2017

Literature-based analysis of the influences of the new forces on ISMS: A conceptual framework

Zahir Al-Rashdi
RMIT University

Martin Dick
RMIT University

Ian Storey
RMIT University

Recommended Citation

Al-Rashdi, Z., Dick, M., & Storey, I. (2017). Literature-based analysis of the influences of the new forces on ISMS: A conceptual framework. DOI: https://doi.org/10.4225/75/5a84e4dc95b42

DOI: 10.4225/75/5a84e4dc95b42
Al-Rashdi, Z., Dick, M., & Storey, I. (2017). Literature-based analysis of the influences of the new forces on isms: a conceptual framework. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.116-124).
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/213

LITERATURE-BASED ANALYSIS OF THE INFLUENCES OF THE NEW FORCES ON ISMS: A CONCEPTUAL FRAMEWORK

Zahir Al-Rashdi, Dr Martin Dick, Dr Ian Storey
School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia
zahir.al-rashdi@rmit.edu.au, martin.dick@rmit.edu.au, ian.storey@rmit.edu.au

Abstract

This paper presents an analysis that arose from a comprehensive review of the academic and professional literature of two areas – information security management systems (ISMS) and information resources – and their relationship with information security. It analyzes the role of ISMS in protecting an organization's information environment and infrastructure. It has identified four key areas that strongly influence the safety of information resources: cloud computing; social media/networking; mobility; and information management/big data. Commonly referred to as 'new forces', these four aspects are all growing exponentially and are not easily controlled by IT. Another key finding of the paper is that organizations aiming to protect their information resources need to adapt their ISMS in an environment where these new forces have exposed them to a range of external entities and influences.

Keywords: accountability, cloud computing, service provision, information security, information resources

INTRODUCTION

Gartner identified a range of emerging technologies that strongly influence information resources, which have been referred to as 'new forces' (Gartner 2013). These new forces – cloud computing, social media/networking, mobility, and information management/big data – cannot be controlled by IT groups (internal or external) and have been predicted as a high priority for IT spending in the next decade (Smith 2013). They are all growing at a fast pace (Gartner 2013), and the traditional controls (firewalls, malware detection, etc.) that IT groups have used to protect an organization's information resources are generally unable to cope with their rapid evolution on a daily basis (Crompton 2015). The following are examples of how these new forces are impacting on the frameworks that IT groups have installed to protect organizations' information resources:

- **Cloud computing:** The new service delivery styles and options offered by the cloud computing trend shift responsibility for security to external providers, where IT groups retain only partial responsibility for security and service delivery (Scholtz 2013).
- **Social media/networking:** This is creating different, more extensive aspects of collaboration, and there has been a change in users' behavior and in the communities in which they work (Kim 2012). Again, this technology has opened up the organization's information resources to external influences.
- **Mobility:** A wide range of new access has been directed at different applications and data, and end users have been offered a broad variety of device options (Markelj & Bernik 2012) – the heterogeneity of location and device.
- **Information management/big data:** This has altered the relationship of technology to information consumption, as the data now flows from different federated sources in either structured or unstructured forms (Marchand 1985). This revealed data is analyzed using new methodologies foreign to various IT groups (Gartner 2013).

These examples show that these new forces have exposed organizations' information resources to a wide range of external entities and influences, which has significant implications for the design, management and use of the organization's information security management systems (ISMS). IT groups need to respond to this exposure by considering the information security aspects against access and exchange of information. This proves challenging as they also need to continue to meet the individual's expectations – those that are now more knowledgeable about the use of technology and are clearly requiring the capabilities these new forces are providing. The existence of the new forces encourages and demands IT groups to work toward reformation of their information security practices.

This paper presents a conceptual framework for understanding the impact of the emergence of these new forces on ISMS. According to Von Solms (2005)), ISMS are the processes and procedures used within an organization to secure the information environment through information security, operational management and information security compliance management. A perfect ISMS is a complete and systematic management system that involves “management of humans, processes, and technologies” (Suhaimi, Goto & Cheng 2013, p. 31), in order to establish, implement, operate, monitor, review, maintain and optimize security to ensure confidentiality, integrity and availability of information.

In summary, the main motivation of this paper is to provide an in-depth understanding of the conceptual factors that comprise ISMS when used in the context of organizations’ information security and information resources, to ensure their commitment to the security of business practices and compliance to address the rapid growth of the new forces (Siponen & Willison 2009).

