2014

The impact of social constructivism on ERP systems security: A critical social review

Kennedy Njenga
University of Johannesburg, knjenga@uj.ac.za

Recommended Citation

Njenga, K. (2014). The impact of social constructivism on ERP systems security: A critical social review.
DOI: https://doi.org/10.4225/75/57b65e7b343d2

DOI: 10.4225/75/57b65e7b343d2

12th Australian Information Security Management Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

THE IMPACT OF SOCIAL CONSTRUCTIVISM ON ERP SYSTEMS SECURITY: A CRITICAL SOCIAL REVIEW

Kennedy Njenga
University of Johannesburg, Department of Applied Information Systems, South Africa
knjenga@uj.ac.za

Abstract

Little is understood about the effects of social constructivism that shapes conflicting concerns regarding Enterprise Resource Planning (ERP) security and usability during implementation. This work looks at social constructivism as produced and reproduced by stakeholders in the ERP systems implementation phase. Social constructivism is characterised by the embedded trade-off for usability, espoused by end-user and security, espoused by developers. Social constructivism was conceptualised qualitatively from a selected case study. Critical Social Theory (CST) was used as the theoretical lens. Stakeholders concerned with ERP security aspects in the implementation phase were interviewed and data transcribed and interpreted. Hermeneutical interpretation was applied towards understanding social constructivism. Exegesis techniques used include textual criticism and reduction criticism. The contribution of the work is twofold: the work provides insights regarding ERP systems security by attempting to explain how social constructivism shapes outcomes of ERP security; the article also shows how hermeneutics could be applied in the discipline of information systems security. Findings for this case reveal that social constructivism does shape ERP security in insightful ways.

Keywords
ERP Systems, security, usability, social constructivism

INTRODUCTION

Developers of secure information systems have increasingly created highly complex artefacts that are almost entirely automated. Because Enterprise Resource Planning (ERP) systems usually integrate entire business operations, these systems have complex security needs (Brdys , 2014; Ho *et al*., 2004). ERP systems are centrally bound and constructed by a processes of planning and *cybernetic control* (Teittinen, Pellinen and Järvenpää, 2013). The implementation phases in ERP systems have been identified as critical to information security (Choobineh *et al*., 2007). The concern is that implementation transcends technical aspects such as software design and is seen as a social constructive endeavour that is greatly influenced by conflicting mental models of key stakeholders.

Proper implementation of complex security systems has been dependent on the support extended by end-users who are perceived as weak links to security (Warkentin and Willison, 2009). Users with enough influence may strengthen the argument for usability against security complexity. Stakeholders such as developers with enough influence may equally strengthen the argument for security complexity against usability. Therefore on one hand, there is conflicting interests by stakeholders towards a push to make systems secure which ultimately makes operations harder to do, while on the other hand, users will ultimately require easier operations which might compromise security. Social constructivism is therefore contextualised by embedded trade-off for *usability* and *security*.

The research is therefore keen to examine the *usability* and *security* trade-off using a qualitative approach. Emphasis is given to how social constructivism is manifested. This is significant considering that many research studies indicate that the success of ERP implementation projects and information security is impacted by social constructive dynamics (Doherty and Fulford, 2005). According to Baskerville, (2005) organisations usually concentrate on the technical side of security and do not pay enough attention to social constructive factors.

Little is understood about the effects of pre-implementation and implementation mental-models that shape stakeholder interests and the imprint on systems security. The research question would then be; how does social constructivism manifest and impact ERP systems security during ERP implementation? It is the purpose of this research to develop a basis for addressing this question and understanding the imprints. The move towards increasing research on the conceptualisation of social constructive perspectives in Information Security is fully understood and encouraged amongst information security researchers (Dhillon, 2004).

The following section introduces key concerns regarding ERP systems security from various perspectives. The next section discusses the social constructive contexts and uses Social Critical Theory as a theoretical lens. The penultimate sections discuss the methodology and finally conclusions are then addressed.

