International Journal of Information Management 36 (2016) 215–225

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Information security management needs more holistic approach: A literature review

Zahoor Ahmed Soomro*, Mahmood Hussain Shah, Javed Ahmed

Lancashire Business School, University of Central Lancashire, Preston, UK

ARTICLE INFO

Article history:
Received 24 September 2014
Received in revised form 29 July 2015
Accepted 9 November 2015

Keywords:
Information security
Management
Information security policy
Managerial practices
Business information architecture
Business IT alignment
Cloud computing
Systematic
Information architecture

ABSTRACT

Information technology has dramatically increased online business opportunities; however these opportunities have also created serious risks in relation to information security. Previously, information security issues were studied in a technological context, but growing security needs have extended researchers' attention to explore the management role in information security management. Various studies have explored different management roles and activities, but none has given a comprehensive picture of these roles and activities to manage information security effectively. So it is necessary to accumulate knowledge about various managerial roles and activities from literature to enable managers to adopt these for a more holistic approach to information security management. In this paper, using a systematic literature review approach, we synthesised literature related to management's roles in information security to explore specific managerial activities to enhance information security management. We found that numerous activities of management, particularly development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management, had a significant impact on the quality of management of information security. Thus, this research makes a novel contribution by arguing that a more holistic approach to information security is needed and we suggest the ways in which managers can play an effective role in information security. This research also opens up many new avenues for further research in this area.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

Information and communication technology (ICT) has made online shopping very easy by eliminating the time and space barriers associated with shopping in the high streets. Nowadays, with the help of ICT, 24/7 shopping is possible, with the added advantages of comparing products and prices with just a few clicks. On the one hand, ICT has created unlimited business opportunities; however on the other hand, it has generated new challenges. These challenges include dramatic changes in organisational designs, data management systems, technological implications and information security risks. In the past, information security management was treated as a technical issue (Singh, Picot, Kranz, Gupta, & Ojha, 2013) and the majority of the attention was given to technological solutions; however these did not prove to be sufficient. Some studies (such as, Ernst & Young, 2012; Phillips, 2013; Singh et al., 2013; Siponen, Mahmood, & Pahnila, 2014) suggest that information security issues should also be considered in a management context. These recommendations have raised the interest of the authors to review extant literature regarding the reported role of management in information security.

This paper is aimed at synthesising existing literature to provide an understanding as to why a more holistic approach is needed for information security management. This is achieved through reviewing and analysing the available literature systematically. Literature in the last ten years regarding suggestions for managerial aspects of information security, such as the management role and human contributions, was reviewed and analysed to deduce meaningful insights. This study also tried to explore various managerial activities that are effective for information security management and the level of management at which information security should be dealt within organisations. To achieve these objectives, extant literature regarding the management role in information security was sought from various electronic databases and a search engine. With the use of a systematic literature review process, efforts were made not to miss any relevant and important work on the issue. The literature was analysed for meaningful synthesis with a focus

* Corresponding author.
E-mail addresses: zasoomro@uclan.ac.uk, zahoorahmedsoomro@gmail.com (Z.A. Soomro), mhshah@uclan.ac.uk (M.H. Shah), jahmed1@uclan.ac.uk (J. Ahmed).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.11.009
0268-4012/© 2015 Elsevier Ltd. All rights reserved.

Table 1a
List of keywords and phrases used for literature search.

S. No	Keywords	S. No	Keywords
1	Management	2	Open source and proprietary software
3	Management practices	4	Promising practices
5	Cloud computing	6	Information security
7	Administrative practices	8	Information security management
9	Administration	10	Security breach
11	Administrative activities	12	IT security
13	Business IT/IS alignment	14	Business/enterprise information architecture
15	Information infrastructure	16	Social media and information security
17	Mechanisms for security assessment	18	Open source and proprietary software

Table 1b
List of data bases and search engine used for literature search.

S. No	Name of data base	S. No	Name of data base
1	Academic search complete	2	Brill
3	Business source complete	4	Cambridge journals online
5	Computers & applied sciences complete	6	EBSCOhost EJS
7	Emerald management e-Journals	8	Sage journals online
9	Science direct	10	Google scholar (search engine)

on finding evidence to support the use of a more holistic approach to information security management. As per our knowledge, no study has been conducted to analyse various activities of management for their significance in information security management. Therefore, this paper discusses the management role and managerial practices for effective information security management.

