

CRITICAL SUCCESS FACTORS AND REQUIREMENTS FOR ACHIEVING BUSINESS BENEFITS FROM INFORMATION SECURITY

Alberto Partida , Jean-Noël Ezingard

Henley Management College

Abstract

The literature on Information Security suggests that Information Security is a strategic undertaking for most organisations. Its success is likely to depend on a clear understanding of management processes and accountabilities and a strict alignment between business objectives and strategy and the Information Security policy of an organisation. The literature also suggests that too often silos install themselves around operational risk management in organisations, preventing integration between different parts of the organisation responsible for operational risk management.

Through a survey of over 80 Information Security professionals and business experts worldwide, we show that organisations that develop their information security practice out of a strong management commitment, integrate their risk management processes and align them, including information security, with their strategy and objectives obtain superior benefits. Currently the three most common benefits identified in organisations are increased stakeholder value, new business opportunities and better governance (compliance).

Keywords: *Critical success factors, information security, risk management, benefits.*

1 INTRODUCTION

Information Security is still at the top of many managers' mind and Information Security stories increase their appearance in the media. This is partly because some of the technical challenges underpinning Information Security are continuously changing, for instance with the growth in Service Oriented Architectures (Akella et al., 2007) and the disappearance of the network boundary (ISF, 2005c). In parallel, the threats to Information Security are not abating and although the number of attacks and misuses reported has increased, there is still a lack of willingness to report incidents (CSI/FBI, 2006). Unfortunately, whilst practitioners report security budget increases, few feel confident about the success of their efforts. More importantly, we seem to be witnessing concerns about the lack of strategic investments in Information Security, with the number of organisations appointing a Chief Security Officer (CSO) or a Chief Information Security Officer (CISO) remaining stubbornly under 25% (Price., 2006). In such circumstances (lack of confidence and lack of strategic investments in Information Security), there is a continued need to understand the benefits for the business of a well-developed approach to Information Security and the critical success factors to achieve them. The research presented here addresses this need through a survey of 86 Information Security and business experts. The results are analysed for correlation between management

commitment, maturity of Information Security practice and risk management processes in general, as well as for alignment with strategic objectives and benefits to the organisation. The paper is organised as follows: first, we present a review of the literature on strategic approaches to Information Security. This is followed by a brief explanation of our hypothesis and research design. The results of the survey are then presented leading to conclusions on the importance of management commitment, development of Information Security, risk management processes and strategic alignment to transform an organisation's Information Security capability into a business enabler (i.e. providing benefits to the organisation).

2 LITERATURE REVIEW

2.1 Critical success factors for Information Security

Human risks are at the top of most risks lists. It is often written that any Information Security process should start with Education, Training and Awareness programmes (Whitman, 2003). Even when paying special attention to human sources of risk, the context of Information Security is wider than most technical approaches can describe (Ashenden & Ezingard, 2005). Risk assessment, and therefore risk management is intertwined in organisational politics, social amplification, and relationships. Consequently, there is still a lack of understanding as to what the critical success factors are in achieving a strategic approach to information security. (Thompson, 2005)

Table 2-1 below lists 8 factors that are often quoted in the literature. These broadly group under two themes: (1) Management Processes and Accountabilities and (2) Alignment.

| Critical Success Factors | Reference |
|--|--|
| Theme 1: Management Processes and Accountabilities | |
| Obtain management commitment. | ISO (2004 and 2005); COSO (2004); Appel (2005) and Ezingard et al., (2004) |
| Establish a programme to improve security management enterprise-wide and enforce it. | Straub (1998), ISF (2005a). |
| Follow a standard. | May (2002), Von Solms (2005a). |
| Communicate the business value of Information Security using a common risk language. | Scholtz (2004b and 2004c), Coles and Moulton (2003). |
| Determine risk ownership undoubtedly. | Coles and Moulton (2003). |
| Theme 2: Alignment | |
| Reflect business objectives in information security elements. | Birchall et al. (2004), Scholtz (2004a), ISO (2005). |
| Link Information Security with IS and overall strategy. | Booker (2006), Leskela et al. (2005), Birchall et al. (2003). |
| Be consistent within the organisational culture. | Birchall et al. (2004), Scholtz (2004a), ISO (2005). |

Table 2-1. Information Security critical success factors.