ERP SYSTEMS SECURITY

Stakeholders #1: End-users as endpoint threats

Research suggests that the greatest threat to many organisations' ERP systems has never been from external sources such as hackers, malware, virus or worms but rather from end-users with different mental models regarding security needs of an organisation (Van Holsbeck and Johnson, 2004; Turban et. al., 2002; Stair and Reynolds 2008). Each end-user characterises an endpoint of the organisation's ERP, and without security-compliant mental models that leads to desired use, there can be no organisational ERP security. Desired end-user activities within ERP environments would constitute end-users changing passwords, making regular back-up, creating password protected screen savers and other activities identified by Whitman (2003). Notably, end-users will designate (often on their own terms) which activities are desirable with their primary action in the ERP user interface. When an ERP system correctly and accurately interprets end-user activity, it becomes possible for such a system to place accurate authorisation protocols for this activity. ERP security is enhanced if assigned protocols match intended systems use (Yee, 2004). The problem occurs when the ERP system cannot determine whether the end-user activity and result is desirable. This may come about when end-users are presented with security as a secondary task which impedes on usability because the end-user will interface with the ERP for other purposes than security (Yee, 2004). The mental model for the end-user as ERP endpoints is that security (such as warning prompts and security alerts, making back-ups, constantly changing passwords and encountering website filters) becomes interruptive and obstructive to their main purpose of interfacing with ERP systems. This can lead to end-users dismissing ERP security prompts and alerts hastily or casually.

Stakeholders #2: ERP Designers as threats

ERP systems are designed to tightly integrate business processes across an organisation (Brdys, 2014; Van Holsbeck and Johnson 2004; Sprecher, 1999). Controls protect ERP systems against theft, data tampering, information extortion, espionage, trespass, human error and human failure (Stair and Reynolds, 2008;Turban *et. al.*, 2002), and are necessary to ensure that tasks are performed completely and accurately, and that no unauthorised changes to the input take place (Von Solms and Von Solms, 2004). Hendrawirawan *et al*., (2007), state that sometimes controls are not implemented during ERP implementation phase due to the fact that the complexity of ERP systems '*makes security configurations very complex'*. Good usability engineering requires developers to understand end-user needs and incorporate appropriate and necessary features throughout the design process. These features should not be superficial (flashy widgets, animations and skins) but those that take cognisance of risks and the associated vulnerabilities (Brdys, 2014; Yee, 2004; Whitman and Mattord, 2003; Devenport, 1998). Modern integrated systems (termed Critical Infrastructure Systems) development requires not only understanding user needs but also strengthening controls. Brdys (2014) looks at current operational conditions of these systems and proposes the use of predictive control technology with elements of 'soft switching' mechanisms that appropriates different control strategies for different users. ERP security has often been perceived as "*bolting security onto an existing system*" which according to Viega and McGrew (2002:14) "*is simply a bad idea*". The idea is ERP systems are already built and characterised by "*configuration settings and prompts*". Research has noted the extra bolts, i.e., extra fixes "*just make it easier to blame end-user error when something goes wrong*" (Yee, 2004:14). If controls and security features are just 'bolts' on usability, instead of being incorporated into ERP systems from ground-up, security will ultimately suffer (Yee, 2004).Common in ERP systems is usability 'quick-fixes' such as hiding security related decisions in the background and away from end-users or choosing lax default settings. In such cases, security and control measures must be iterative and implemented as a part of the ERP design. Such measures are illustrated by **Figure 1** below.