2. Research methods

With a systematic review of existing literature on the management role in information security, this paper was aimed at synthesizing existing knowledge in this domain. This research has two main parts. The first part is about searching for literature, which has a critical impact on the quality of any review article. For this, relevant literature has been identified through a rigorous systematic search process. The second part consists of analysis and synthesis of the identified literature.

2.1. Searching the literature

In order to present a wide-spread overview on the management role in information security, a systematic search process was conducted. A rigorous literature search process was adopted to ensure the validity and reliability. In this review article, reliability is based on selected databases, publications, the covered period and keywords used for literature search which are documented for replication of the literature search process.

For reliability, prior to the literature search a list of key words was developed (see Table 1a) to focus on relevant studies. Thereafter, the literature was sought from eight databases and a search engine (see Table 1b). The specified databases were searched for key words in full text; title or abstract; and as a result; a total of 482 articles were downloaded for further processing.

After downloading, the list was checked for repetitions and duplicate articles were deleted from the list. Subsequently, an abstract of each article was read and further filtering took place. Selection of the most relevant articles was based on predetermined inclusion and exclusion criteria. Academic articles in the field of information security in the management context were included, regardless of the rating of the journal, research methodology or geographic region. However, non-academic articles (white papers and industry magazine articles), books and conference papers were excluded due to lack of methodological rigour. Keeping in view the aim of this study, we only included articles published within the last 10 years. Furthermore, only articles in the English language were included. Finally, to check articles' relevance to the context under study, abstracts were read, and in some instances, other parts of articles were also skimmed for screening purposes. As a result, a total of 67 articles were deemed useful for this study.

2.2. Analysing the identified literature

The results of the reviewed articles were categorised into different management activities as reported in the articles. The publication year of articles shows trends of information security in the management context.

Table 2 shows the trend of the number of articles published yearly since 2004. The quantity of articles in the last three years shows that the research trend in exploring the management role in information security is growing.

Along with the role of management as a whole, various management aspects mentioned in Table 3 were found to have a significant role in information security management.

Table 3 shows various aspects of management having a significant role in information security management. The management role in information security is becoming increasingly important and is gaining the attention of researchers. The literature shows that development and implementation of an effective information security policy has a critical role in managing information security. The other managerial aspects discussed in the literature are the human factor, information policy awareness and compliance training, employee role in data breaches, top management support and integration of technical and managerial activities for successful information security policy. The management role is also highlighted in the security related decisions regarding cloud computing, business IT alignment, developing enterprise information architecture and security issues related to social media. All these activities are important elements of information security management, so management may play an effective role in information security management.

3. Background

In online business organisations, information security management is a primary concern as data breaches, identity theft and other online frauds are fatal to the organisations. Data breach is a very critical issue for the developing world. In the UK alone, 93% of large organisations and 87% of small businesses suffered from

Table 2
Year-wise number of research articles used in this study.

No of articles	04	03	03	08	05	08	08	06	07	10	05
Year of publication	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014 (Up to Sep)

Table 3
Management and its aspects discussed in literature with number of articles.

S. No	Concept	Number of articles
1	Management role is critical for Information Security	12
2	Management role in business IT alignment and security issues	05
3	Management role in enterprise information architecture	03
4	Management role in information infrastructure development	04
2	Effective information security policy, awareness and training impact on information security management	13
3	Role of human factors in information security management	08
4	Information security should be a board level issue	04
6	Employee role in information security breaches	03
7	Employee adherence to security policy and its effects	02
8	Top management support is critical for information security	05
9	Integration of technical and managerial activities for information security effectiveness	04
10	Information security should be dealt as a business issue	03
11	Security issues in cloud computing and management role	06
12	Security risk assessment and management role	06
13	Management role in security issues related to social media	02

data breaches (Ring, 2013). The average cost of a breach in the UK, as reported by Warwick Ashford, (2012), is about £1.4 million, and the recovery period to normal conditions is about 9.3 months. Such studies mostly quantify the costs directly related to data breach incidents, whereas actual costs may be higher if reduction in sales (3 out of 4 customers stop shopping) (Computer Weekly, 2007), decreased profits, downsizing and such other affects are taken into account.