2.2 Management processes and accountability: Silos, absence of development and lack of integration as a barrier to achieving a strategic approach to Information Security

There have been a number of calls for Information Security to move away from Information Technology (IT). Security teams should move out of the IT organisation and into corporate risk and compliance teams (Scholtz, 2004a). The argument for such a move is that organisations often tend to keep too focussed on IT issues rather than on risks related to the business (Coles and Moulton, 2003). The drive for integration of risk management efforts is leading many organisations to attempt to integrate information security into their wider risk management efforts – and in particular operational risk management. According to the Basel II Accord (2003), operational risk is ‘the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events’. Although this definition is mostly used in the financial world, all organisations are exposed to operational risks (Viney, 2005). There are four main sources of operational risk for any organisation: business processes, technology, people and the environment (Birchall et al., 2004). Organisations need to manage their risks following their risk appetite (COSO, 2004) in a coordinated manner to address current global complexity (OECD, 2003 and Ernst&Young, 2005), regulations (Proctor, 2005; Booker, 2006 and Rybczynski, 2006) and to obtain defined benefits. However, many have been managing risk in silos with little common understanding, few common reporting tools and no common risk language when dealing with the diverse risk fields in the organisation such as strategic risk, market risk, credit risk, operational risk and reputational risk (adapted from Aabo et al., 2004). This has also been the case for information security: physical security, business continuity, insurance risk & operational risk (Birchall et al., 2004). Yet there are increasing needs to follow meaningful (systematic and repeatable) risk models (Alvarez, 2005; Hughes, 2005) and adopt comprehensive and transparent policy to develop risk management in the organisation (Giraud, 2005). To achieve this development it is necessary to ensure that operational risk is no longer dealt within silos, for instance through the creation of a full-time executive office with the overarching authority to develop and implement risk management procedures enterprise-wide (Leskela et al., 2005). Other practical suggestions in the literature to move away from silo operational risk management include creating communities of interests to share information about risks faced by the organization (Hamel, 2006).

2.3 Strategic alignment

There is an increasing body of academic literature and practitioner opinion suggesting that Information Security is a strategic undertaking. A strategic approach transforms information security into a business enabler that can help organisations compete (Thompson, 2005). As a consequence, executives draw their attention to ensure that Information Security is aligned with the organisation’s strategy (ISO, 2005). This stems from three reasons:

- Increasing difficulty for any organisation to achieve its strategic objectives if its Information Security is lacking in any way. This is because Information Security is the cornerstone of business continuity and customer confidence (DTI, 2004; Ezingard, McFadzean & Birchall, 2005).
- Information is one of the most significant assets in today’s organisations. In addition, most of the organisation’s information depends on information

technology (Coles & Moulton, 2003; Aabo et al, 2004; ISO, 2004 and Alvarez, 2005) and their security is therefore paramount.

- Compliance requirements for many organisations require them to have a robust Information Security in place (Lin, 2006). Increasingly there is a convergence between risk assessment and corporate governance (Power, 2004)

Despite these reasons, there is evidence that the alignment between Information Security and Organisational Strategy is not always achieved. This has been a concern in the literature for some time (see e.g. Kovacich, 2001; Von Solms, 2001). Boards and senior executives still take little sustained interest in the matter (Dutta and McCrohan, 2002; IAAC, 2003). In many organizations Information Security has been implemented as a process. Typically the stages in this process concern risk identification, risk classification (in terms of impact and probability) and risk mitigation or avoidance. Whilst treating Information Security as a process is now seen as good practice, the approach is very ‘functionalist’ (McFadzean et al., 2007) and can easily be seen as lacking completeness (if not linked with the overall strategy) because of its potential to be misaligned with an overall strategic picture.

3 RESEARCH DESIGN

3.1 Development of analytical themes and research model

The review of the literature has shown that there is potentially a link between (1) Achieving success in Information Security, (2) Management Processes and Accountability and (3) Strategic Alignment with the possibility for organisations to obtain superior benefits. Three hypotheses are derived from this link: H1: Strong management commitment to Information Security has a positive impact on transforming Information Security into a business enabler (providing benefits to the organisation). H2: Developing Information Security as a part of an integrated Risk Management approach is beneficial to the organisation. H3: Alignment between Information Security, business strategy and culture provides benefits to the organisation.

