**Knowledge Sharing and Information Security: A Paradox?**

Ghosia Ahmed, Gillian Ragsdell, Wendy Olphert
Loughborough University, Leicestershire, United Kingdom
g.ahmed@lboro.ac.uk
g.ragsdell@lboro.ac.uk
c.w.olphert@lboro.ac.uk

**Abstract:** This paper presents the findings of a knowledge sharing and information security literature review and identifies an interesting research gap in the intersection of the two practices.

In a fast changing environment where there is increasing need to understand customers' demands and competitors' strategies (Lin et al, 2012), knowledge sharing is recognised as an essential activity for organisational success (Wasko and Faraj, 2005; Renzl, 2008). Organisations continuously aim to exploit existing knowledge, seek new ways to improve and increase knowledge sharing activities, as well as to identify and reduce possible knowledge sharing barriers. However, albeit the integral role and benefits of knowledge sharing having been widely recognised, the security or protection of knowledge has not received the same level of attention. Although the importance of protecting knowledge has been stressed by some researchers (e.g. Gold et al, 2001; Desouza and Awazu, 2004; Desouza 2006; Ryan, 2006), research into the 'softer' or the human behaviour aspects of knowledge protection is scarce.

Information security is another field that has grown tremendously and is now a globally recognised discipline (Gifford, 2009) receiving attention from academics and practitioners (Wiant, 2005). Information security measures aim to prevent the loss or leakage of an organisation's valuable information and manage the resulting cost of any loss. Despite organisations' investments in prevention measures, information security breaches are still common where humans are often seen as the weakest link and 'incorrect' human behaviour as the most common point of failure. However, much of the research carried out to prevent information security breaches focuses on technical facets (Gordon and Loeb, 2006; Coles-Kemp, 2009).

From the literature review, it is evident that knowledge sharing and information security have become well-established concepts in academia and within organisations. However, the middle ground between these two equally important, and adjacent, practices, has received inadequate attention. Knowledge sharing aims to encourage individuals to share knowledge with colleagues, organisational partners and suppliers; on the other hand, information security initiatives aim to apply controls and restrictions to the knowledge that can be shared and how it is shared.

This paper draws attention to the perceived paradoxical nature of knowledge sharing and information security and raises awareness of the potential conflict that could compromise the protection of knowledge, or alternatively, reduce the openness of knowledge sharing.

**Keywords**: Knowledge sharing, information security, knowledge protection, literature review

## 1. Introduction

Organisations pay particular attention to knowledge management as knowledge forms an integral intangible asset facilitating organisational success and competitive advantage (Mueller, 2012). Advancing tremendously, knowledge management research has focused primarily on recognising, capturing, and the sharing of knowledge for improvement and innovation (Ryan, 2006). Knowledge sharing underpins the success of knowledge management initiatives (Wang and Noe, 2010) and has been recognised as a vital activity for organisational success (e.g. see Wasko and Faraj, 2005; Renzl, 2008). However, whilst focusing on exploiting and maximising the value of knowledge, research into knowledge protection has been lacking (Desouza, 2006).

Information security has also now become a globally recognised discipline (Gifford, 2009) within organisations and academia. Affecting individuals in organisations on a daily basis (Albrechtsen, 2007), information security measures aim to manage the loss of information and the subsequent cost of that loss (Winkler, 2011) by protecting the confidentiality, integrity and availability or accessibility of information (Grama, 2010; Gifford, 2009; Kim and Solomon, 2010). Despite the fundamental role of human awareness and behaviour in making information security practices successful being acknowledged by various researchers (e.g. Coles-Kemp, 2009; Albrechtsen, 2007; Bishop, 2006;

Stanton et al, 2005), literature has mainly focused on technical or formal aspects such as technologies, access controls and policies (Coles-Kemp, 2009).

Albeit the widespread recognition and implementation of the two practices, the middle ground between knowledge sharing and information security is an area that has been overlooked. Furthermore, there could be a paradox between knowledge sharing and information security practices (Desouza, 2006; Ryan, 2006) as one practice aims to encourage sharing of knowledge whereas the other tries to control the sharing through security measures. The following two sections comprise a literature review of knowledge sharing and information security, including a discussion of definitions, purposes and factors affecting each practice. Following this, we identify the middle ground between the two practices where a potential conflict of interest may exist and, finally, present the research gap.