In a single incident of data breach in the USA, 40 million credit card numbers and about 70 million addresses, phone numbers and other personal information details were compromised (Riley, Elgin, Lawrence, & Matlack, 2014). The affected firm spent US$ 61 million in less than one year of the breach for damages and recovery. Along with a cash loss, profit also dropped by 46% in one quarter of the year. The situation in the rest of the country is very similar, as in the year 2013, 619 data breaches were reported which compromised about 58 million personal or financial records (Frenkel, 2014). Costs of data breaches are very high: McKendrick (2013) mentions that on average in the USA, the cost of a security breach incident was US$ 4.4 million for the year 2013, while another survey reported by Sposito (2013) reveals an average cost of US$ 9.4 million for 56% of the firms surveyed. On the other hand, customers' perception about financial risks, especially online payment risks, have a negative influence on online shopping (Hong & Cha, 2013), which is a great threat to the e-tail industry.

The extant literature mentions various reasons for data breach. Jaeger (2013) reports that 38% of the causes of data breaches were lost paper files, 27% related to misplaced portable memory devices and only 11% were due to hackers. Malicious insiders are also a big threat to information security due to the fact that compared to outside attackers they possess a higher level of knowledge, resources, and access (Vance, Lowry, & Eggett, 2013). Access policy violation is another major insider threat, especially when accompanied with malicious intentions of fraud, theft of intellectual property, sale or disclosure of sensitive information and identity theft (Rubenstein & Francis, 2008). The Poneman Institute, 2012 reveals that 39% of all incidents involved negligent employees or contractors, 37% were due to hackers or criminal insiders and 24% were the result of system "glitches". So it may be argued that the human factor is the weakest link in information security (Yeniman, Ebru Akalp, Aytac, & Bayram, 2011). Therefore, there is a need, especially for online organisations, to have a formal information security policy and increased levels of policy awareness and education (Whitman, 2004). The alarming data regarding the human factor in information security breaches invites management researchers to study human behaviour in the information security context. Thus, there is a need to explore various managerial roles and activities including human resources management to safeguard information assets.

4. Analysis of the results

The extant literature has many studies on various aspects of management in the information security management context. To give a clearer picture of different management aspects, this article categorises these as: information security and management; information security policy awareness and training; integration of technical and managerial activities for information security management; human aspects of information security management; and information security as a business issue.

4.1. Information security and management

Various technological solutions for information security have been developed and more are in progress, yet information security issues are a great challenge to most organisations (Grant, Edgar, Sukumar, & Meyer, 2014). Technological solutions also depend on information security policy and organisational strategies, so in the broader aspect, it should be explored from a managerial perspective. Ernst and Young (2012) suggest that information security should be deemed as a Board level priority so its responsibility should not be limited to technical or information officers only. Previously, information security was considered in a technological context (Singh et al., 2013); however studies by Cortada (2010), Chang and Ho (2006), Chang and Lin (2007), Ernst and Young (2012), Ezingeard and Bowen-Schrire (2007), Knapp, Marshall, Rainer Jr., and Morrow (2006), Siponen et al. (2009, 2014), Phillips (2013) and Von Solms and Von Solms (2004), have paved the way to consider information security from a managerial perspective. Table 4 shows literature suggesting a management role in information security management.

In a broader aspect, management has a core responsibility for business affairs, so it has a significant impact on each of the business activities. Information security is primarily a management and business issue, so top managers should be aware of the importance

Table 4
Literature suggesting significance of management in information security.

Author (s) & year	Findings
Chang and Ho (2006)	A firm should have a comprehensive management structure and practices for information security
Knapp et al. (2006)	Top management support is the most critical issue of an information security program
Ezingeard and Bowen-Schrire (2007)	Top management interest and participation is vital for continued improvements in information security systems
Ma et al. (2009)	Management support is possibly the most important component of an effective information security management
Hu, Dinev, Hart, and Cooke (2012)	Top management participation in information security management has a significant influence on employees' attitude and behavior over compliance with information security policies
Whitman and Mattord (2012)	Safe and secure operation of information assets is a senior management responsibility
Kwon et al. (2012)	Top management involvement in policy formulation has a positive impact on information security effectiveness
Phillips (2013)	Management practices have a significant role in information technology system effectiveness

Table 5
List of articles on information security policy, awareness and training.