BACKGROUND

There are two key concepts which need to be examined in the context of this paper: (1) ISMS; and (2) the concept of information resources.

Information security management systems (ISMS)

Hong et al. (2003) defined ISMS as technical methods, along with managerial processes, practically applied to information resources such as hardware, software and data, to ensure that organizational assets and personal privacy are protected. Research on ISMS has produced a considerable amount of definitions, embodying the different spheres of ISMS research. Both academics and practitioners have differing views and interpretations of the ISMS concept. For example, Eloff and Eloff (2003) argued that an ISMS can be defined as a management system employed to secure an information environment within an organization, with a good establishment and maintenance process and procedure to manage information technology security. The management and execution of ISMS requires some necessary actions: (1) identify the information security requirements; (2) ensure the right strategies are in place to meet these requirements; (3) verify the continuous evaluation and measurement of achieved objectives/results; and (4) ensure the compatibility and usability of both protection strategies and the ISMS by reviewing and improving them over time (Yeniman Yildirim et al. 2011).

Based on the above varying definitions of ISMS, it is clear that ISMS entails a number of components that form the information environment within an organization: (1) information system technology resources (hardware); (2) information system human resources (IT skilled people); (3) information system software resources (software); and (4) information system data resources (data). In this context, this study has used the ISMS definition offered by Hong et al. (2003)), because it covers the most important aspects of technology used in any organization, and is considered the most valuable asset to an organization in today’s world.

Information resources

Information resources comprise hardware, software, data and IT human resources in an organization, and represent the main source for information (Bharadwaj 2000). The effective use of information resources is often a key indicator of an organization’s ability to achieve a high level of information security and organizational privacy; although such a high investment in IT can also be a key indicator of failure, if not properly adjusted and controlled (Nolan 1994).

What is the relationship between information resources and ISMS?

Most organizations today are heavily dependent on the use of IT and information resources – the foundation of an organization, representing a key element of its growth and survival (Bharadwaj 2000).

Thus, there are escalating organizational concerns about information security including privacy and protection, risk management, and the management of information resources, which is ever-increasing. A proper solution therefore needs to be implemented to secure information resources. Some information resources are sensitive; meaning that a cost-optimal solution for secure access to information located across different servers or databases is needed, along with guidelines to ensure that the security and privacy of sensitive, unclassified information is not leaked. A combination of the latest technologies and strong human IT skills would strengthen organizational capability to safeguard information. Similarly, successful organizations should use technology and human IT skills to ensure the protection of organizational information resources and personal privacy. ISMS is commonly considered a socio-technical system that encourages a combination of both technical and human elements (Siponen & Willison 2009).

RESEARCH METHODOLOGY

A systematic literature review of ISMS, information resources, the new forces and their relationship with an organization's information security was conducted using an adapted version of the methodology of Okoli and Schabram (2010). The key steps in the methodology are:

1. *Purpose of the Review* – As described in the introduction of this paper
2. *Protocol and Training* – As only one reviewer was used, training did not have to be done and the protocol focused on the intersection between the four new forces and ISMS.
3. *Searching for the Literature* - via two sources: (1) papers published in academic and professional literature; and (2) industrial reports published by well-known organizations such as Gartner, Microsoft, IBM, Cisco, and Business News Daily. When accessing the literature, the following keywords were used to search IEEE Xplore, ScienceDirect, the ACM Digital Library, ProQuest, and Google Scholar: cloud computing; cloud computing security; information security; ISMS; information systems; information resources; vulnerability; risk assessment and risk management; threats and information security breaches; auditability and trust; confidence; social media/networking; information security for cloud computing; information systems security; information technology security; information security management; cyber security; information resources; the new forces of information resources; information assurance; and information security practices and standards. The preliminary results were sourced from 500+ scholarly articles, industry standards and technical reports;
4. *Practical Screen and Quality Appraisal* – A review of the abstracts eliminated many of these papers and those remaining were then appraised as to their relevance to the purpose of the review. In total, over 350 papers were eliminated, leaving 150 papers were left remaining as suited to the literature review.
5. *Data Extraction* – The remaining papers were then examined thoroughly and relevant data was extracted.
6. *Synthesis of Studies* – A thematic analysis was performed based on the extracted data.
7. *Writing the review* – a summarized form of the review is presented in this paper.