## 2. Knowledge sharing

Christensen (2007) defines knowledge sharing as a process that exploits existing knowledge by identifying, transferring and applying it to solve tasks better, faster and cheaper. It is the essential mechanism through which employees apply their knowledge and contribute to an organisation's innovation (Jackson et al, 2006), but happens at the willingness of the individual (Gibbert and Krause, 2002). Huysman and De Wit (2002) claim that knowledge sharing is the foundation for organisational learning yet Hendriks (1999: 92) argues that "in a strict sense, knowledge cannot be shared" as it is entwined with a knowing subject, thus, certain prior knowledge is required to reconstruct and acquire knowledge.

Terms such as 'knowledge transfer' and 'knowledge exchange' are also sometimes used for referring to knowledge sharing (Foss et al, 2010) and bring ambiguity e.g. O'Dell and Grayson (1998), Inkpen and Tsang (2005), and Wasko and Faraj (2005) Cabrera et al (2006), Christensen (2007) and Haas and Hansen (2007).

Though these definitions and perspectives of knowledge sharing vary in many respects, they do share similar core concepts such as, using existing knowledge within the organisation to solve problems, generating new learning, and empowering the organisation for innovation.

### 2.1 Important factors in knowledge sharing

Knowledge sharing is a behaviour of choice (Ajzen, 1991; Gagné, 2009), thus, there are factors discussed by researchers (e.g. Hendriks, 1999; Bock and Kim, 2002; Lin, 2007; Gagné, 2009; Wang and Noe, 2010) that can motivate or hinder this behaviour. Alternatively, Riege (2005) has reviewed extensive knowledge sharing literature and identified three categories of barriers to knowledge sharing, including, individual factors (e.g. lack of trust and fear of loss of power,), organisational factors (e.g. lack of leadership and lack of appropriate reward systems,), and technological factors (e.g. inappropriate systems and lack of training).

This literature review also highlights three categories of factors affecting knowledge sharing; human factors, technological factors and organisational factors.

#### *2.1.1 Human factors*

According to Reagans and McEvily (2003), *social connection* with the knowledge receiver is likely to motivate the knowledge owner to share knowledge. However, a study by Thomas-Hunt et al (2003) found that socially isolated members made greater contributions than socially connected members, and, their contributions were better acknowledged by others. Phillips et al (2004) also found positive congruence between social connections and effective group performance, but this was not the case in larger groups as it led to divisions and formation of sub-groups.

*Trust* between individuals is a fundamental principle of an effective social exchange (Blau, 1964), thus, trust improves an individual's motivation to supply useful knowledge (Tsai and Ghoshal, 1998), and accept the knowledge given by others (Mayer et al, 1995). Contrariwise, Bakker et al (2006) argue that, while the presence of high levels of trust does not necessarily increase knowledge sharing, a lack of trust may inhibit individuals' knowledge sharing motivation.

Cabrera et al (2006) explain that individuals may share knowledge by the perceived *rewards* associated with it, and according to Yao et al (2007), a lack of incentives can be a knowledge sharing barrier. Opposing arguments claim that extrinsic reward schemes can become a knowledge sharing

barrier and have a counter-effect on existing intrinsic practices and motivations (Huber, 2001; Robertson and Swan, 2003).

The concepts of '*knowledge hiding*' and '*knowledge hoarding*' have also been highlighted as possible barriers to knowledge sharing. Knowledge hiding, according to Connelly et al (2011: 65), is "an intentional attempt by an individual to withhold or conceal knowledge that has been requested by another person". 'Knowledge hoarding' on the other hand, is when an individual accumulates knowledge that may or may not be shared in the future (Hislop, 2003) and can be caused by competition (Hansen et al, 2005). Both concepts can be characterised as a category of possible knowledge withholding behaviours (Connelly et al, 2011).

*2.1.2 Technological factors*

Ruddy (2000) asserts that technology combined with cultural or behavioural awareness is essential for effectively sharing knowledge. Knowledge Management Systems (KMS) are specifically implemented for documenting, distributing and transferring of knowledge between employees (Voelpel et al, 2005). However, research on knowledge sharing technologies has mainly focused on explicit and formal types of knowledge (Oshri et al, 2008), whereas a significant amount of organisational knowledge is shared informally and sometimes requires informal systems (Davison et al, 2013).