Author (s) & year	Findings
Whitman (2004)	Information security needs higher levels of awareness, education and policy
Loster (2005)	IT management should develop effective security policies, identify critical assets and encourage communication between IT and risk managers
Chang and Lin (2007)	Effective security policy and practice is vital for information security as only technical measures are not sufficient for this purpose
Hagen et al. (2008)	Information security awareness creation is more effective than other measures
Siponen et al. (2009)	The visibility of information security policy has a positive impact on employees' behaviour towards policy compliance
Ma et al. (2009)	Information security training is possibly the most important measure for its effectiveness, as it increases awareness and understanding
Doherty et al. (2009)	Security breaches can be reduced by protecting a firm's information through an effective information security policy
Puhakainen and Siponen (2010)	Information security policy compliance training has a positive effect on employees' behaviour for compliance
Albrechtsen and Hovden (2010)	Employee participation and knowledge creation incorporate positive changes towards information security awareness and behaviour
Singh et al. (2013)	A comprehensive policy and effective management process for its implementation is necessary for information security management
Rubenstein and Francis (2008)	A major internal threat to information security is access policy violation with malicious intentions
Siponen et al. (2014)	Information security awareness has a significant impact on employees' compliance with information security policy
Parsons et al. (2014)	Awareness training and education have positive impact on employee attitude and behaviour towards information security policy

of information security policy development and implementation and should pay more attention to effectively carrying out pre-set security controls (Chang & Ho, 2006). Organisational factors such as industry type, organisation size and structure strongly influence the implementation of information security management. Large financial organisations are relatively more sensitive to the effectiveness of information security management on account of a higher potential for security threats. Apart from the development of information security policy, management support is also significant for effective implementation of the policy (Knapp et al., 2006; Ma, Schmidt, & Pearson, 2009).

Organisational structure is also enormously important in the management of information security (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Kayworth & Whitten, 2010). Ma et al. (2009) suggest that information security management requires an organisational structure that facilitates reporting, efficient communication, clear authority and quick work flows. The existing literature supports a formal structure for the better management of information security (Kayworth & Whitten, 2010). A decentralised decision system is also advocated for effective information security management such as Pulkkinen, Naumenko, and Luostarinen (2007) suggest that if security decisions at all levels within organisations are implemented, a secure information architecture will be in place to exchange confidential information in the business network.

Development of information security systems is not enough to prevent information intervention from fraudsters. An effective information security governance programme and policy; quality of executive management support (Johnston & Hale, 2009); and continuous reviews and incorporation of certain changes to meet new challenges are key factors to its effectiveness (Ezingeard & Bowen-Schrire, 2007). All these activities need the interest and attention of higher level management, so the top management role may be critical for effective information security management. Cortada (2010) maintains that there has been disparity between information security threats and organisations' responses since the introduction of information technology in business firms. In a global information security survey by Ernst and Young (2012), respondents highlighted lack of top management support, budgetary constraints, absence of skilled human resources and lack of tools as key obstacles to information security effectiveness. Management is responsible for addressing these obstacles and a major role is to be played by the top level management. Therefore, information security managers should adopt a more holistic approach to information security which should include the involvement of the top management of e-tailors.

Technology is unable to provide a reliable solution to organisational information security needs and challenges (Singh et al., 2013). So to overcome the ever challenging issue of information security, a balanced approach of technical, human and organisational factors will be more effective (Werlinger, Hawkey, &

Table 6
Articles on integration of managerial and technical activities.

Author (s) & year	Findings
Ji et al. (2007)	Integration of technological and managerial solutions is pre-requisite for combating identity theft
Young and Windsor (2010)	Organisational data and information resources can effectively be protected by integrating the information security and business planning activities
Kayworth and Whitten (2010)	Effective information security can be ensured by aligning multiple organisational and social factors combined with competence in technology

Beznosov, 2009). Technical factors regarding planning and acquisition of new technologies, budgetary allocations and purchase of hardware and software is at management's discretion. Human factors, for instance, talent hunting, hiring of specialised personnel, employee training and motivation and execution of various policies, are management responsibilities under the umbrella of the human resources management department. Organisational factors, like development of security policy, awareness, compliance and implementation of best practices, are basic measurements for information security (Chang & Lin, 2007). All these activities are the responsibility of a firm's management, so it may be argued that a more holistic approach should be adopted for information security management.