CONCEPTUAL UNDERSTANDING OF THE NEW FORCES

The main outcomes of this review were that the scope of information resources has changed dramatically and is not really limited to one single source. That is extensive exchange of data across the Internet between different organizations has become common practice; it is not a choice anymore, but rather a mandatory task, an organization is forced to undertake. Such data exchange is represented by a variety of ways/media, made up of cloud computing, mobility, social media/networking, and information management/big data. These are a group of new technologies which are strongly interacting with information resources, which is why they are referred to as the 'new technology forces' or 'new forces'.

This review also revealed that traditional IT security methods are often unable to cope with information security issues that arise from the new forces of technology. ISMS can and needs to be frequently adjusted to deal with the evolving information security aspects revealed across the various information resources including cloud computing, mobility, social media/networking, and big data.

In addition, there are some internal characteristics that are likely to influence to what extent organizations apply ISMS, such as the business model, data holdings, technologies and applications, and the privacy risks they may raise for clients. For example, organizations managing highly sensitive data would need to implement the largest amount of ISMS components. Thus, each organization needs to customize its ISMS to accommodate the new forces.

Due to this vast and sophisticated technology (Prensky 2011), information resources are rapidly growing (Webster 2014). The scope of information resources (Kazan et al. 2012) has dramatically shifted from internal to external management (Lawrence et al. 2013), including the exchange of information Lacity and Hirschheim

(1993). Such changes are driven by different aspects of technology, based on the new forces – cloud computing (Xu 2012), social media/networking (Kim 2012), mobility (Tokuyoshi 2013), and information management/big data – which are all growing strongly and are not easily controlled by IT (Smith 2013). The organizational approach towards ISMS is therefore transforming, based on the new requirements of these new forces (Scholtz 2013). Figure 1 below presents a conceptual framework arising from the analysis that shows the overall interactions between the four new forces , information resources and ISMS.

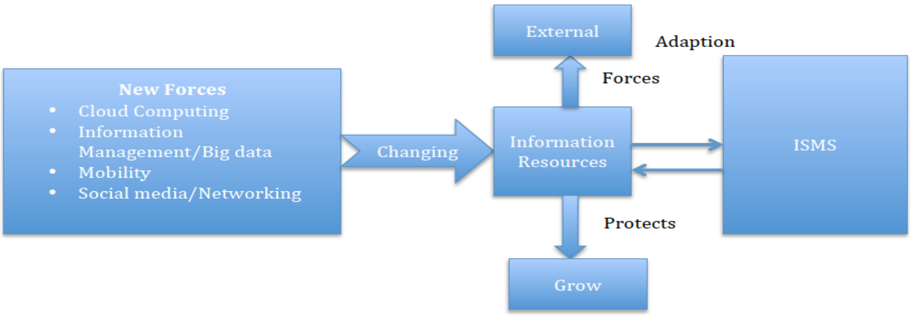

Figure 1: Conceptual Framework of the interaction of the New Forces with ISMS and Information Resources

Social media/networking

Social media/networking is the emergence of a new paradigm on the internet which allows communication and collaboration between online users and family, friends, social groups and other communities via social media channels and tools including Twitter, Facebook, MySpace and YouTube (Kim 2012).

Founded on the above definition, social media networks are considered one of the most influential factors for information resources (Xiang & Gretzel 2010), as a lot of information is gathered and exchanged (Kaplan & Haenlein 2010) among different internet users. Today, online communications via social networking applications is growing strongly and is used both personally and professionally (Jansen et al. 2009). Millions of users (Ellison 2007) are being attracted by social network sites (SNSs) such as MySpace, Facebook, Twitter and YouTube. These social media networks are receiving considerable attention from today’s business executives, decision-makers and leaders, who are trying to introduce new ways of increasing their profits (Xiang & Gretzel 2010) by using social media applications such as Wikipedia, YouTube, Facebook, Second Life, and Twitter, which means lots of information (Kaplan & Haenlein 2010) is going to be exchanged and transferred.