Despite the benefits of such technologies, knowledge sharing can become challenging for people if there is a lack of integration of technological systems and processes, shortage of technical support, a gap between what individuals require and what the systems provide, and a lack of familiarity and training on systems (Riege, 2005). Further, unrealistic expectations of employees in relation to the technology's capability (Riege, 2005) or the technology being too complex (Babcock, 2004) also have a negative impact on knowledge sharing.

*2.1.3 Organisational factors*

Martiny (1998) claims that change must be driven by management in the form of clear support and employees will share knowledge if they feel that it is desirable and expected by management. This argument is supported by studies such as Connelly and Kelloway (2003) and Cabrera et al (2006). A lack of support and direction from management can inhibit knowledge sharing (Riege, 2005), however, Mueller (2012) argues that, since knowledge sharing is not recognised as a formal activity, management should not interfere with informal processes and leave this responsibility for employees.

## 3. Information security

Information security has become a globally recognised discipline (Gifford, 2009) and is one of the various requirements of an employee's working day (Albrechtsen, 2007). According to Winkler (2011), information security is concerned with managing the loss of information and the subsequent cost of that loss, yet a more common definition is about protecting the confidentiality, integrity and availability or accessibility of information (Gordon and Loeb, 2006; Grama, 2010; Gifford, 2009; Kim and Solomon, 2010).

Information security cannot be achieved by technologies alone, thus, policies and procedures play an important role (Von Solms, 2001; Bishop, 2006; Coles-Kemp, 2009; Klaic and Hadjina, 2011). Although, in order to make them work, a human perspective on information security is fundamental (Coles-Kemp, 2009; Albrechtsen, 2007; Stanton et al, 2005). Where correct and constructive human behaviour can enhance the effectiveness of information security, incorrect and negative behaviour could inhibit it (Stanton et al, 2005).

### 3.1 Information security threats and measures

Despite organisations implementing prevention measures, information security breaches are common (Gordon and Loeb, 2006). PricewaterhouseCoopers (2013), stated 93% of large and 87% of smaller organisations reported facing security breaches. Gordon and Loeb (2006) stress that organisations must have the ability to detect and rectify information security breaches, however, in reality, even well established organisations that have disaster response measures in place, still suffer significantly from such breaches (Anderson, 2003).

Information is exposed to technologies, people and processes (Posthumus and Von Solms, 2004), which is why, unsurprisingly, the majority of serious information security breaches take place due to failure from a combination of these (PricewaterhouseCoopers, 2013). Technologies can never be

resistant to attack so information security needs to be a multi-layered approach (Smith, 2013). Yet majority of the research carried out to prevent information security breaches focuses on mainly technical measures (Gordon and Loeb, 2006) despite the widespread acknowledgement of humans being the weakest link in information security (e.g. Stajano and Wilson, 2011; Spears and Barki, 2010).

*3.1.1 Human related threats and prevention measures*

Marks and Rezgui (2009) assert that most security managers focus primarily on technical facets and solutions, yet research strongly suggests that non-technical aspects are equally as important (Siponen and Oinas-Kukkonen, 2007; Dhillon and Torkzadeh, 2006). Further, according to KPMG's (2012-2013) security survey, the most common point of failure in information security is human behaviour - despite the recognition of human input being essential in the success of information security initiatives (e.g. Albrechtsen, 2007; Bulgurcu et al, 2010).

Dhillon and Backhouse (2000) claim that most security breaches are caused by existing employees, possibly due to a lack of employee integrity, whereas Shropshire (2009) believes it could be due to personal hardships or vengeance. However, in many cases the breaches are not planned with malicious intent, but are rather unintentional, accidental or out of the involved party's control (Shropshire, 2009). Stajano and Wilson (2011: 70) argue that "security engineers only thought about their way of protecting the system, not about how real users would react to maliciously crafted stimuli".

Siponen (2001) argues that information security awareness should form an integral part of the general knowledge of individuals - where anyone who sees information as an important asset, should also be aware of the potential threats. Awareness and education should be designed to respond to the cultural variations within organisations (Coles-Kemp, 2009) so that employees focus on working for, or with security, rather than against it (Furnell and Thomson, 2009).