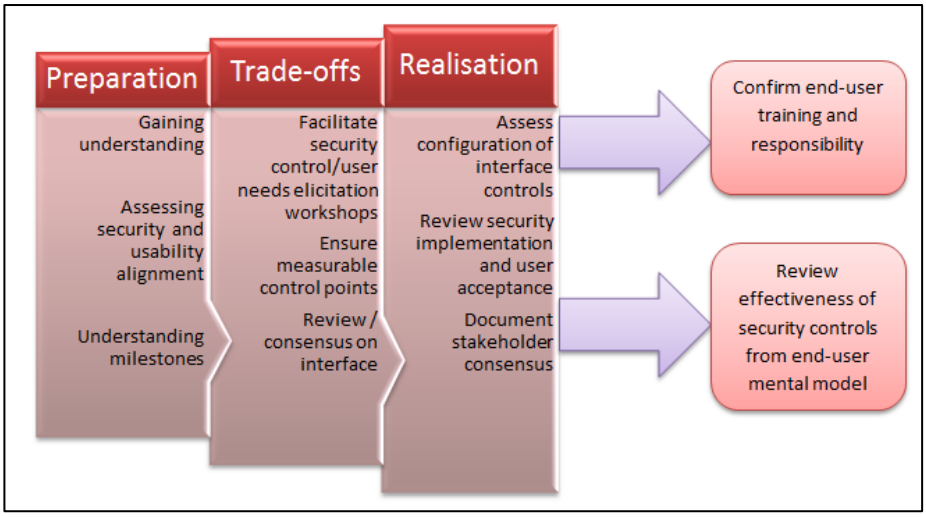

Figure 1: Security complexities and ERP Implementation

Social constructivism and vested interests: Stakeholder #1 and #2 trade-offs

Social constructivism applies constructivism in social settings and examines groups in their social contexts wherein these groups construct knowledge and are collaborative in creating '*shared artefacts'* with '*shared meaning'*. When it comes to ERP systems security, it is of essence to understand experiences of stakeholders such as end-users of ERP systems and developers of these systems and how they socially construct different meanings towards a negotiated trade-off regarding ERP security issues. Based on discussions from previous sections, these negotiated trade-offs may result from an attempt to align, in this case, usability concerns *vis-à-vis* security complexities as highlighted from **Table 1** below.

Common Usability concerns	**Common ERP Security concerns**					**Mapping Misalignment of usability and security** *inputs for negotiated social constructive process for stakeholders #1 and #2*
	Prompts	Alters/ Warnings	Back-ups	Authent-ication and Passwords	Website filters	
Communication	✸	✸				*Reduces effectiveness*
Use of Online services	✸	✸			✸	*Hidden processes, limits workflow*
Time management			✸	✸		*Interruption*
Composition/Editorial	✸	✸				*Interruption*

Table 1: Negotiated Trade-off between Usability and Security of ERP

Social constructivism for purpose of this work focuses on the negotiated elements for usability and security from stakeholders. This is based on the mental models wielded by stakeholders and the understanding of security requirements. For instance **Table 1** above shows that the primary need for communication by end-users is paramount and that the more security features placed on an ERP system, the greater the perception that security *reduces the effectiveness* to communicate in a way desired by the end-user.

By focussing on social constructivism as it manifests during ERP implementation, it is easier to understand how security issues are managed and how effective such a management process is (Baskerville, 2005; Dhillon and Backhouse, 2001; Straub and Welke, 1998). A number of researchers are of the opinion that social constructive factors are critical to the success of ERP implementations than technical or economic factors (Alvarez and Urla, 2002; Wood and Caldas, 2001; Markus e*t al*., 2000; Ein-Dor and Segev,1982). From a social constructivism perspective, stakeholders' social '*engagements*' would entail power structuring and social exchanges (Huysmans, 2002). The dilemma here would be the sensitivity of stakeholders towards what is central in their mental models regarding security and usability concerns. One way of avoiding conflict in engagement process

from social constructivism approach, is that social constructivism helps seek ways to elicit and use as much accurate information from the end-user's normal interaction with the ERP interface.

Critical Social Theory

Critical Social Theory (CST) may be used as a conceptual lens to understand the engagements regarding usability and security. CST has been put forward as an alternative to traditional approaches to Information Systems research and practice (Ngwenyama 1991) and focuses on the improvement of the human condition by conceptualising social organisation. CST takes into account social constructivism (construction of life and reaction) and is concerned with finding "*alternatives to existing social conditions which more adequately address human desires*". CST "*focuses on the emancipation of individuals and the human species in general*" (Ngwenyama, 1991:2). This research therefore takes CST and grounds the social constructivism for ERP concerns with the following assumptions; (Ngwenyama, 1991:2)

(1) Stakeholders concerned with ERP needs for security and usability are creators of their social worlds and as such can change it if they wish;
(2) Knowledge about the social context to which these stakeholders exist is socially constructed.