The social networking sites (SNSs) are being integrated with user’s daily practices (Hathi 2009) through mobile connectivity, blogging, photo sharing and video sharing as new communication tools (Ellison 2007). This indicates that the of sensitive information will be transferred and exchanged with different interests (Kim 2012). For example, Facebook (Edosomwan et al. 2011) is one of the most popular and strongest growing web applications in social networking services, where more than 500 million users all over the world use it either for work (Duggan & Brenner 2013) or pleasure, like playing games (Foster, Francescucci & West 2010). The emergence of social media and online social networking applications created real revolution to the working environment (Sturdevant 2011) in large enterprises. For example, IBM reported that (Hathi 2009) more than 40% of their employees preferred to work from customer location or home rather than attending IBM premises. Similarly, Cisco (Cisco 2010) reported that over 60% of their employees believe that productivity no longer means to work from the office, but rather productivity depends on knowledge and the ability to share that knowledge. Thus, lots of enterprises allow their employees to access online social networking sites; however this brought many security breaches to business and organisations (Kaplan & Haenlein 2010). For example, the usernames and passwords of Facebook and MySpace being sold to underground networks where sensitive information was stolen by cybercriminals (Shulman 2010), meanwhile their accounts were being hijacked (Kim 2012) and the stolen accounts used by hackers for phishing scams (Kaplan & Haenlein 2010).

Therefore, information security is a new and increasing challenge in the field of cyber security brought along by the use of social networks and the integration of ISMS within organisation to closely and properly monitor the use of different aspects of social media became a mandatory practice to eliminate the breach of information that would occur through this new rapidly-growing force.(Edosomwan et al. 2011).

Mobility

The use of mobile devices such as laptops, smartphones and PDAs to access data has become far more frequent in recent times (Markelj & Bernik, 2012). This increase in the use of mobility raises questions about corporate data security and privacy (Miller, Voas & Hurlburt 2012), which should not be exposed or compromised (Rose 2013). The future of cyber risk prevention is an area that needs to be urgently addressed by researchers, technology experts and policymakers (Kenny 2014). Most mobile device users are not proactive in dealing with information stored in their mobile by taking proper protection actions (Tokuyoshi 2013). Therefore, losing the mobile device could result in exposure of sensitive information, which is sometimes much more important and valuable than the mobile itself (Markelj & Bernik 2012). Thus, corporations' information security policies and risk management procedures and should be constantly reviewed and upgraded (Markelj & Bernik 2012).

There are many studies (Escherich 2014; Miller, Voas & Hurlburt 2012; Morrow 2012; Rose 2013; Tokuyoshi 2013) that have focused on mobility, especially the use of mobile devices in the workplace. According to a recent survey conducted by Gartner Inc. in 2013 which measured the use of personal devices for business use, or bring your own devices (BYODs) (Escherich 2014), almost one-quarter acknowledged they had experienced a security issue with their private device; yet only 27% of those users who contributed to the survey reported the issue to their employer. In summary, it would appear that mobility raises many problems for an organization's ISMS, and most will need to accelerate an introduction of "the right mix of mobile security defences to balance protection, governance and user flexibility" (Escherich 2014, p. 1).

Information management/big data

Information management in a business and organizational context means a collection of data from different departments, made ready for processing, with decisions made at the higher levels of the organization – mostly strategic rather than tactical – and external information becoming more relevant than information sourced internally (Marchand 1985). Information management is now considered a critical resource to ensure privacy (Bélanger & Crossler 2011) due to the advanced use of IT and information systems like intranets (Curry & Stancich 2000).

Dhillon (1999)) contended that one of the main issues in regards to current information management is information security – that is, the protection of information assets of the body corporate, due to the massive use of IT and growth dependent on electronic network resources.

In the past five years, the media/entertainment industry has shifted to digital recording, production and delivery, and as a result large amounts of rich content including user viewing behaviors are collected. Furthermore, significant amounts of data are now collected within the transportation, logistics, retail, utilities and telecommunications sectors via various media/technology such as GPS transceivers, RFID tag readers, smart meters and cell phones; call data records CDRs and all collected data are used to optimize operations and drive operational business intelligence (BI) to realize immediate business opportunities (Kaisler et al. 2013).

This literature review indicates that a huge amount of organizational information is being shared among users and organizations, within the provision of information management. Thus, the security of information management is deemed one of the key factors for measuring the quality of service by organizations or service providers. The implementation of ISMS would eliminate many of these information management security issues.

Cloud computing

Cloud computing relates to the use of online computing services, and is considered an on-demand IT service or product based on a business model. This is where users can access software and hardware via cloud services including SaaS, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), which are managed remotely by third parties (Sreenivas et al. 2013). It can therefore be perceived as significantly opening an organization's information resources to the external world.

