Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches

Andreas E Wagner and Carole Brooke
Lincoln Business School, University of Lincoln, UK
andreaswagner75@yahoo.de
cbrooke@lincoln.ac.uk

Abstract: Security is still too orientated towards technology and behavioural aspects are under prioritized. Organisations focus on the ability of technology to minimise risks. This paper as a preliminary research of a PhD thesis will argue that this assumption and approach is misguided, so we will focus on how a critical approach is more useful to exposing these issues. The key to secure systems is employees' perception and the action they take in accordance with the learned and perceived need for an understanding of compliance. The paper is about critical approaches to research and it just happens to be information and communication technology (ICT) that is the subject area.

Keywords: critical research, ICT security, organizational misbehaviour, learning, compliance.

1. Introduction

The growing use of information and communication technology (ICT) is affecting modern businesses. As a result, security issues have become more apparent. It is now regarded as essential that knowledge management is supported by high security processes in order to protect and deliver organisational success. The traditional brick and mortar boundaries of organisation have disappeared and are replaced by connectivity involving internal and external users.

Security is still too orientated towards technology and behavioural aspects are under prioritized. Organisations focus on the ability of technology to minimise risks. This paper will argue that this assumption and approach is misguided. A large number of security breaches result from peoples' behaviour, which cannot be solved by the use of technology itself. It is about people and specifically about organisational misbehaviour.

Organisations do have to manage peoples´ expectations, power, and fear. People are more likely to engage themselves in security to the extent that they believe in its importance for business success. People, who trust that they will benefit while engaged in the process, both by acting according to guidelines and by promoting compliance, will support organisational security. However, people will always find a way around the system.

Employees need to believe that they will benefit while acting in a secure way and if this is not the case then they will not make their contribution. Awareness programmes, education and training often seem more likely to put people to sleep than to improve their behaviour.

This paper will examine a gap in management practice and the existing literature. The first author has been involved for over seven years in consulting of ICT security, thus familiar with actions and developments. His current position at an international service provider and his relationships in a large network of ICT experts is used to access the thoughts and experience of colleagues and partners in the practices of ICT security. Practice shows that the role of behaviour is not considered comprehensively enough, even though its importance has been widely recognised. Current research in this area fails to address the holistic approach, especially by lacking to focus on subjective issues. More attention needs to be paid to these aspects in order to learn why misbehaviour takes place and how it can be reduced.

To tackle these weaknesses, we propose a conceptual foundation for security behaviour. The key to secure systems is employees' perception and the action they take in accordance with the learned and perceived need for an understanding of compliance. This is explored in more depth and a framework of issues proposed for addressing the problems critically. There is a need for critical research. Listening to and understanding language and power issues are themes which have to be explored further.
Our initial research question will focus on the identified gap. Practice and theory do not pay enough attention to the use of technology. ICT, especially security because of the weakest link phenomenon (this will be described later in-depth), is always human dependent. But organisations are focusing on technology although most of ICT professions and experts know that the human factor is key. Mostly there is a strong

Reference this paper as:
Wagner A. and Brooke C. (2007) "Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches." *The Electronic Journal of Business Research Methods* Volume 5 Issue 2, pp 117 - 124, available online at www.ejbrm.com

separation in organisations to solve ICT and behavioural issues. ICT administration focuses on infrastructure and the human resources or marketing department (e.g. internal communication) addresses behaviour.

Similar ideas regarding an existing gap of missing out human issues in practice are found in other research (Brooke 1994, Stahl 2005, Backhouse & Dhillion 1996, Backhouse 2004, Sauer 1993). These authors are not addressing the specific field of ICT security, but they use critical research (Brooke 1994) or social constructivism (Stahl 2005, Sauer 1993) to explore the cause of the problem for not reaching the organisation's goal. On one hand Brooke identified a quality gap in total quality management (TQM), Sauer why IS projects often fail, and on the other hand Stahl and Backhouse focus on the necessity to build in ´soft stuff drivers´ to minimise failures in IS.