*3.1.2 Technology related threats and prevention measures*

Despite being protected by intricate safeguards, systems are frequently vulnerable to attack (Stajano and Wilson, 2011). Deloitte (2013) reports that, although new technologies provide powerful capabilities to organisations, the risks introduced by these technologies are evolving at an overwhelming pace. In particular, Internet related security attacks such as viruses and hacking are immense and increasing (Herley, 2009), yet, PricewaterhouseCoopers (2013) found that 83% of large and approximately 75% of small organisations have stored 'confidential' or 'highly confidential' data on the Internet. Additionally, many organisations allow their employees to use personal devices to access organisational systems, emails and data under the 'Bring Your Own Device' trend, despite the growing security risks posed by it (Deloitte, 2013).

Siponen and Oinas-Kukkonen (2007) claim that anti-virus software aims to guarantee the requirements of confidentiality, integrity and availability are satisfied, however, this alone is insufficient even if organisations feel 'protected' through it (Smith, 2013). Technological information security solutions impact and frame the users' behaviour and act as a "foolproof security mechanism" when they use a system (Albrechtsen, 2007: 277). Such mechanisms may automatically and unnoticeably prevent users from performing a potentially unsafe action, but it does raise questions about the level of security awareness and understanding the users of such systems have.

*3.1.3 Policy related threats and prevention measures*

Ernst & Young (2012) reports that, since 2006, organisations have been forced to implement new security policies that incorporate the risks arising from new technologies being used in the workplace. According to PricewaterhouseCoopers (2013), 93% of organisations where a security policy existed but was poorly understood by the employees, had employee related breaches, whereas in the organisations where the policy was understood, 47% still experienced staff related breaches. Thus, having information security policies in place does not guarantee such policies being followed by employees and the effectiveness of the implementation of these policies becomes disputable.

Information security policy compliance is currently one of the biggest challenges and concerns for organisations (Al-Omari et al, 2012). Further, an employee's attitude towards compliance of security policies may be determined by possible consequences of their experiences, for example, the time and effort required if they comply or the punishment if they do not (Bulgurcu et al, 2010). Al-Omari et al (2012) argue that compliance with security policies is influenced by quality of information, facilitating

conditions and habits of employees, whereas Knapp et al (2006) believe it is top management support that is most influential.

**4. Middle ground between knowledge sharing and information security**

In section 2, we discussed the importance of knowledge sharing in order for organisations to gain advantage from their most valuable asset – their knowledge. However, the field of knowledge management has mostly focused on maximising the value of and exploiting knowledge. Subsequently, research into protection of knowledge has been lacking (Desouza, 2006). Although, some researchers have highlighted concerns and aimed to explore the area of knowledge protection (e.g. De Faria and Sofka, 2010; Desouza, 2006; Ryan, 2006; Holsapple and Jones, 2005; Desouza and Awazu, 2004; Gold et al, 2001), the research on this topic remains sparse.

In section 3 we discussed how and why organisations implement information security measures to prevent and manage the loss of their valuable information. It is essential for organisations to secure knowledge, should they wish to make it a 'truly competitive resource' (Desouza, 2006), however, much of the literature on information security has focused on technical aspects (Coles-Kemp, 2009) – albeit the integral role of human awareness and behaviour being acknowledged by various researchers (e.g. Coles-Kemp, 2009; Albrechtsen, 2007; Bishop, 2006; Stanton et al, 2005).