METHODOLOGY

This section builds on the previous sections and describes the methodology employed in order to understand the negotiated trade-off between usability and security from stakeholder perspectives. An explanatory case study was used to understand social constructivism in context of this trade-off (Yin, 1994). Explanatory single cases *seek to link an event with its effects and suitability* (Yin, 2003). A important difference between case studies and any other alternative method is that the case study researcher may have less *a priori* knowledge regarding variables of interest (Benbasat *et al.*, 1987). The case was selected because of its size (medium enterprise with over ninety employees) and that it was in the process of rolling out an ERP system. Another justification for selecting this case is that the phenomenon (of social constructivism) could be examined in its natural setting, and that it was possible to collect data by multiple means (Benbasat *et al*., 1987).

The ERP roll-out had executive approval and incorporated three middle-level department heads from marketing, finance and administration (stakeholders **#1**). In addition to these three, the researcher also focused on a core team of three selected persons from the organisation's Information Technology (IT) department (judgmental sampling) that were part of the implementation. The team members in IT included the project leader and two systems analysts (stakeholders **#2**). The IT department was responsible for coordinating secure distribution of real-time channels for its critical applications. Since the organisation offered financial services, it placed importance on working within a strict regulatory environment. In total six interviews were carried out involving the six representatives. Interviews lasted at least one and half hours. The interviews were semi-structured and prodding was used for clarification.

This work reports on the first phase of data collection which involved preliminary interviews of six representatives (stakeholders **#1** and **#2**). Observation techniques were also employed to examine manifestation of social constructivism. The observation protocol used was a structured template that denoted the following elements; location, start and end times, activity observed and researcher memo regarding understanding of what was observed. Observation took one week to complete.

The organisation's representatives (stakeholders **#1** and **#2**) were asked to recall and relate their experience of the implementation process. The researcher applied the CST framework to understand social constructivism for usability and security of ERP systems from stakeholder **#1** and **#2** perspectives. It was observed that on one hand, the three management representatives (stakeholders **#1**: marketing, finance and administration) were concerned with usability while on the other hand the core IT team (stakeholders **#2**) was concerned with controls. The researcher used the CST framework to understand the reflections, decisions, actions and experiences of stakeholders **#1** and **#2** using the qualitative paradigm. This is shown by the **Figure 2** below.

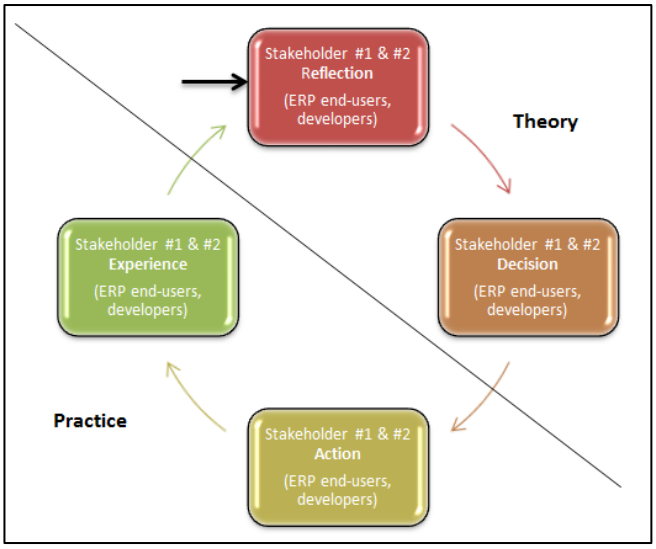

Figure 2: Negotiated Trade-off between Usability and Security of ERP

The next section explains how the researchers went about understanding social constructivism based on the above CST framework and the meaning behind what was said by stakeholders **#1** and stakeholders #2 (textual interpretation).