Our research question focuses on the human factor. Each individual him-/herself is the Achilles heel for security of the organisation's infrastructure (Gonzales 2002, Zegers 2000). In practice we found that battling attacks is only reactive and mostly technology dependent. Our critical approach will address relationships and language as central issues to improve the existing decision making (because organisations are wasting time) and to trigger understanding (Thomson and von Solms 1998) for the importance of sensitive and responsive behaviour. Practice shows that expertise (in our context the ICT professional) tends to ´push the right mind set´ rather than ´pull the suitable behaviour´ (Clegg 2004). The rates of accidents appear to be high, and rates of compliance low. Therefore people have to be triggered to move towards compliance.

We do not present solutions but bring ideas with this paper. The recommendations we will present are for managers of organisations and research fellows. We believe there is a need to stimulate further debate concerning whether and how the existing gap can be filled.

2. The extensive nature of literature

To set this interdisciplinary paper in context we wish to make three interrelated points. Firstly, there is a lot of research in the technology area, especially on ICT security and its adoption but a lot of it is best practices-based and draws attention to the involved technologies itself or service processes supporting the organisation's business. The important question is: What is good practice, and perhaps just as importantly, which lessons learned are drawn from bad practices. There are a lot of practice-oriented approaches to ICT security, but only leading vendors and service providers summarise some best practices. In general ICT security is presented as a heterogeneous landscape.

Second, our research makes strong claims of the necessity to address the individual user. The effectiveness of ICT infrastructure is dependent on the individual. People enable technologies and processes. Inevitably perhaps, there are general needs, wants and demands of each individual. We recognise that behaviour is dependent on the ability to behave in a right way and the drivers which influence behaviour. Therefore it is crucial to acknowledge individual's ability in spite of perception, experience, education, and training. On the other hand we will critically review drivers such as motivation, attitude, and intention of the individuals.

Finally, it is apparent that most of ICT security approaches have to balance technical issues and at the same time human-related changes. We identified some generic points of relevance, which we will bring together to fill the existing gap. Change management, knowledge creation, and communication play an important role in organisations. ICT security has to be addressed continuously to minimise threats and vulnerabilities. Why are most of the organisations wasting time?

For ICT security the centre of interest should be the individual. This phenomenon calls Ghosh (1998, 2001) weakest link scenario in his two books. It is not only a buzzword to involve people, to drive participation, and to trigger real ownership of the individuals. It is a real need of organisations, which adjudicates (in the worst case) if an organisation will survive or not. Misbehaviour of only one individual regarding access to vulnerable information at a specific time (in this context high threatening time frame) could give him/her or a third person (with or without his/her knowledge) the possibility to attack, destroy or modify important information. The wave of simplification in ICT networks and the growing complexity (e.g. access anywhere and anytime) makes the tasks of ICT professionals difficult. Vulnerabilities and threats are the counterparts of business needs, which should be addressed through the right perception of the individuals and the suitable action they take. In a way ICT professionals have to deliver a secure system which adds value to the business.

3. Identifying the gap

The extensive literature and research on one hand and our gained experience out of practice on the other hand show that traditional views are still dominating this field. The subjective nature of behaviour is rarely addressed but its influence is still increasing (which is also seen and accepted by practitioners and researchers). In this paragraph we will take a deeper look into best practises and standards of organisations, which can be summarised by three areas: technology focus, process focus, and general management.

Pye and Warren (2005) are benchmarking security models and framework. They are taking a technology-oriented approach if they claim that ´security has to become proactive by reviewing and continuously improving security' (p.80). As a lot of ´technology only´ approaches they underline the importance of measures and policies, so ´security can only proactively be realised through periodic revision´ (2005, p.80). We picked out of the mass of research, papers and books their work, because they are drawing relationships to continuous improvement principles of TQM. At this point we cannot agree that it is realistic to reach their mission by focusing on TQM principles (see our former research, especially Brooke 1994). Moreover Pye and Warren (2005) conclude their research by claiming that a security chain is only as strong as its weakest link, but ´highest importance have measures and policies which are designed to deliver guidance, manageability and consistency´ (2005, p.86). Again, we disagree because they focus on explicit knowledge enabling management to drive an input-output mechanism, so human behaviour becomes a computed machine. Pye and Warren modify their viewpoint by trying to involve soft stuff, but they see it as an added value if the technology stuff is solved (they call it as a ´need to encourage a culture of security awareness´ (2005, p.86).

