, 8(3), pp. 107-116.

Korukonda, A.R. and Hunt, J.G. (1991), Premisses and Paradigms in Leadership Research, *Journal of Organizational Change Management*, 4(2), pp. 19-33.

Koskosas, I. (2011), Cultural and Organizational Commitment in the Context of e- Banking, *International Journal of Internet Technology and Secured Transactions*, 4(1), pp. 26-41.

Koskosas, I. And Paul, R. (2003), The Performance of Risk Management in the Context of Goal Setting: The Case of Internet Banking, *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*, Editors: Thomas Acton, June 24th, pp. 242-249.

McBride, N. and Wood-Harper, A.T. (2002), Towards User-Oriented Control of End- User Computing in Large Organizations, Journal of End-User Computing, 14(1), pp. 33-41.

Merten, A. (1982), *Putting Information Assets on a Balance Sheet*. Risk Management, January.

Mingers, J. (2001), Embodying Information Systems: The Contribution of Phenomenology, *Information and Organization*, 1(2), pp. 103-128.

Moreno, V. JR. (2001), On the Social Implications of Organizational Engineering, *Information Technology and People*, 12(4), pp. 359-389.

Nissen, H.E. (1989), ISD for Responsible Human Action, In: Systems Development for Human Progress (Klein, H.K. and Kumar, K., eds), pp. 99-113, Amsterdam: Elsevier Science Publications.

Lichtenstein, S. (1996), Factors in The Selection of a Risk Assessment Method, *Information Management and Computer Security*, 4(4), pp.20-25.

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

Rickards, T. (1999), Creativity and the Management of Change, Oxford: Blackwell Publishers.

Saltmarsh, T. and Browne, P. (1993), Data Processing- Risk Assessment, In: *Advances in Computer Security Management*, Vol.2, Wofsey, M. (eds), pp.93-116, Chichester: John Wiley and Sons.

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

Siponen, M.T. (2000), A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, 8(1), p.31-41.

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 Millenium*, Dhillon, G. (eds.), Hershey: Idea Group Publishing.

Straub, D.W. and Welke, R.J. (1998), Coping with Systems Risks: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22(4), pp.441-469.

Von Solms, R. (1998), Information security management (1): why information security is so important, *Information Management and Computer Security*, 6(5), pp.224-225.

Webler, T., Rakel, H. and Ross, R.J.S. (1992), A Critical Theoretic Look at Technical Risk Analysis, *Industrial Crisis Quarterly*, 6(4), pp. 23-38.

Willcocks, L., and Margetts, H. (1994), Risk Assessment and Information Systems, *European Journal of Information Systems*, 3(2), pp.127-139.

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