3.2 Development of survey instrument and unit of analysis

In order to investigate the three hypotheses given above we developed a quantitative approach. We designed a survey to investigate how current information security practices bring tactical, strategic and organisational benefits (Ezingeard et al., 2005). The instrument included 6 open questions and 38 closed statements measured on a Likert scale. The survey covered four main themes and a total of 9 constructs, as explained in table Table 3-1. It is available from <http://securityandrisk.blogspot.com>.

| Themes | Constructs | Question sources |
|---|---|---|
| Theme 1 (6 questions + 3 statements) Demographic questions and Management practices | - Demographics and unit of analysis. - Complexity of Information Technology environment. | Straub and Welke (1998) Venkatraman (1994) Ezingard et al. (2004) Aabo et al. (2004) ISO (2004) |
| Theme 2 (5 statements) Risk Management and Corporate Governance practices | - Degree of development of enterprise-wide approach to Risk Management. - Influence of Corporate Governance on Information Security. | COSO (2004) Aabo et al. (2004) |
| Theme 3 (14 statements) Information Security practices | - Management commitment. - Degree of development in Information Security. -Degree of development in Operational Risk Management. | ISO (2004), COBIT (2000) ISF (2005a) Soo Hoo (2000) |
| Theme 4 (16 statements) Benefits | - Business benefits - Strategic alignment | Birchall et al. (2004) |

Table 3-1. Survey constructs.

The questionnaire was administered online to Information Security and business professionals and resulted in 82 valid returns. Over 63% of respondents work in the information security or IS security field. Close to 60% of survey participants have more than 3 years experience in their current position. 68% of respondents come from the Information Technology field. Although more than 30% respondents still report to the CISO, almost 20% of respondents report to the organisation's CEO or Board. About 40% of respondents influence between 100 to 1000 employees. More than 50% of respondents work in the financial sector. Scale reliability was tested using Chronbach's Alpha. Themes with a high number of individual statements provided alpha values higher than or close to 0.7. In the survey, 0.62 was the alpha cut-off value to constitute composite variables. The constructs 'complexity of IT' and 'strategic alignment' resulted in alpha values lower than the proposed cut-off figure. Consequently, statements included in those two constructs were individually analysed to warrant inclusion in the analysis.

4 FIELDWORK RESULTS

4.1 Information Security Practices – critical success factors

As discussed in 2.1, two groups of Critical Success Factors emerge from the literature for Information Security Practices: *Management Processes and Accountabilities*, and *Alignment*. The picture that emerged from the survey around the first theme is a mixed one. As explained in the literature review, 'best practice' management processes revolve around clear

risk identification and ownership and clear lines of accountability (COSO, 2004 and ISO, 2005 among many others). In terms of risk identification, only 50% of the surveyed organisations perform risk analysis based either on business impact or threat and vulnerability analysis. In almost 70% of the total of cases, information owners receive their risk analysis, although in 44% of the occasions, they don't have an active role accepting or mitigating risks. In 58% of the cases the security policy is not communicated to all employees. In 75% of the cases an executive committee is accountable for implementing information security controls and only in 23% of the cases does an executive committee have an overall accountability for information security. The second theme that emerged from the literature review is that of silos and integration barriers. Here, only 40% of answers show collaboration between information security and IS security. Just in 22% of the cases the acceptable risk policy statement is documented and even less than a lower percentage of respondents, 20%, have access to this acceptable risk policy statement. However, a promising 61% of respondents received a general risk acceptance message from management.

4.2 Benefits

As discussed in the literature review, a clear understanding of the benefits from Information Security is important for any Information Security programme. Making the case for Information Security investments can be difficult as the scope of benefits is wide. Table 4-1 provides a ranking of benefits according to the agreement percentages obtained in the survey. An interesting remark is that the top three benefits quoted are high order benefits. This could be explained by the fact that our respondents are drawn from the Information Security community and are therefore potentially biased towards describing the impact of their role or their function on the organisation as more important than it actually is. Nonetheless, it is interesting to notice that the 'reach' of Information security good practice is increasingly seen as wide.

| Type | Information security benefit | % agree |
|----------------|-------------------------------|---------|
| Organisational | Increased stakeholder value | 62 |
| Tactical | New business opportunities | 61 |
| Strategic | Better governance | 55 |
| Tactical | Partner and customer loyalty | 55 |
| Strategic | Lower costs | 54 |
| Organisational | Competitive advantage | 51 |
| Strategic | Improved financing capability | 44 |
| Tactical | Easier compliance | 40 |
| Strategic | More sales | 38 |
| Tactical | Improved operations | 33 |

Table 4-1. Benefits ranking.