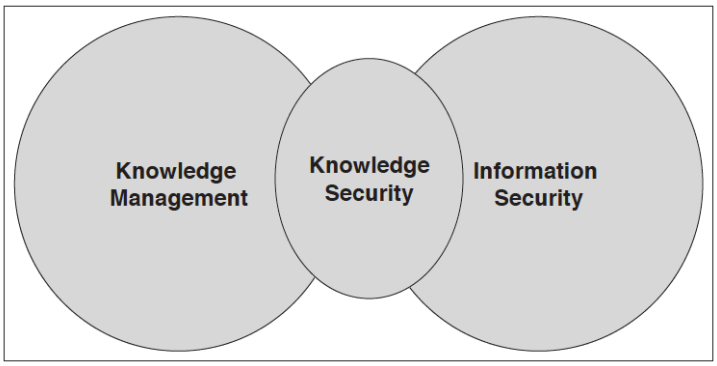


**Figure 1: Knowledge security (Desouza, 2006: 2)**

Despite the widespread recognition and implementation of the two practices, there could be a paradox between knowledge sharing and information security (Desouza, 2006; Ryan, 2006). Ryan (2006) discusses the security needs of knowledge management and proposes further research to help organisations effectively manage the tension between knowledge sharing and knowledge protection. Ryan (2006: 45) claims that the cause of this conflict is the "intersection of the nature of innovation and the rewards of innovation", since innovation requires novel ideas and concepts to be imagined and shared, but on the other hand, there are needs to protect intellectual capital. Similarly, Desouza (2006) draws attention to a research space that he calls, 'Knowledge Security' (see Figure 1), existing between knowledge management and information security (Desouza, 2006; Desouza and Awazu, 2004).

Achieving knowledge security is not easy and has various challenges associated with it. Desouza (2006) argues that, unlike information, knowledge is difficult to visualise and capture, in particular tacit knowledge that resides in people's heads, and if this knowledge cannot be visualised, how can it be managed? There are additional, perhaps greater, challenges that have not been raised by Desouza (2006) or Ryan (2006). For example, when looking at the possible conflict between the practices of knowledge sharing and information security, how can organisations find evidence of this clash existing in practice? Another challenge is identifying the level of knowledge security awareness amongst individuals and how this affects their knowledge sharing behaviour in the workplace, which would be a critical early step in identifying how serious an issue, if at all, knowledge security is.

**5. Research gap**

From our review of the literature, we argue that the research gap of 'knowledge security' exists in the middle ground between the practices of knowledge sharing, rather than the knowledge management discipline as a whole, as argued by Desouza (2006), and information security. The possible conflict between knowledge sharing and information security is an area that needs vital exploration before moving onto the next step of attempting to achieve knowledge security.

Although Desouza (2006) and Ryan (2006) have discussed the existence of this clash and other researchers (e.g. De Faria and Sofka, 2010; Ryan, 2006; Holsapple and Jones, 2005; Gold et al, 2001) have stressed the importance of 'knowledge protection', evidence of this problem in practice has not yet been presented. Further, from a practical perspective, little research has been carried out to understand an employee's behaviour and whether they experience a paradox when attempting to share knowledge whilst simultaneously abiding by the security expectations. If a paradox exists, does it make individuals careless when sharing knowledge and compromise on security, or, does their knowledge sharing become inhibited? This would be a good starting point for further research in this enticing research area.

## 6. Conclusion

By conducting this literature review, it has become evident that the research in these areas has grown tremendously, primarily driven by globalisation, advancements in information and communication technologies and the Internet. These factors have already changed, and continue to change, the way organisations operate and the way people work. However, the practices of knowledge sharing and information security could be in conflict due to their intrinsic opposing natures. The possibility of a conflict has not been widely recognised in academia or in organisations, and thus, requires further research to explore and understand the scale and seriousness of the problem and its impact on the knowledge sharing behaviour of individuals.

## References


Ajzen, I. (1991) The Theory of Planned Behavior, *Organizational Behavior and Human Decision Processes*, Vol.50, No.2, pp.179-211.

Al-Omari, A., El-Gayar, O. and Deokar, A. (2012) Security Policy Compliance: User Acceptance Perspective, In 2012 Proceedings *of 45th Hawaii International Conference on System Science (HICSS)*, Maui, Hawaii, January 2012, IEEE.

Albrechtsen, E. (2007) A Qualitative Study of Users' View on Information Security, *Computers & Security*, Vol.26, No.4, pp.276-289.

Anderson, J.M. (2003) Why We Need a New Definition of Information Security, *Computers & Security*, Vol.22, No.4, pp.308-313.

Babcock, P. (2004) Shedding Light on Knowledge Management, *HR Magazine*, Vol.49, No.5, pp.46-51.

Bakker, M., Leenders, R.T.A.J., Gabbay, S.M., Kratzer, J. and Van Engelen, J.M.L. (2006) Is Trust Really Social Capital? Knowledge Sharing in Product Development Projects, *The Learning Organisation*, Vol.13, No.6, pp.594−p.59

Bishop, M. (2006) Teaching Context in Information Security, *ACM Journal of Educational Resources in Computing*, Vol.6, No.3, pp.3.