Schneier´s book ´Secrets and lies´ (2000) pays more attention to the individual by addressing security not as a product. For him security is a process, so he claims not to find the perfect solution but working on a process to secure systems which can not be completely broken. We see the interesting fact that the author looks not for a 100 percent secure system (because it is impossible to realise) but a way to minimise threats and vulnerabilities. For Schneier (2000) the right service process is the key. Therefore he claims to design, implement and maintain suitable processes, which can be best solved by ´outsourcing of security processes´ (2000, p.387). We see that this ideology of process-oriented approaches such as IT infrastructure library (ITIL), COBIT, ISO17799 or BS7799 limits the ability of the ICT professionals to perceive subjectivity. These standards generate a shared use of language. In practice ICT professionals of the outsourcer tend to separate fundamentally the outsourced infrastructure to behavioural issues. Neither have they seen the need to involve the individuals nor to look for participation of stakeholders. On the other hand only issues are solved which are defined in a contract and service level agreement (SLA). Consequently behaviour and process are not seen as intertwined aspects. Again, ICT-security faces a general management challenge.

Other authors pay more attention to how security is handled by management in general. Especially Hancock (2002) deals with the management of a security event as part of corporate crisis management. We identified in practice that the importance of security gets ´management attention´ if a real crisis happened. Regularly the ´crying wolf syndrome´ appears – this means that every single security problem is treated as a corporate crisis. Consequently not only management attention is rising but general sensitivity to threats and vulnerabilities is exploding. The (re-) action of top management is often not suitable because they set security temporally on highest importance (but if the crisis is gone they are losing focus). Again, these management decisions do not offer any solution to the generic security problem, because not all individuals are involved continuously. Ongoing involvement is fundamentally important to get them participating in the security activities and taking over ownership for it. Besides we see in practice that top management support is important but middle management has to leverage compliance by triggering all users.

Our research is inspired by the idea to secure the weakest link, so there is no way to avoid focusing on the individuals' behaviour. Knowledge about the entire vulnerability landscape is important but the key is to expose a security ideology to build up the language and involve people to own the weakest link challenge, change the existing environment, and secure it (e.g. minimise incidents). Only the individuals can minimise security risks.

4. Choosing the suitable research methodology

The sophistication of hacker tools is steadily intensifying whilst at the same time resulting in less technical knowledge being needed to break into systems. The necessary resources are given, but does it mean that they are also used? Schneier (2000) put it into the following words: ´Cyberspace crime includes everything you'd expect from the physical world: theft, racketeering, vandalism, voyeurism, exploitation, extortion, con games, fraud´ (p.15). And if we are speaking about vulnerabilities and threats we do not focus only on external attacks or those which are driven by intention. Malicious or benevolent behaviour is possible, which has different effects if the ´hacker´ is an expert or a novice (to get more information about the types of threats and vulnerabilities see Stanton et al., 2005). We will address this challenge later on, but in the first step we will explain why we use critical research.

Organisations have to bear in mind that every user could be the weakest link. Traditional views assume a way of deducting future occurrences from past ones. This implies objectivity is given. We reject this view point, because of the subjectivity of human theory. Behaviour is socially constructed depending on language and ideologies. Our research emphasises relationships and gives privilege to investigating the organisational context. For us language is central, and we propose that ICT security research should put more focus on meaning and perception.

No academic group as far as we can tell has considered a holistic ICT security approach. We do not want to give the impression that this is fully uncharted territory but rather that it is not explored much by management research nor does it take into account the highly subjective nature of ICT security.