Managerial practices regarding information technology are the driver of IT effectiveness (Phillips, 2013). Management has a variety of practices regarding information technology, while Phillips (2013) has studied only a portion of controlling practices of control objectives for IT (COBIT). Higher investment practices have been evident for more protection and resilience to attack from fraudsters (Khansa & Liginlal, 2009) and budgetary constraints have been realised as an obstacle to information security management (Ernst & Young, 2012). So it may be suggested that not only controlling practices, but all better managerial practices related to information security would make it more efficient and aligned to business objectives. Therefore, information security managers should adopt a more holistic approach to include better managerial practices for effective information security management.

4.2. Information security policy, awareness and training

Apart from the management role as a whole, extant literature also contains studies about various managerial practices, effective in information security management. The most discussed practices are information security policy development, policy awareness and training and policy compliance.

Table 5 represents a brief summary of research on the importance of security policy and the impact of awareness, training and compliance on information security effectiveness.

Information security policy has a significant role in the security of organisational data. Formulation of information security policy and effective implementation are two main contributors to information security effectiveness (Chang & Lin, 2007; Doherty, Anastasakis, & Fulford, 2009; Singh et al., 2013). Siponen et al. (2009) suggest that there should be a clear information security policy in practice for effective compliance as their visibility has a positive impact on employee adherence to information security policy. Existence of an effective information security policy without awareness and training is not very effective; therefore, many authors (such as Hagen, Albrechtsen, & Hovden, 2008; Ma et al., 2009; Puhakainen & Siponen, 2010; Siponen et al., 2014; Whitman, 2004) have suggested that measures should be introduced to enhance information security policy awareness and the provision of training. Whitman (2004) suggests three factors for effective information security management: a comprehensive policy; existence of security control mechanisms; and an awareness and training programme. Management is responsible for all these activities, so a holistic approach to information security management is necessary for effective information security management.

Information security policy awareness makes employees aware of the reasons to keep information assets safe from malicious attacks and other vulnerabilities, while training enables them to effectively carry this out. Hence, both aspects of information security are as important as the policy itself. Table 5 depicts a picture of articles mentioning the role of information security policy compliance and training effectiveness. A large number of articles in this table mentioning the role of training and awareness are evidence of their significance in information security management. A comprehensive information security plan should ensure a means of knowledge transfer about the importance of, and the potential security threats to, information assets with adequate hands-on training and awareness to comply with security policy (Siponen et al., 2014). Policy compliance is dependent on awareness and training: awareness creation is more effective than other measures for information security (Hagen et al., 2008) and training changes the behaviour of employees (Albrechtsen & Hovden, 2010) towards policy compliance.

Compliance training has a critical role in the development of awareness and understanding (Ma et al., 2009) so such trainings may have a significant role in information security effectiveness. Compliance trainings not only create information security awareness but can also drive the behaviour of employees to avoid access policy violation. Access policy violation with malicious intention is a major internal threat to information security (Rubenstein & Francis, 2008), because employees can access the most critical data. Compliance trainings have therefore multiple and significant effects on information security of any organisation (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Awareness creation programmes and trainings are the responsibility of management so inclusion of overall management for a holistic approach to information security may make business information more secure.

4.3. Information security and integration of managerial and technical activities

Extant literature also advocates the integration of technical and managerial activities for effective information security management. As information systems include hardware and software, technical expertise in information systems is as important as managerial professionalism. Table 6 presents literature suggesting the integration of technical and managerial activities.

The literature discussed earlier mentioned the role of management and managerial practices, while some management researchers (see Table 6) have suggested integration and alignment of managerial and technical activities. As information security management can be divided into two major parts, i.e. technical and managerial, so integration of these two aspects will ensure the effectiveness of information security (Ji, Wang, Min, & Smith-Chao, 2007; Kayworth & Whitten, 2010; Young & Windsor, 2010). Management has to deal with the non-technical aspects of information security such as security policy development, awareness training, acquisition of security hardware and software, internal

control and decisions regarding data processing. Without technical support from IT and security professionals, management would find it difficult to manage information security. On the other hand, in existing literature it is evident that IT professionals cannot safeguard information resources without management support and involvement (Singh et al., 2013). Therefore, it may be concluded that the safeguarding of information assets and data security can be ensured through the integration of technical and managerial activities (Young & Windsor, 2010).