Blau, P. (1964) Exchange and Power in Social Life, Wiley, New York.

Bock, G.W. and Kim, Y.G. (2002) Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing, *Information Resources Management Journal (IRMJ)*, Vol.*15*, No.2, pp.14-21.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness, *MIS Quarterly*, Vol.34, No.3, pp.523-548.

Cabrera, A., Collins, W.C. and Salgado, J.F. (2006) Determinants of Individual Engagement in Knowledge Sharing, *The International Journal of Human Resource Management*, Vol.17, No.2, pp.245-264.

Christensen, P.H. (2007) Knowledge Sharing: Moving Away from the Obsession with Best Practices, *Journal of Knowledge Management*, Vol.11, No.1, pp.36-47.

Coles-Kemp, L. (2009) Information Security Management: An Entangled Research Challenge, *Information Security Technical Report*, Vol.14, No.4, pp.181-185.

Connelly, C.E. and Kelloway, E.K. (2003) Predictors of Employees' Perceptions of Knowledge Sharing Cultures, *Leadership & Organisation Development Journal*, Vol.24. No.5/6, pp.294−p.29

Connelly, C.E., Zweig, D., Webster, J. and Trougakos, J.P. (2011) Knowledge Hiding in Organisations, *Journal of Organisational Behaviour*, Vol.33, No.1, pp.64-88.

Davison, R.M., Ou, C.X.J. and Martinsons, M.G. (2013) Information Technology to Support Informal Knowledge Sharing, *Information Systems Journal*, Vol.23, No.1, pp.89-109.

De Faria, P. and Sofka, W. (2010) Knowledge Protection Strategies of Multinational Firms - A Cross-country Comparison, *Research Policy*, Vol.39, No.7, pp.956-968.

Deloitte (2013) Blurring the Lines: 2013 TMT Global Security Study [pdf] Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT_GlobalSecurityStudy_English_final_020113.pdf [Accessed 26 March 2014].
Desouza, K.C. (2006) Knowledge Security: An Interesting Research Space, *Journal of Information Science and Technology*, Vol.3, No.1, pp.1-7.
Desouza, K.C. and Awazu, Y. (2004) Securing Knowledge Assets: How Safe is Your Knowledge?, *J@pan.Inc*, Vol.58, pp.22-25.
Dhillon, G. and Backhouse, J. (2000) Technical Opinion: Information System Security Management in the New Millennium, *Communications of the ACM*, Vol.43. No.7, pp.125-128.
Dhillon, G. and Torkzadeh, G. (2006) Value-focused assessment of information system security in organizations, *Information Systems Journal*, Vol.16, No.3, pp.293-314.
Ernst & Young (2012) Fighting to Close the Gap - Global Information Security Survey [pdf] Available at: http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf [Accessed 26 March 2014].
Foss, N.J., Husted, K. and Michailova, S. (2010) Governing Knowledge Sharing in Organisations: Levels of Analysis, Governance Mechanisms, and Research Directions, *Journal of Management Studies*, Vol.47, No.3, pp.455-482.
Furnell, S. and Thomson, K.L. (2009) From Culture to Disobedience: Recognising the Varying User Acceptance of IT Security, *Computer Fraud & Security*, No.2, pp.5-10.
Gagné, M. (2009) A model of knowledge-sharing motivation, *Human Resource Management*, Vol.48, No.4, pp.571-589.
Gibbert, M. and Krause, H. (2002) Practice Exchange in a Best Practice Marketplace, In Knowledge Management Case Book: Siemens Best Practices, T.H. Davenport and G.J.B. Probst (Eds.), Publicis Corporate Publishing, Erlangen, Germany, pp.89-105.
Gifford, N. (2009) Information Security: Managing the Legal Risks, CCH Australia Limited, Australia.
Gold, A.H., Malhotra, A. and Segars, A.H. (2001) Knowledge Management: An Organisational Capabilities Perspective, *Journal of Management Information Systems*, Vol.18, No.1, pp.185-214.
Gordon, L.A. and Loeb, M.P. (2006) Budgeting Process for Information Security Expenditures, *Communications of the ACM*, Vol.49, No.1, pp.121-125.
Grama, J. (2010) Legal Issues in Information Security, Jones & Bartlett Learning, Sudbury.
Haas, M.R. and Hansen, M.T. (2007) Different Knowledge, Different Benefits: Toward a Productivity Perspective on Knowledge Sharing in Organisations, *Strategic Management Journal*, Vol.28, No.11, pp.1133-1153.
Hansen, M.T., Mors, M.L. and Løvås, B. (2005) Knowledge Sharing in Organizations: Multiple Networks, Multiple Phases, *Academy of Management Journal*, Vol.48, No.5, pp.776-793.
Hendriks, P. (1999) Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing, *Knowledge and Process Management*, Vol.6, No.2, pp.91-100.
Herley, C. (2009) So long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, In *New Security Paradigms Workshop (NSPW'09),* Oxford, UK, September 2009, ACM.
Hislop, D. (2003) Linking Human Resource Management and Knowledge Management Via Commitment: A Review and Research Agenda, *Employee Relations*, Vol.25, No.2, pp.182–202.
Holsapple, C. and Jones, K. (2005) Exploring Secondary Activities of the Knowledge Chain, *Knowledge and Process Management*, Vol.12, No.1, pp.3-31.
Huber, G.P. (2001) Transfer of Knowledge in Knowledge Management Systems: Unexplored Issues and Suggested Studies, *European Journal of Information Systems*, Vol.10, No.2, pp.72-79.
Huysman, M.H. and de Witt, D. (2002) Knowledge Sharing in Practice, Kluwer Academic Publishers, Dordrecht.
Inkpen, A.C. and Tsang, E.W. (2005) Social Capital, Networks, and Knowledge Transfer, *Academy of Management Review*, Vol.30, No.1, pp.146-165.
Jackson, S.E., Chuang, C.H., Harden, E.E. and Jiang, Y. (2006) Toward Developing Human Resource Management Systems for Knowledge-Intensive Teamwork, *Research in Personnel and Human Resources Management*, Vol.25, pp.27-70.
Kim, D. and Solomon, M.G. (2010) Fundamentals of Information Systems Security, Jones & Bartlett Learning, Sudbury.