In order to verify the type of relationship between the benefits quoted by the respondents and Information Security practice, we calculated the correlation between the level of Information Security development and these benefits (we used Pearson's correlation). The results are shown in Table 4-2. There is a significant and fairly strong positive correlation between information security development and benefits for the organisation. Therefore, we can

conclude that the benefits listed in Table 4-1 are indeed associated with Information Security developments.

| Pre-condition | Benefits | Correlation | Sign. level |
|----------------------------------|---------------------------|-------------|-------------|
| Information security development | Tactical & Strat benefits | 0.673 | 0.01 |
| | Organisational benefits | 0.750 | 0.01 |
| | All benefits | 0.772 | 0.01 |

Table 4-2. Correlation for the development of information security.

4.3 Hypothesis testing

Each of the three hypothesis given in 3.1 was tested using Pearson's correlation. The results are shown in Table 4-3, Table 4-4 and Table 4-5

| Pre-condition | Benefits | Correlation | Sign. level |
|-----------------------|---------------------------|-------------|-------------|
| Management commitment | Tactical & Strat benefits | 0.734 | 0.01 |
| | Organisational benefits | 0.709 | 0.01 |
| | All benefits | 0.792 | 0.01 |

Table 4-3. Correlation for management commitment.

| Pre-condition | Benefits | Correlation | Sign. level |
|---------------------------|---------------------------|-------------|-------------|
| Risk management processes | Tactical & Strat benefits | 0.656 | 0.01 |
| | Organisational benefits | 0.495 | 0.01 |
| | All benefits | 0.644 | 0.01 |

Table 4-4. Correlation for the development of risk management processes.

| Pre-condition | Benefits | Correlation | Sign. level |
|---|---------------------------|-------------|-------------|
| Strategic alignment in information security | Tactical & Strat benefits | 0.449 | 0.01 |
| | Organisational benefits | 0.371 | 0.01 |
| | All benefits | 0.456 | 0.01 |

Table 4-5. Correlation for the strategic alignment in information security.

5 CONCLUSIONS AND RECOMMENDATIONS

We have, so far, established that the development of information security (for instance, establishing an information security programme to improve security management enterprise-wide, as proposed by ISF, 2005b) can be linked to achieving organisational, strategic and tactical benefits. Organisations with an evolved Information Security practice (i.e. supported by management, mature and integrated in enterprise risk management processes) provide increased value to their stakeholders. Equally, organisations taking care of Information Security enjoy new business opportunities and show better compliance with current regulations. In summary, the three most common benefits (following the benefits framework from Ezingard et al., 2005) identified by the fieldwork are value increase to stakeholders, new business opportunities and better compliance. The literature suggests that a requirement to achieve these benefits is management commitment to develop a strong Information Security practice (ISO, 2004 and 2005; COSO, 2004; Appel, 2005 and Ezingard et al., 2004 among many others). The study presented here has shown this to be the case with the strongest correlation between management commitment and the achievement of *tactical and strategic* benefits. Other high level organisational benefits are also strongly correlated with management commitment to Information Security. This suggests that there is potentially a 'virtuous circle' in existence where management commitment to Information Security helps achieve success in Information Security that in turns helps achieve business benefits. Our study also shows that achieving this 'virtuous circle' seems to be dependant on the transparent integration of risk management processes, as suggested by the reviewed literature (Alvarez, 2005; Hughes, 2005 and Giraud, 2005). The results of the survey show that integrated risk management processes are, indeed, strongly correlated to achieving most of the benefits associated with Information Security. Interestingly, the link between benefits and the alignment of information security with the strategy of the organisation is not as strong as suggested by the literature (Birchall et al., 2004 and ISO, 2005). Although the correlation is significant, it is lower than many of the other correlations we observed. This suggests that the link between the two constructs exists but that the alignment by itself does not explain much of the benefits. Further statistical testing will be necessary to determine whether in fact alignment is a mediating or moderating variable in the other relationships we observed. This study has a number of implications for managers. Information Security can lead to business benefits for organisations that go beyond technical benefits. However, to achieve these benefits, strong commitment from managers and attention to the detail of the Information Security practices is needed. In addition, our study indicates that managers should increasingly regard Information Security as part of a wider Operational Risk management framework to ensure that business benefits are achieved. For many organisations this could have significant organisational implications, meaning that reporting lines may need to be changed. Potentially, this could create the need for new interfaces between the IT Security function and Operational Risk management as we know from the literature that the creation of silos is often counter productive for the implementation of a risk management framework.