Hermeneutical interpretation of meaning

Philosophical hermeneutics (Gadamer 1976), has primarily focused on the act of interpretation as exemplified by Heidegger (1962), who saw interpretation as a primary mode of human existence. Hermeneutics is popular in application and use in Information Systems research (Borland, Newman and Pentland 2010). While hermeneutics refers to the theory of interpretation, exegesis applies the techniques for doing the interpretation. Within the hermeneutical circle, there are two realms to consider; the textual realm (*applying textual criticism to text)* and the social realm (*applying context to text, termed redaction criticism)*. The exegetical techniques employed from the transcripts was thus twofold; namely that of *textual criticism* and that of *redaction criticism* (Borland *et al.* 2010).

The researcher transcribed the recordings and started "engaging the data" (*textual and redaction criticism)* using a hermeneutical approach described above. The researcher started by looking for elements of *social constructivism.* Data was fractured or "compartmentalised" into cells for analysis and traces of *social constructivism*. The compartmentalisation process involved breaking down data. The process of breaking down and analysing the data and assigning labels is described as *content analysis* by researchers (Glaser and Strauss 1967).

The following table **(Table 2)** shows the preliminary approach taken towards understanding how hermeneutic exegesis was applied to explain trade-offs in social relations as practitioners exchanged ideas during implementation.

Content analysis of Data (Qualitative) *Compartmentalised into cells*	**STEP 1 Textual Criticism** This step involved, critically examining texts that the researcher transcribed from the recollection of developers and end-users regarding the implementation process.	**STEP 2 Hermeneut Metrics on Social constructivism** This step involved coding based on an understanding of the context of *social constructivism* (the recollection) regarding *security* and *usability* as and when these affected ERP implementation and consequently, ERP systems security.	**STEP 3 Reduction criticism: Interpretation and creation of concepts** This involved understanding contextual meaning.	**CST framework Application** **Researcher's memo**
Cell 1 *"…so we had to make [create] a few more categories…so it doesn't just get as simple as you just having access ..and you don't get this.. [but rather] you having access and you belong to marketing…and you belong to IT…"*	Concern regarding placing controls for access (stakeholders **#2) –** reflecting on action. <u>Examples from cells</u> **Cell 1**: creating control adjustments (*so we had to make [create] a few more categories)* **Cell 2**: Revisiting control adjustments (*we got hundreds and hundreds of calls…saying they couldn't get through)*	**Key codes:** • *'we had to'* • *'we did and worked on what they said'* It was not easy to create controls while at the same time enable unmonitored access by marketing department. The fact that IT was inundated with 'hundreds and hundreds' of calls forced them to rethink the best way to effect controls. The 'calls' were considered an element of social constructivism and was interpreted as so by the researcher.	Marketers required access for research based work (stakeholders **#1)** **Observation data** The marketing research work needed to be done (usability). This was confirmed by the marketing manager	***Action and Experience*** Through social constructivism, stakeholders **#2** were able to accommodate needs of stakeholder **#1**(Marketers). Both stakeholders were able to recognise that *they are creators of their own world.*
Cell 2 "*…and we did and worked on exactly what they said.. and of course within the first few days.. of putting access controls in [the system]…we got hundreds and hundreds of calls…saying they couldn't get through".*				***Reflection and Decision*** Both stakeholders were aware about the contexts of the issues faced and this would eventually influence the decisions they arrived at towards accommodating each other's needs.

Table 2: Hermeneutic Exegesis on manifestation of social constructivism during ERP implementation

Traces of *social constructivism* (elements of social negotiation between stakeholder **#1** and stakeholder **#2**) were noted in researcher's memos (Step 2). Observation data, data from stakeholder **#1** and stakeholder **#2** was compared (constant comparative analysis) so that the meaning of what was said would be understood in context.