5. Using critical research and postmodernism

In this paper we propose a research methodology that harnesses aspects of critical research and postmodernism. We do this because it enables us to access different voices and consider the balance power involved.

Organisational behaviour (e.g. leadership, motivation) is strongly qualitative. Broader and richer descriptions help to build up more sensitivity to the ideas and meanings. The main tasks for critical research are to break up established ways of using language and to problematise language. For Alvesson and Deetz (2000) critical theory is participative and dialogic addressing insights, critique, and transformative re-definition. ´Critical research calls for at least the first 2 elements´ (Alvesson and Deetz 2000, p. 164).

Interpretation produces insights by addressing the non-obvious, by making sense, and by enriching the situation whilst broadening the angle of perspectives to highlight problems and also possibilities. Our critique (through deconstruction of language and balances of power) seeks to undo frozen meanings; an example being that ICT has nothing to do with the 'soft stuff' of research inquiry. It then becomes possible to attend to detail (e.g. behaviour of the individual), to institutional macro-oriented themes (e.g. ICT attacks and cyberspace crime), and to counteract taken-for-granted goals and ideas (e.g. ICT has been bounded as 'hard stuff' while leaving out 'soft stuff'). Our critique explores domination and the repression of ICT labelling. Just as transformative re-definition as a counterpart to insight and critique helps us to produce new ways of seeing and thinking, so ICT-related hard stuff is bridged to the human-related soft stuff. The context for individuals' action has to be re-thought, re-felt, and re-experienced. In a way of transformative re-definition we will try to indicate an alternative way, and not wasting valuable management time. Listening to and understanding language and power issues are crucial themes.

In Alvesson and Deetz (2000) point of view postmodernism could mean one of three things: (1) using Freud more unconventionally, (2) heeding structuralist language theory from Saussure, and (3) focusing on language. We will focus on the third one in this paper. Language is intrinsically related to meaning and perception, because it becomes central through discursive practises.

The combination between postmodernism and critical theory may well provide ´the best remaining option´ (Alvesson and Deetz 2000, p. 103). For Alvesson and Deetz (2000) postmodernism is more a pull theory and critical theory more a push theory. The goal is to develop critical sensitivity. Therefore ´de-familiarization becomes a key´ (Alvesson and Deetz 2000, p.178). We negate current ICT approaches to get the familiar foreign (e.g. wasting time: The mission impossible with respect to technology-oriented security approaches). Our research will set direction for ICT security, commitment to the individuals and sharpness for the importance of the 'soft stuff'.

6. The subjective nature of ICT security

The subjective nature of ICT security is formatively driven by the individual. Cultural, social, personal, and psychological factors influence behaviour. The latter one includes motivation, perception, learning, beliefs and attitudes influencing behaviour. This paper does not offer the space to discuss all these facets nor present the silver bulletin solution but raises attention to promote subjective approaches within ICT security decision making. Therefore we will pick some of the most influential ones for security.

To describe the inability of technology and the importance of behaviour we will describe the case that documents in trash are often more valuable than the same data in a computer. It is a human problem. First of all the right perception of threats and vulnerabilities is crucial. Often people overestimate or underestimate the probabilities of attacks because they do not have the experience, training, education on one hand or the right ´drivers´ on the other hand (our term ´drivers´ we will explain later on).

In the case of there being too many alarms the individuals will learn to ignore them (e.g. in an extreme instance the ´crying wolf syndrome´ causes total ignorance). In this case the individual is not driven by anything such as motivation, attitude or intention because people stop asking why things happen. They only do their work without thinking about the consequences. (An example might be where an employee is called by another employee or external partner whom they do not personally know and with whom they exchange confidential data over the telephone because they think the one who is calling will be trustworthy).

These cases offer a hint that is important to take a deeper look into why people do not understand risks or are not acting accordingly to the known. Practice shows that there is a big difference how people are behaving at work if you compare it with the behaviour at home. In our point of view it is all about the right combination of ability and drivers.