References

- Aabo, Tom, Fraser, John R.S., Simkins, Betty J. (2004). The rise and transformation of the chief risk officer: a success story on enterprise risk management. Version of December 10, 2004. Revised version available in Journal of Applied Corporate Finance, Winter 2005. Pages 1-34, Available from: <http://www.gloriamundi.org/detailpopup.asp?ID=453057237> [Accessed 16 April 2006]
- Akella, Janaki, Kanakamedala, Kishore and Roberts, Roger P. (2007). What's on CIO agendas in 2007. McKinsey Quarterly web-exclusive, January 2007.
- Alvarez, Gene (2005). 'An Operational Risk Management Framework'. Chapter 11 of the book titled 'Operational Risk: Practical approaches to implementation'. Edited by Ellen Davis. Risk books. Pages 227-236.
- Appel, Willie (2005). 'Redefining IT Governance Readiness', Meta Group, Meta Practice 2369. Pages 1-8.
- Ashenden, D. & Ezingard, J.-N. (2005) The Need for a Sociological Approach to Information Security Risk Management. 4th Annual Security Conference. Las Vegas, Nevada, USA.
- Basel Committee on Banking Supervision. Risk Management Group. Cole, Roger (chairman) et. al. (2003). 'Sound practices for the management and supervision of operational risk', Bank for International Settlements (BIS). Pages 2-5 and 8.
- Birchall, David, Ezingard, Jean-Noël and McFadzean, Elspeth (2003). Information security. Setting the boardroom agenda. Grist and Henley Management College sponsored by Qinetiq. Executive summary also referenced. Pages 1-51.
- Birchall, David, Ezingard, Jean-Noël and McFadzean, Elspeth (2004). Information assurance. Strategic alignment and competitive advantage. Grist and Henley Management College sponsored by Qinetiq. Executive summary also referenced. Pages 1-73.
- Booker, Robert (2006). 'Re-engineering enterprise security', Computers & Security 25. 13-17.
- COBIT. IT Governance Institute (2000). 'Control objectives for information and related technologies' COBIT, 3rd edition. Pages 1-12.
- Coles, Robert S. and Moulton, Rolf (2003). 'Operationalizing IT risk management', Computers & Security 0167-4048/03. Pages 487-492.
- Committee of Sponsoring Organisations of the Treadway Commission COSO (2004). Enterprise Risk Management Framework – Executive summary – Exposure Draft for Public Comment (pages 1-103) downloadable from www.coso.org/publications.htm
- CSI/FBI (2006). 11th Annual CSI/FBI computer crime and security survey. Computer Security Institute, 2006.
- DTI (2004). "Information Security Breaches Survey," DTI and PriceWaterhouseCoopers.
- Dutta, A., McCrohan, K. (2002), "Management's role in information security in a cyber economy", California Management Review, Vol. 45 No.1, pp.67-87.
- Ernst&Young (2005). Ernst & Young's 8th annual Global Information Security Survey [online]. Pages 1-28. Available from: http://int.sitestat.com/ernst-and-young/international/s?Global-Information-Security-survey-2005&ns_type=pdf [Last accessed 8 May 2006]. Press release Available at http://www.ey.com/GLOBAL/content.nsf/International/Press_Release_-_2005_Global_Information_Security_Survey [Last accessed 8 May 2006].
- Ezingard, J.-N., McFadzean, E. and Birchall, D. (2005) A model of Information Assurance Benefits. Information Systems Management, 22, 20-29.
- Ezingard, J.-N., M. Bowen-Schrire, et al. (2004). Triggers of Change in Information Security Management. ISOneWorld Conference, Las Vegas, Information Institute (<http://www.information-institute.org/>). Pages 1-37.
- Giraud, Jean-Rene (2005). 'Managing hedge funds' exposure to operational risks'. Chapter 14 of the book titled 'Operational Risk: Practical approaches to implementation'. Edited by Ellen Davis. Risk books. Pages 275-283.
- Hamel, Gary (2006). 'The Why, What and How of Management Innovation'. Harvard Business Review. February 2006. Pages 1-12.
- Hughes, Peter (2005). 'Using transactional data to measure operational risk'. Chapter 1 of the book titled 'Operational Risk: Practical approaches to implementation'. Edited by Ellen Davis. Risk books. Pages 3-12.
- Information Assurance Advisory Council (2003), Engaging the Board: Corporate Governance & Information Assurance, Information Assurance Advisory Council, Cambridge. IAAC (2003).
- Information Security Forum ISF (2005a). December 2005, Improving Security Management. Enterprise-wide. Reference ISF 05-053. Pages 1-46.