Cloud computing has expanded into one of the fastest-growing portions of the IT industry (Chung & Chun 2014), and has become a promising business concept where a huge amount of information for both individuals and enterprises is now placed. However, transformation of data distribution and storage in the cloud has generated a real concern towards data privacy and data protection, and a rise in questioning about how safe the cloud environment is. Such questioning should be considered by organizations before making the decision to deploy their business into the cloud (Subashini & Kavitha 2011).

Securing information that has been transferred to the cloud is a critical issue for the success of information systems, communications and information security (Zissis & Lekkas 2012). As can be seen, there is a clear need for organizations to adapt ISMS to this new, fast-growing force.

ADAPTING ISMS TO THE NEW FORCES

The new forces – mobility, social media/networking, cloud computing, and information management/big data – are rapidly changing the information resources of organizations. Consequently, the ISMS with its core mission of protecting the information resources of the organization must adapt. In particular, increased external openness of information resources must be considered when adapting an organization's ISMS to these new forces. The following section details the adaptions that were identified from the literature analysis to allow organizations to adapt their ISMS to the impacts of the four new forces. Of course, this analysis is limited to adaptions that have already been identified in the existing literature in this area.

Organizations need to move from applying traditional information security controls such as firewalls and malware detection, and pay more attention to users behavior or internal staff that are using their own devices. This is achievable by ensuring a solid and acceptable change in the security infrastructure, design and implementation of controls to minimize preventative measures and balance the use of policies, controls, rights and responsibilities. Such balance would maximize human potential by increasing trust and independent decision-making (Scholtz 2013).

One way that organizations need to adapt is by moving from static to dynamic defences. Gartner (2013) has predicted that one of the likely scenarios of the information security changes caused by these new forces is that by 2020 the allocated budget of enterprise information security will rise to 60%, up from less than 10% in 2013, for rapid detection and response approaches.

Another key adaption is the development of ISMS policy that allows for these new forces. For example, in terms of mobility, it has been recognized that "security policies are still incomplete in many organizations, and contain gaps and other inconsistencies that don't measure up to business obligations" (Escherich 2014, p. 1). Such policy gaps need to be addressed.

Another significant adaption aspect is the strategic consideration of the new forces. First, how they will impact on the potential for interruption/disruption to IT within the business, including evaluating the risk associated with enterprise information security. Second, the organization needs to strategically determine the required investment in ISMS when adopting the new forces, and how much needs to be allocated to adapt it to an acceptable level of risk.

In addition, it should also be highlighted that these new forces are not a comprehensive list of every technology that is ready for adoption or incorporation into the strategic planning process. Enterprises should use them as a starting point and customize them based on their industry, unique business needs, technology adoption model, and which category their business is classified, and then customize their ISMS accordingly. Table 1 summarises the impacts of the new forces on Information Resources and ISMS

New Force	Impact on Information Resources	Impact on ISMS
Social Media/Networking	• Significantly increased information is gathered and exchanged • Interaction between personal and professional data and integration with user's daily practices • Use of social media as a business tool	• Many security breaches to business and organisations due to the extensive use of information brought along by the use of social networks (Edosomwan et al. 2011).
Mobility	• Increased usage and generation of information due to the very rapid uptake of mobile technology • The rapid advancement in	• Increased vectors for cyber attack, including much easier physical loss and theft • The addition of personal

	functionality of mobiles is also causing increased information resources	devices to the business environment due to BYOD • Poor security practices in many mobile devices
Information Management/Big Data	• The control of information physically became more complex. • The uncoordinated and fragmented nature of much big data • The need for much better understanding of the information resources to allow knowledge management and machine learning	• Privacy becoming a much more important issue • Coping with information overload
Cloud Computing	• Made storage of information resources much more affordable and manageable	• Management of the 3rd party outsourcing relationship with regards to the ISMS • Ensuring compatibility with external ISMS

Table 1 Impact of New Forces on Information Resources and ISMS

CONCLUSIONS AND FUTURE WORK

This study has conducted an extensive analysis of literature relating to ISMS, including the various aspects of information resources for information security to develop a model of how the new forces influence an organization’s ISMS. It has been recommended here that organizations adapt their ISMS to accommodate the changes these new forces have on information resources, with a number of suggestions made on how the ISMS should be adapted; although this is far from exhaustive. This research is part of an ongoing research program in this area.