We put the term ability in the context that the individual knows what compliance is. Each individual has to have the understanding why security is crucial for the organisation and how to behave if a certain incident appears (or even having a hint what to do or whom to involve). For us the right perception (what is going on), experience (comparing past incidents with the current problem), fundamental education (why security is so important) and training (how to behave in a certain situation) are intertwined.

There are several authors (Hazari 2005, Krueger and Dickson 1994, Sitkin and Weingart 1995) researching the area of perception to get more insights into the notion of perceived behavioural control and self-efficacy. But this research regarding perception alone does not help. For us perception has to be bridged the other aspects. In a way experience has a certain impact on education and training, and vice versa. For an experienced person it is easier to match practical insights with explicit knowledge (which is educated) or tacit knowledge (which is trained). The other way round education and training helps to reach a better learning curve regarding the ability to behave. Experienced behaviour is the outcome. Vom Brocke and Buddendick´s research (2005) focuses on skills and competence which is generated by education and training. Again, their research allows us to question education and training in general but a contextualisation is required.

We will move forward, albeit incrementally, to generate a holistic view while raising attention to promote suitable ´security drivers´. ´Drivers´ are extrinsic and intrinsic parameters to take action according to compliance. In our point of view security drivers can be subsumed by motivation, attitude and intention. For some authors (Cullen 1997, Osterloh and Frey 2000) extrinsic motivation, e.g. using punishment and rewards, is the key. If we put it in the context of security it is not sufficient to use only punishment and rewards because they are reactive. Intrinsic motivation is more important than extrinsic motivation, because it is the only way to transfer tacit knowledge. Tacit knowledge plays an important role for security behaviour. Technology- and process-oriented approaches focus on explicit knowledge– and our research shows that there is still a gap regarding secure behaviour.

Attitude and intention are more long-term drivers, which we are not addressing further in this paper. To bridge attitude and intention to ICT security we identified a supportive nature of the organisation’s mission to safeguard existing resources (e.g. security as a long-term objective to stay competitive), but it is a long way to go to get such high-level organisational stuff transferred to the individual. In a way this has an effect on the relationship between ICT and ideology.

7. Filling the gap

Filling the gap means stopping the waste of time by following only technology- and process-oriented security approaches. We have just touched these approaches the organisations implement and maintain in practice. The key to fill the existing gap is that organisations have to pay more continuous attention to the users’ behaviour. From a critical point of view the individual is unique.

Ability and drivers have to be understood and organisations have to follow a holistic approach with respect to an embedded organisational development and change. Organisations must trigger a sense of urgency, because business becomes e-business so the survival of organisations is dependent on the security of their core resources. There is no way round to be connected with partners, suppliers, and lots of remote users. Business gets enabled through the use of technology (ICT revolutionised business and there is just a new wave coming up: Leveraging business through web services and service-oriented architectures (SOA)). That is one side of the coin. The other one is ´gaining´ vulnerabilities and threats with which the organisation is confronted. Management has to reflect change, to support knowledge creation, and to create a security culture.

The environment changes, competition moves and the organisation itself goes through an evolutionary process. Attention has to be paid to human and organisational challenges. Understanding has to be generated, language has to be modified and the suitable behaviour has to be put in place. We see a continuous transition towards ICT security culture change as the right mission to follow. Transition bridges the traditional and the new approach by developing the organisation from ending the traditional views to a new beginning. Our view is supported by Clegg (2004), who calls for a replacement of push-based with pull-based approaches to involve the individuals, to get them participating, and to influence their behaviour by generating ownership. Changing the user's behaviour means driving the individual through a psychological transition process. We see knowledge creation in a key role to create a security culture, which minimises the waste of time.

In this context we cite Balogun and Jenkins (2003), who claim to re-conceive change management and put it into a knowledge-base perspective. Knowledge generation supports the change process with the mission to generate a security culture. Nonaka and Takeuchi´s (1995) knowledge creation spiral puts attention to the tacit and explicit dimensions of knowledge while middle management plays an important role to drive this process. In practice wasting time begins and ends with middle management.