4.4. Information security management and the human aspect

Humans are the most critical element in information security management. Within organisations, employees have a two way effect. On one hand, employees may have a negative role, for instance, they may be involved in stealing information with malicious intention and violating access policy, which is a major threat to business organisations (Vance et al., 2013). However on the other hand, employee compliance to security policy, awareness and training will have a significant positive impact on information security. Consequently, there is a need to look at human aspects in detail in order to diminish human deficiencies and to furnish efficiencies towards better information security management. Human resources management is a function of business management, so management can also play a critical role by monitoring, controlling and diverting employee behaviour towards effective information security management.

Table 7 highlights current literature on human aspects of information security management. A firm's management is responsible for all activities of human resources, such as planning, acquisition, motivating, training, behaviour modelling and the controlling of human activities in the organisations, so it becomes the responsibility of management to control and divert these activities towards the security of information. Development of a security policy is not a guarantee for security unless compliance is observed by employees; however security policy awareness and training have significant impact on employee behaviour and intention to comply with information security policy (Puhakainen & Siponen, 2010).

Information security policies have a significant impact on the security of information systems and successful business operations. Hence, the importance of the human factor in information security management cannot be ignored. Extant literature demonstrates that the human factor has a critical role in information security issues. Trcek, Trobec, Pavesic, and Tasic (2007) argue that humans are the most critical factor of information security, and in every information security system there is a complex interaction of human and technical factors. So this study suggests that the role of employees should be considered in the formulation and implementation of information security policy and risk management (Loster, 2005).

Most of the data breaches and information security vulnerabilities are partly due to ignorant employees (Yeniman et al., 2011). In an empirical study, Jaeger (2013) reports causes of data breach as: 38% due to lost paper files, 27% as a result of misplaced memory devices and 11% due to hackers. The reports show that employees are a major cause of data breaches and information security risks as compared to hackers and system failures. The reasons behind employees being a major cause of data breaches may be lack of awareness, lack of compliance to information security policy, access policy violation (Rubenstein & Francis, 2008), lack of training, ill motives (Vance et al., 2013) and deficiencies in managerial control.

Addressing the human deficiencies in information security and data breaches, Hagen et al. (2008) argue that information security awareness creation is the most effective compared to other measures. In this regard, employee training for information security awareness and motivation for compliance has a significant positive impact on information security policy compliance (Ma et al., 2009; Puhakainen & Siponen, 2010) and an indirect negative impact on the number of security breaches and incidents. Management at this point can play an effective role by developing various information security training and awareness programmes. Therefore, a more holistic approach to information security management, which includes human resources management, may make it more effective.

4.5. Information security as an overall business security issue

The extant literature on information security in management context also includes some studies (such as Goles, White, & Dietrich, 2005; Kwon, Ulmer, & Wang, 2012; Von Solms & von Solms, 2005) suggesting the usefulness of viewing information security in a broader context and for it to be regarded as a business security issue (see Table 8)

Information security risk mitigation has a positive impact on the share price and market position of business firms, so it should be treated as a business issue (Von Solms & von Solms, 2005). As top management and board rooms deal with other business issues having an impact on overall business position, information security issues should also be discussed there (Chabinsky, 2014) as they have the same effects. Information security, if discussed at higher level meetings, would get aligned with overall business planning and policies, which would ensure its effectiveness (Kayworth & Whitten, 2010; Young & Windsor, 2010).

Information security should be treated as business security rather than a technical issue (Kwon et al., 2012). If management prioritise the matters of information security and deal accordingly as other security issues are dealt with, there is no doubt that information would be more protected. Protection of data and information from potential threats should be a part of business strategy, as it can give a competitive edge in a vulnerable online business market. Failure or lack of focus of governing boards on information security is a management failure as it does not rank information security vulnerabilities high enough in priority (Atkins, 2013). Whitman (2004) suggests management should become more aware of security threats, increase their awareness and recognise their underestimation of potential risks inherent in the online environment. Therefore, management should adopt a broader approach towards information security, and governing boards should get involved in information security issues.