DISCUSSION

From the interview session, it was highlighted that an end-user (stakeholder **#1)** expressed concern regarding controls in ERP with comments such as; *Why is the computer stopping me from accessing this module [feature]?* It was clear that the end-user did not fully appreciate "*visibility"* controls. The negotiated 'trade-off' as reflected by a systems analyst (stakeholder **#2)** was transcribed as follows**: "***we had to make [create] a few more categories…so it doesn't just get as simple as you just having access and you don't get this...[but rather] you having access and you belong to marketing".* The researcher coded this as an instance of social constructivism because the marketing manager (stakeholders **#1)** confirmed that market research work needed to be done using data from modules held by finance department and analysts had to work their way around the ERP system for this to be possible. An interesting statement made by stakeholders **#2** was; "*we understand their process needs and prefer to embed these…[security] features*" inferring the need to incorporate security

decisions into end-users workflow as parts of primary tasks. The researcher's own interpretation regarding social constructivism was that there were signs that end-user stakeholders were initiating engagement regarding issues that needed consensus; questions like "*who will now be handling this*?" emphasised a clear tension and anxiety regarding what developers expected done and what end-users found inexplicable to their needs. Social constructivism also involved accommodating the other parties interests. This was evidenced by statements from stakeholders **#2** such as "*…and we did and worked on exactly what they said…and of course within the first few days.. of putting access controls in [the system]…we got hundreds and hundreds of calls…saying they couldn't get through"* and "*we know we have a task to do… but we don't want to end up confusing the user…*"

It did not come across that the end-users did not appreciate security but rather social constructivism was geared towards accommodating needs highlighted by end-users and which tended to create favourable outcomes for end-user. This reinforces arguments espoused by Critical Social Theory (CST). The next section discusses what this means to both theory and practice.

Implication to Theory

This research addresses and answers the question of how social constructivism manifests and impacts ERP systems security during ERP implementation. Qualitative data suggests that social constructivism is a negotiated construct that balances security needs and user needs through the process of social interaction. Insights provided are significant considering that there is a dearth of academic research studies that look at the social organisational complexities regarding information systems security. Much of the available literature has concentrated on the actual implementation of ERP systems and not on the complex social organisational dynamics that affect ERP system security. The study therefore adds rich insights by considering the "soft" side of ERP system security.

Implication to Practice

This paper aims to offer organisations practical ways of understanding social constructivism during ERP implementation processes and how such initiatives could be improved on particularly when better understanding is created. This paper also aims to educate practitioners on the importance of social interaction and trade-offs during ERP implementation. If social constructivism is recognised, then this would create an avenue for information security practitioners to manage the process and not be taken by surprise if for instance security proposals are discounted.

CONCLUSION

This work has provided a basis for the conceptualisation of social constructivism during ERP implementation by examining the dynamics of usability and security. Conceptualisation has been done using hermeneutical exegesis. It is hoped that the paper has provided useful and applicable insights on how social constructivism could affect ERP system security. It is hoped that such insights will assist organisations and particularly practice in the information security disciple become more effective and resolute in the role they might play during ERP implementation.

REFERENCES

Alvarez, R., Urla, J., (2002). Tell me a good story: using narrative analysis to examine information requirements interviews during an ERP implementation. *The DATA BASE for Advances in Information Systems* 33 (1), p. 38–52.

Baskerville, R. (2005) "Information Warfare: a comparative framework for Business Information. *European Journal of Information Systems*, 1(2), p.121-130.

Benbasat, I., Goldstein, D. K., and Mead, M. (1987) "The Case Research Strategy in Studies of Information Systems," MIS Quarterly Vol. 11:3 pp. 369–386.

Borland RJ, Newman M and Pentland BT (2010) ,Hermeneutical exegesis in information systems design and use, *Information and Organization* 20, p. 1–20.

Brdys, M.A., (2014) Integrated monitoring, control and security of Critical Infrastructure Systems Annual Reviews in Control 38 p. 47–70.

Choobineh, J., Dhillon, G., Grimaila, M.R., and Rees, J. (2007)"Management of information security: Challenges and research directions," Communications of the Association for Information Systems (20:1), p. 958- 971.

Davenport, T.H., (1998). Putting the enterprise into the enterprise system. Harvard Business Review, (July-August), pp. 121-131. Security", *Journal of Information System Security*, Vol. 1:1 p. 23-50.