We underline the importance of ability, especially tacit knowledge, and intrinsic drivers to solve the dilemma of the weakest link. Knowledge creation is dependent on, but also influences, culture. Relationships within the organisation provide a basis for a form of socialisation which is important in exchanging tacit knowledge. Sharing knowledge can be enabled by adequate communication to create useful relationships between the individuals to share their knowledge and learn from each other. For Balogun and Jenkins (2003) an enabling context has to legitimise this behaviour. We come back to the important role of middle management as ´enabler for secure behaviour´. The culture has to trigger thinking and understanding to be efficient and effective regarding the security challenges the organisation is confronted with.

The twin of each change is communication. We see that security culture has to be brought to life by communication and can only survive by continuous communication. To generate a common understanding, suitable language and a security view regarding conversations and dialogues with the individuals are necessary. The enabling context (influenced by and supporting ideology) has to be owned by the users and driven by middle management. A lot of socially driven activities have to be orchestrated by individuals (and legitimised by top management) to meet both formal and informal requirements. Language is the key to enable perception and anticipation on one hand and to leverage action and responsiveness on the other hand. From a critical research standpoint a 100 percent security culture is not achievable. It is unrealistic or utopia. Security culture can reduce risks and helps to handle vulnerabilities and threats.

An organisation can only move forward into a secure direction if the culture supports the suitable perception of current problems and anticipation of future incidents. Real ownership by the individual regarding security acknowledges the effectiveness of a security culture development. Communication, response, convenience, language, expectations, understanding, participation, and a lot of similar aspects improve the senses to anticipate security vulnerabilities and threats.

To see what is going on is not good enough. Each individual has to take action and to leverage his/her responsiveness. In this context we refer to Locke (1991), who focuses on the motivation sequence and developed a model which combines a lot of well-know theories. Overall Locke's model describes that a certain performance outcome can be affected if adequate ability and knowledge is given, but a precondition is that the individual chooses commitment to a certain outcome. Again, we see that the aspect of ownership is stressed, so management has to put security at the heart of the organisation.

Barlow and colleagues (2005) explored how to transform business to a sensitive and responsive organisation. For them the organisation has to develop itself upside down, which we would like to see as accompanied by middle management (and legitimised by top management). Again, we can conclude that a knowledge-driven culture with respect to security has to be realised to minimise risks. Barlow and colleagues (2005) underline this ´no waste mentality´ (p.191).

8. Conclusions

The traditional view of organisations controlling and knowing all activities has to disappear and to be replaced by a mission generating ownership of all internal and external users to secure the core resources. Yet even if people are committed 100 percent security is impossible. Technology- and process-oriented best practices and standards can not support the mission to have an immune network. Because of its subjective nature, especially the weakest link phenomenon in ICT security, these approaches can not fulfil the mission they are driving for. Organisation development, knowledge creation and security culture are fragments to get the security puzzle solved. Throughout we are arguing in this paper to put the individual into the focus of interest. Understanding language and power are crucial to leverage ICT security (which is supported by technology and processes but enabled by the individuals themselves). In order to protect and deliver organisational success in practice more and more secure organisations get rid of these traditional assumptions and approaches, because they are misguided. The key to secure ICT infrastructure is employees' (anticipative) perception and the (responsive) action they take in accordance with the learned and perceived need for an understanding of compliance. There is a need for further research, which we are opening up with our paper.

9. Recommendations

A more critical attitude can support practitioners and researchers, particularly in ICT security. The cumulative effect would be a move to the subjectivity of the individual. In practice more and more organisations stop believing that if vulnerabilities and threats can be understood, risk is manageable by ´hard stuff-oriented´ best practices and standards. Holistic research can balance the above mentioned limitations. The mission could be the minimisation of ICT incidents, but it is not realistic to assume this will achieve a secure environment. Overall we tend to connect ICT security to performance goals of the organisation. Only then, can it break free of the view that security is owned by the ICT department. We propose that it is all about people management, especially language and power and its subjective nature.