Klaic, A. and Hadjina, N. (2011) Methods and Tools for the Development of Information Security Policy—A comparative Literature Review, In *MIPRO, 2011 Proceedings of the 34th International Convention*, Opatija, Croatia, May 2011, IEEE.
Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006) Information Security: Management's Effect on Culture and Policy, *Information Management & Computer Security*, Vol.14, No.1, pp.24-36.
KPMG (2012-2013) Luxembourg IT Security Survey 2012-2013 [pdf] Available at: http://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/Lux-IT-Security-Survey-2012-2013.pdf [Accessed 26 March 2014].
Lin, H.F. (2007) Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions, *Journal of information science*, Vol.*33*, No.2, pp.135-149.
Lin, R.J., Che, R.H. and Ting, C.Y. (2012) Turning Knowledge Management into Innovation in the High-tech Industry, *Industrial Management & Data Systems*, Vol.112, No.1, pp.42–63.
Marks, A. and Rezgui, Y. (2009) A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing, In 2009 Proceedings of *International Conference on Management and Service Science (MASS'09)*, Wuhan, China September 2009, IEEE.
Martiny, M. (1998) Knowledge Management at HP Consulting, *Organisational Dynamics*, Vol.27, No.2, pp.71-77.
Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) An Integration Model of Organisational Trust, Academy of *Management Review*, Vol.20, No.3, pp.709–734.
Mueller, J. (2012) Knowledge Sharing between Project Teams and its Cultural Antecedents, *Journal of Knowledge Management*, Vol.16, No.3, pp.435-447.
O'Dell, C. and Grayson, C.J. (1998) If only we knew what we know: Identification and Transfer of Internal Best Practices, *California Management Review*, Vol.40, No.3, pp.154-174.
Oshri, I., Fenema, P. and Kotlarsky, J. (2008) Knowledge Transfer in Globally Distributed Teams: The Role of Transactive Memory, *Information Systems Journal*, Vol.18, No.6, pp.593–616.
Phillips, K.W., Mannix, E.A., Neale, M.A. and Gruenfeld, D.H. (2004) Diverse Groups and Information Sharing: The Effects of Congruent Ties, *Journal of Experimental Social Psychology*, Vol.40, No.4, pp.497−49
Posthumus, S. and Von Solms, R. (2004) A Framework for the Governance of Information Security, *Computers & Security*, Vol.23, No.8, pp.638-646.
PricewaterhouseCoopers (2013) Information Security Breaches Survey - Technical Report [pdf] Available at: http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf [Accessed 26 March 2014].
Reagans, R. and McEvily, B. (2003) Network Structure and Knowledge Transfer: The Effects of Cohesion and Range, *Administrative Science Quarterly*, Vol.48, No.2, pp.240-267.
Renzl, B. (2008) Trust in Management and Knowledge Sharing: The Mediating Effects of Fear and Knowledge Documentation, *Omega*, Vol.36, No.2, pp.206−p.20
Riege, A. (2005) Three-dozen Knowledge-Sharing Barriers Managers Must Consider, *Journal of Knowledge Management*, Vol.9, No.3, pp.18-35.
Robertson, M. and Swan, J. (2003) Control – What Control? Culture and Ambiguity within a Knowledge firm, *Journal of Management Studies*, Vol.40, No.4, pp.831–58.
Ruddy, T. (2000) Taking Knowledge from Heads and Putting it into Hands, *Knowledge and Process Management*, Vol.7, No.1, pp.37-40.
Ryan, J.J. (2006) Knowledge Management Needs Security Too. *Vine*, Vol.36, No.1, pp.45-48.
Shropshire, J. (2009) A Canonical Analysis of Intentional Information Security Breaches by Insiders, *Information Management & Computer Security*, Vol.17, No.4, pp.296-310.
Siponen, M. (2001) Five Dimensions of Information Security Awareness, *Computers and Society*, Vol.31, No.2, pp.24-29.
Siponen, M.T. and Oinas-Kukkonen, H. (2007) A Review of Information Security Issues and Respective Research Contributions, *ACM Sigmis Database*, Vol.38, No.1, pp.60-80.
Smith, D. (2013) Life's Certainties: Death, Taxes and APTs, *Network Security*, No.2, pp.19-20.
Spears, J.L. and Barki, H. (2010) User Participation in Information Systems Security Risk Management, *MIS Quarterly*, Vol.34, No.3, pp.503-522.
Stajano, F. and Wilson, P. (2011) Understanding Scam Victims: Seven Principles for Systems Security, *Communications of the ACM*, Vol.54, No.3, pp.70-75.
Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005) Analysis of End User Security Behaviors, *Computers & Security*, Vol.24, No.2, pp.124-133.
Thomas-Hunt, M.C., Ogden, T.Y. and Neale, M.A. (2003) Who's Really Sharing? Effects of Social and Expert Status on Knowledge Exchange within Groups, *Management Science*, Vol.49, No.4, pp.464-77.