Dhillon, G. (2004). Guest Editorial: the challenge of managing information security. *International Journal of Information Management. 24*. p. 3 – 4.

Dhillon, G. and Backhouse, J. (2001) "Current Directions in IS Security Research: Toward Socio-organizational Perspectives," Information Systems Journal 11(2). p.

Doherty, N. F., and H, Fulford. (2005) "Do Information Security Policies Reduce the Incidence of Security Breaches? An Exploratory Analysis," *Information Resources Management Journal,* 18(4) p. 21-39.

Ein-dor., P and Segev E. (1982) The ′people principle′: Successful IT implementations begin with the people it affects. *Convergence*. 4(1) p. 120-5.

Gadamer, H.G. (1976). *Philosophical hermeneutics*. University of California Press. Berkeley, CA.

Glaser, B.G., and Strauss, A.L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine Transaction: New Jersey.

Heidegger, M. (1962), *Being and time.* (J. MacQuarrie & E. Robinson, Trans.) (1st English ed.). SCM Press, London.

Hendrawirawan, D.,Tanriverdi, H., Zetterlund, C., Hakam, H., Ho Kim, H, Paik and Yoon,Y.(2007). 'ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution'. *Information Systems Journal,* (2).

Ho,C., Wu, W. and Tai, Y. (2004). 'Strategies for the adaptation of ERP systems'. Industrial Management and Data Systems, 104(3): p.234-251.

Hussey, J. and Hussey, R. (1997). *Business Research: a practical guide for undergraduate and post graduate students*. Macmillan Press.

Miranda, R. (1999). The rise of ERP technology in the public sector. Government Finance Review, August 1999, p. 9-17.

Remenyi, D., Williams, B., Money, A. and Swartz, E. (2005) *Doing research in business and management: an introduction to process and methods*. Sage Publications, London.

Russell C., and Mitchell MS. (2005), "Social Exchange Theory: An Interdisciplinary Review," *Journal of Management,* 31 (6), p. 874-900.

Sprecher, M. (1999). The future of ERP in the public sector, Government Finance Review.
Stair, R and Reynolds, G. (2008). *Fundamentals of Information Systems*. 4th ed. Thomson Course Technology.

Straub, D.W. and Welke, R.J., (1998) 'Coping with Systems Risk: Security Planning Models for Management Decision Making', *MIS Quarterly,* 22(4) p. 441-464.

Teittinen,H., Pellinen, J., and Järvenpää M. (2013) ERP in action-Challenges and benefits for management control in SME context , *International Journal of Accounting Information Systems,* 14(4) p. 278–296.

Turban, E., McClean, E. and Wetherbe, H. Bolloju, N. and Davidson, R. (2002). *Information Technology for Management: Transforming business in the digital economy.* 3rd ed. John Wiley and Sons Inc.

van Holsbeck, M and Johnson, J.Z. (2004). Security in an ERP World [Online]. Available from http://www.net-security.org/article.php?id=691&p=4 [Accessed 15 March 2010].

von Solms, B. and von Solms R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23 p. 371-376.

Viega, J. and McGrew, G. (2002) Building Secure Software, Addison-Wesley.

Warkentin, M.E., and Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat, *European Journal of Information Systems* (18:2), p. 101-105.

Whitman, M.E. (2003). "Enemy at the gates: Threats to information security." Communications of the ACM **46** (8): 91- 95

Whitman, M.E and Mattord H.J. (2003). *Principles of Information Security.* Thomson Course Technology.

Wood, T. and Caldas, M. (2001). Reductionism and complex thinking during ERP implementations. *Business Process Management Journal*, 7 (5) p. 387-393.

Yee, K (2004). Aligning Security and Usability, *IEEE Security & Privacy*, p. 48-55

Yin, R., K. (1994) "Case Study Research, Design and Methods", (2nd ed.) Sage Publications, Newbury Park, CA.

Yin, R., K. (2003) "Case Study Research: Design and Methods", (3rd ed.) Sage Publications, Newbury Park, CA.