This study is expected to have several important implications for practitioners and researchers. The findings will likely contribute to the growing awareness of the importance of the proper implementation of ISMS; resulting in a better understanding of the importance of information security factors that motivate policymakers to adopt ISMS projects prior to, during and after their implementation. It will also assist information security decision-makers to evaluate what has happened and why in terms of any security issues. This study also provides a holistic and heuristic ISMS framework that enables a theoretical-based description and analysis of the gap that exists between the ideal and the actuality of the institutional and technical environments of ISMS implementation in regards to the protection of information resources.

Finally, this study is expected to contribute to the body of knowledge of information systems and information security as part of the development of new theory. It provides a practical contribution, where new insights for ISMS implementers and investors will help improve their services. Developing this model will be achieved by conducting a series of case studies to examine the real-life experiences of organizations in ensuring information security when adopting ISMS, including analyzing the four conceptual factors that underlie the new forces.

REFERENCES

Bélanger, F & Crossler, RE 2011, 'Privacy in the digital age: a review of information privacy research in information systems', *MIS Quarterly*, vol. 35, no. 4, pp. 1017-42.

Bharadwaj, AS 2000, 'A resource-based perspective on information technology capability and firm performance: an empirical investigation', *MIS Quarterly*, pp. 169-96.

Chung, D & Chun, SG 2014, 'ADOPTION AND IMPLEMENTATION OF CLOUD COMPUTING SERVICES: A RAILROAD COMPANY CASE', *Issues in Information Systems*, vol. 15, no. 2.

Cisco 2010, *Cisco, Social Media: Cultivate Collaboration and Innovation*.

Crompton, JC 2015, *Gartner's Top 10 Strategic Technology Trends For 2015* January 26, <http://blogs.sap.com/innovation/innovation/gartners-top-10-strategic-technology-trends-2015-webinar-recap-02113450

Curry, A & Stancich, L 2000, 'The intranet — an intrinsic component of strategic information management?', *International Journal of Information Management*, vol. 20, no. 4, pp. 249-68.

Dhillon, G 1999, 'Managing and controlling computer misuse', *Information Management & Computer Security*, vol. 7, no. 4, pp. 171-5.

Duggan, M & Brenner, J 2013, *The demographics of social media users, 2012*, vol. 14.

Edosomwan, S, Prakasan, SK, Kouame, D, Watson, J & Seymour, T 2011, 'The history of social media and its impact on business', *Journal of Applied Management and Entrepreneurship*, vol. 16, no. 3, pp. 79-91.

Ellison, NB 2007, 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210-30.

Eloff, JH & Eloff, M 2003, 'Information security management: a new paradigm', paper presented to Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, pp. 130-136.

Escherich, M 2014, 'Gartner Survey Shows U.S. Consumers Have Little Security Concern With BYOD', viewed 19 May 2014.

Foster, MK, Francescucci, A & West, BC 2010, 'Why users participate in online social networks', *International Journal of e-Business Management*, vol. 4, no. 1, p. 3.

Gartner 2013, *Analysts to Explore Emerging Business Strategies at Gartner Symposium/ITxpo 2013*, Gartner, <http://www.gartner.com/newsroom/id/2613016

Hathi, S 2009, 'How social networking increases collaboration at IBM', *Strategic Communication Management*, vol. 14, no. 1, p. 32.

Hong, K-S, Chi, Y-P, Chao, LR & Tang, J-H 2003, 'An integrated system theory of information security management', *Information Management & Computer Security*, vol. 11, no. 5, pp. 243-8.

Jansen, BJ, Zhang, M, Sobel, K & Chowdury, A 2009, 'Twitter power: Tweets as electronic word of mouth', *Journal of the American society for information science and technology*, vol. 60, no. 11, pp. 2169-88.

Kaisler, S, Armour, F, Espinosa, JA & Money, W 2013, 'Big data: Issues and challenges moving forward', paper presented to System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Kaplan, AM & Haenlein, M 2010, 'Users of the world, unite! The challenges and opportunities of Social Media', *Business horizons*, vol. 53, no. 1, pp. 59-68.