- Information Security Forum ISF (2005b). The Standard of Good Practice for Information Security. Reference ISF 05-104. Pages 1-28.
- Information Security Forum ISF (2005c). Disappearance of the Network Boundary. April 2005. Reference ISF 2005-04-02. Pages 1-25.
- ISO (2004). ISO/IEC 13335-1 Information technology – Security techniques – Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management. Reference: ISO/IEC 13335-1:2004(E). Pages 1-28.
- ISO (2005) ISO/IEC 17799 Information technology – Security techniques – Code of practice for information security management. Second edition 2005-06-15. Reference: ISO/IEC 17799-1:2005(E). Pages 1-115.
- Kovacich, Gerard L. (2001). The Corporate Information Assurance Officer (CIAO). *Computers & Security* 20(4): 302-307 (2001).
- Leskela, Lane; Knox, Mary; Schehr, David; Furlonger, David; Redshaw, Peter (2005). 'Client issues 2005: How to achieve regulatory compliance and ERM', Gartner, Research note. 29 March 2005. ID Number: G00126561. Pages 1-4.
- Lin, P. Paul (2006). System Security Threats and Controls. *The CPA Journal*. New York: Jul 2006. Vol.76, Iss. 7; pg. 58, 8 pgs.
- McFadzean, E. Ezingear, J.-N. and Birchall, D. (2007). Mastering the art of corroboration: A conceptual analysis of information assurance and corporate strategy alignment, *Journal of Enterprise Information Management*, vol 20, issue 1, p96-118.
- May, Cliff (2002). 'Risk Management – Practising what we preach', *Computer Fraud & Security*, 8: 10-13.
- Organisation for Economic Co-operation and Development (2003). Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security. Working Party on Information Security and Privacy. 2 July 2003. Pages 1-6.
- Power, M. (2004). The risk management of everything: rethinking the politics of uncertainty, London, Demos.
- PriceWaterHouseCoopers, 2006. The global state of Information Security.
- Proctor, Paul (2005). 'Security and Risk Compliance Overview. Security & Risk Strategies, Security Infusion', Meta Group, Meta Practice 2339. Pages 1-7.
- Rybczynski, Tony. Podcast from Wharton titled 'Security, Business Continuity and the 'Real-time Virtual Enterprise' interviewing Tony Rybczynski (director of strategic marketing and technologies for Nortel)[online]. Available from: http://knowledge.wharton.upenn.edu/audio/WTC_RybczynskiINT.mp3 [Last accessed 5 May 2006].
- Scholtz, Tom (2004a). 'Articulating the Business Value of Information Security. Security & Risk Strategies, Security Infusion, Global Networking Strategies', Meta Group, Meta Delta 2774. Pages 1-4.
- Scholtz, Tom (2004b). 'META Group Information Security Services Framework Update: Version 3: Enterprise Planning & Architecture Strategies, Security & Risk Strategies, Security Infusion', Meta Group, Meta Delta 3137. Pages 1-6.
- Scholtz, Tom (2004c). 'Organising for security: trends and best practices. Executive directions, security and risk strategies, security infusion'. Meta Practice. 27 July 2004. Practice 2223. Pages 1-8.
- Soo Hoo, Kevin J. (2000). 'How much is enough? A risk-management approach to computer security' Consortium for Research on Information Security and Policy (CRISP) Working paper. June 2000. Pages 1-6 and 15-20.
- Straub, D. W. and R. J. Welke (1998). "Coping with systems risk: Security planning models for management decision making." *MIS Quarterly* 22(4): 441-469.
- Thompson, John with Martin, Frank (2005). Strategic management. Thomson 5th edition. Key success factors and E-V-R congruence. Pages 114 and 125-130.
- Venkatraman, N. (1994). "IT-Enabled Business Transformation: From Automation to Business Scope Redefinition." *Sloan Management Review* 35(2): 73-87
- Viney, Christopher (2005). 'Model behaviour'. Chapter 9 of the book titled 'Operational Risk: Practical approaches to implementation'. Edited by Ellen Davis. Risk books. Pages 201-214.
- Von Solms, B. (2001), "Corporate governance and information security", *Computers & Security*, Vol. 20 No.3, pp.215-8.
- von Solms, Basie (2005a). 'Information Security Governance: COBIT or ISO 17799 or both?', *Computers & Security* 24, 99-104.
- Whitman, M. E. & Mattord, H. J. (2003) Principles of information security, Boston, Mass.; London, Thomson Course Technology.