Tsai, W. and Ghoshal, S. (1998) Social Capital and Value Creation: The Role of Intrafirm networks, *Academy of Management Journal*, Vol.41, No.4, pp.464–476.
Voelpel, S.C., Dous, M. and Davenport, T.H. (2005) Five Steps to Creating a Global Knowledge-sharing System: Siemens' ShareNet, *The Academy of Management Executive*, Vol.19, No.2, pp.9-23.
Von Solms, B. (2001) Information Security-A Multidimensional Discipline, *Computers & Security*, Vol.20, No.6, pp.504-508.
Wang, S. and Noe, R.A. (2010) Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, Vol.20, No.2, pp.115-131.
Wasko, M.M. and Faraj, S. (2005) Why Should I Share? Examining Social Capital and Knowledge Contribution in Electronic Networks of Practice, *MIS Quarterly*, Vol.29. No.1, pp.35-57.
Wiant, T.L. (2005) Information security policy's impact on reporting security incidents, *Computers & Security*, Vol.*24*, No.6, pp.448-459
Winkler, I. (2011) Zen and the Art of Information Security, Syngress, Rockland, MA.
Yao, L.J., Kam, T.H.Y. and Chan, S.H. (2007) Knowledge Sharing in Asian Public Administration Sector: The Case of Hong Kong, *Journal of Enterprise Information Management*, Vol.20, No.1, pp.51−p.5