Kazan, W, Font, A, Akmal, M, Grossberg, SD, Penov, FP, Truelove, BN, Chandrasekaran, V & Bahrainwala, S 2012, *PRESENTING CONTENT ITEMS SHARED WITHIN SOCIAL NETWORKS*, US Patent 20,120,151,383.

Kenny, J 2014, *Privacy problems are here to stay*, Blouin News USA,Manhattan, <http://blogs.blouinnews.com/blouinbeattechnology/2014/05/29/privacy-problems-are-here-to-stay/

Kim, HJ 2012, 'Online social media networking and assessing its security risks', *International Journal of Security and Its Applications*, vol. 6, no. 3, pp. 11-8.

Lacity, MC & Hirschheim, R 1993, 'The information systems outsourcing bandwagon', *Sloan management review*, vol. 35, no. 1, p. 73.

Lawrence, S, Peterson, S, Gregory, M, Gourley, CR, Korth-McDonnell, P & Stewart, J 2013, *Linking a retail user profile to a social network user profile*, Google Patents.

Marchand 1985, 'Infonnation management: strategies and tools in transition', *Information Management Review*, vol. 1, pp. 27-34.

Markelj, B & Bernik, I 'Mobile devices and corporate data security'.

---- 2012, 'Mobile devices and corporate data security', *International Journal of Education and Information Technologies*, vol. 6, no. 1, pp. 97-104.

Miller, K, Voas, J & Hurlburt, G 2012, 'BYOD: Security and Privacy Considerations', *IT Professional*, vol. 14, no. 5, pp. 53-5.

Morrow, B 2012, 'BYOD security challenges: control and protect your most sensitive data', *Network Security*, vol. 2012, no. 12, pp. 5-8.

Nolan, R 1994, 'Note on estimating the value of the IT asset', *Harvard Business School*, vol. 9, pp. 195-7.

Okoli, C & Schabram, K 2010, 'A guide to conducting a systematic literature review of information systems research'.

Prensky, M 2011, 'Digital wisdom and homo sapiens digital', *Deconstructing digital natives. New York and London: Routledge*, pp. 15-29.

Rose, C 2013, 'BYOD: An Examination Of Bring Your Own Device In Business', *Review of Business Information Systems (RBIS)*, vol. 17, no. 2, pp. 65-70.

Scholtz, T 2013, *Gartner Says the Nexus of Forces is Transforming Information Security*, 1, Gartner, India, Goa, <http://www.gartner.com/newsroom/id/2613016

Shulman, A 2010, 'The underground credentials market', *Computer Fraud & Security*, vol. 2010, no. 3, pp. 5-8.

Siponen, M & Willison, R 2009, 'Information security management standards: Problems and solutions', *Information & Management*, vol. 46, no. 5, pp. 267-70.

Smith, DM 2013, 'The Top 10 Strategic Technology Trends for 2014', paper presented to Symposium ITXPO 2013.

Sreenivas, V, Narasimham, C, Subrahmanyam, K & Yellamma, P 2013, 'Performance evaluation of encryption techniques and uploading of encrypted data in cloud', paper presented to 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).

Sturdevant, C 2011, 'Socializing the enterprise', *eWeek*, vol. 28, no. 1, pp. 34-.

Subashini, S & Kavitha, V 2011, 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11.

Suhaimi, A, Goto, Y & Cheng, J 2013, 'An analysis of software supportable tasks in information security management system life cycle processes', paper presented to International Conference on Information and Social Science, Nagoya, Japan.

Tokuyoshi, B 2013, 'The security implications of BYOD', *Network Security*, vol. 2013, no. 4, pp. 12-3.

Von Solms, S 2005, 'Information security governance–compliance management vs operational management', *Computers & Security*, vol. 24, no. 6, pp. 443-7.

Webster, F 2014, *Theories of the information society*, Routledge.

Xiang, Z & Gretzel, U 2010, 'Role of social media in online travel information search', *Tourism management*, vol. 31, no. 2, pp. 179-88.

Xu, X 2012, 'From cloud computing to cloud manufacturing', *Robotics and computer-integrated manufacturing*, vol. 28, no. 1, pp. 75-86.

Yeniman Yildirim, E, Akalp, G, Aytac, S & Bayram, N 2011, 'Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey', *International Journal of Information Management*, vol. 31, no. 4, pp. 360-5.

Zissis, D & Lekkas, D 2012, 'Addressing cloud computing security issues', *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-92.