10. Further research

This paper as a preliminary research of a PhD thesis is backed up by literature of connected areas and the experience we gained in practice and research. We highlight the need for further research in the field of ICT security. Qualitative research in all its facets would generate more insights into this area. Research of a more quantitative nature (e.g. large surveys) could be done to explain further the market views of vendors and analysts, which underline that the understanding of people is one of the key issues securing organisations´ business. It would be interesting to explore technology- and process-orientated approaches and the way they could be leveraged by a holistic people-centred practice. Perhaps then we can create a mission that is less impossible?

References

Alvesson, M., and Deetz, St. (2000) *Doing critical management research,* Sage, London.

Backhouse, J., and Dhillon, G. (1996) "Structures of responsibility and security in information systems", *European journal of information systems*, 5, 2-9.

Backhouse, J. (2004). *Risk management in cyberspace*, London School of Economics and Politics, London.

Balogun, J., and Jenkins, M. (2003) "Re-conceiving change management; a knowledge-base perspective", *European management journal*, 21 (2), 247-257.

Barlow, S., Parry, St., and Faulkner, M. (2005) *Sense and respond: The journey to customer purpose*, Palgrave, London.

Brooke, C. (1994) "Information technology and the quality gap", *Journal Employee Relations*, 16 (4), 22-34.

Clegg, C.W., and Walsh, S. (2004) "Change management: Time for a change", *European journal of work and organisational psychology*, 13 (2), 217-239.

Cullen, D. (1997) "Maslow, monkeys and motivation theory", *Organization*, 4 (3), 355-373.

Ghosh, A. K. (1998) *E-commerce security*, Wiley & Sons, New York.

Gosh, A. K. (2001) *Security and privacy for e-business*, Wiley & Sons, Weinheim.

Gonzalez, J. J. (2002) "A Framework for human factors in information security", *Rio de Janeiro: WSEAS Int. Conf. on Information Security*.

Hancock, B. (2002) “Security crisis management - The basics”, *Computers and security*, 21 (5), 397-401.

Hazari, S. (2005) “Perceptions of end-users on the requirements in personal firewall software: An exploratory study”, *Journal of organizational and end user computing*, 17 (3), 47-65.

Krueger, N. Jr, and Dickson, P. R. (1994) “How believing in ourselves increases risk taking: Perceived”, *Decision Sciences*, 25 (3), 385-400.

Locke, E. A. (1991) “The motivation sequence, the motivation hub, and the motivation core”, *Organizational behavior and human decision processes*, 50, 288-299.

Nonaka, I., and Takeuchi, H. (1995) *The knowledge-creating company*, Oxford University Press, Oxford.

Osterloh, M., and Frey, B. S. (2000) “Motivation, knowledge transfer, and organizational forms”, *Organization science*, 11 (5), 538-550.

Pye, G., and Warren, M. (2005) “Benchmarking e-business security: A model and framework”, *Proceedings of 3rd Australian information security management conference*, 80-87, Edith Cowan University, Perth.

Sauer, Ch. (1993) *Why information systems fail: A case study approach*, Waller, Hatfield.

Schneier, B. (2000) *Secrets and lies*, Wiley & Sons, New York.

Sitkin, S. B., and Weingart, L. R. (1995) “Determinats of risky decision-making behaviour: a test of the mediating role of risk perceptions and propensity”, *Academy of management*, 38 (6), 1573-1592.

Stahl, B. C. (2005) “Reflective responsibility for risk”, *unpublished paper*, Leicester.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005) “Analysis of end user security behaviors”, *Computers and security*, 24 (2), 124-133.

Thomson, M. E., and von Solms, R. (1998) “Information security awareness: Educating our users effectively”, *Information management and computer security*, 6 (4), 167-173.

vom Brocke, J., and Buddendick, Ch. (2005) “Security by learning – the contribution of e-learning to security awareness management”, *unpublished paper*, Muenster.

Zegers, N. (2000) *Battling insider attacks: Deterring improper security behaviour,* Erasmus University Rotterdam, Rotterdam.