4.6. Strategic alignment of business and IT/IS and security management issues

The extant literature also discusses the strategic alignment of business and IT/IS for optimisation of information security (see Table 9). The issue is as old as the introduction of IT in business organisations, because effectiveness of information systems' security depends on the strategic business IT alignment (Anthony, Terry Lewis, & Bryan, 2006; Bergeron, Raymond, & Rivard, 2004). Kayworth and Whitten (2010) argue that on account of lack of alignment between business and IT security groups, the security policies and security budgets of the firms do not reflect the business needs. Discussing the technical competencies of information security Kayworth & Whitten, (2010) maintain that it must be complemented with a strategy to align security with organisational strategies, which will result in improved compliance, better policy alignment and fewer security incidents. Business strategies change with market position and environmental uncertainties and lack of consideration of the information security management causes unsynchronised alignment (Chen, Sun, Helms, & Jih, 2008). Therefore, such alignment should be ensured with every change in business strategy as IT security is critical to organisational success.

Table 7
Articles describing the importance of human aspects in information security management.

Author (s) & year	Findings
Loster (2005)	Information security managers should consider human aspects of information security
Trcek et al. (2007)	The most important factor behind ensuring information security is humans, because in every information security system, there is complex interplay between human and technology
Yeniman et al. (2011)	The most common security vulnerability has been human carelessness so; the human factor remains the weakest link in information security
Rhee, Ryu, and Kim (2012)	Effective information security management must consider human aspects along with technological dimensions
Vance et al. (2013)	Malicious insiders possessing a higher level of knowledge, resources and data access are a big threat to information security as compared to outsiders
Jaeger (2013)	The major causes of data breaches are employees' errors rather than hackers

Table 8
Articles suggesting information security as business security issue.

Author (s) & year	Findings
Von Solms and von Solms (2005)	Information security governance is a board level responsibility, as risk mitigating impact has effects on share price and market position
Kayworth and Whitten (2010)	Senior management and information security executives should treat information security as a business issue rather than a technical issue
Goles et al. (2005)	
Kwon et al. (2012)	Information security should be dealt by top management as it is a business security issue
Chabinsky (2014)	Cyber security issues should be discussed in board rooms and executive meetings in place of server rooms

Table 9
Articles suggesting for strategic alignment of business and IT/IS.

Author (s) & year	Findings
Siponen and Oinas-Kukkonen (2007)	It is important to integrate information security into mainstream aspects of the business
Chen et al. (2008)	In a changing business strategy lack of consideration of the information security management issues causes an unsynchronised alignment
Kayworth and Whitten (2010)	Lack of alignment between security group and business, may result in security policies and budgets not reflecting the business needs

As IT is being embedded in business strategies so it becomes more critical, therefore, its security management should not be left to the IT professionals only. Information security management should adopt a holistic approach to include overall business management to act in line with business strategies. Likewise with other business strategies, IT security management should be discussed in top management or board meetings (Chabinsky, 2014).

4.7. Business/enterprise information architecture, infrastructure and security management

A well-managed business/enterprise information architecture is critical to the management of information security (Martin, Dmitriev, & Akeroyd, 2010). Pulkkinen et al. (2007) also argue that enterprise architecture provides the basis for information security management and work as a coordination tool to plan and design solutions to security problems. Favouring the notion Johnso, Lagerström, Närman, and Simonsson (2007) argue that development of information architecture is an established approach for holistic management of information systems and suggest that such architecture models should be amenable to the analysis of the level of information security. So it may be concluded that in the absence of a well-managed enterprise architecture, information security management cannot be effective to safeguard information assets. For an effective information security system management Devece (2013) confirms the vital role of top management, so a holistic approach should be adopted for information security management.

The notion of information architecture is a promising tool for integrating and expanding business processes across the boundaries of business functions (Da Xu, 2011). Describing the varying needs of different business functions, Jung and Joo (2011) argue that different business functions represent distinct information system requirements. Even the same business functions with varied business processes need specialised information architectures (Da Xu, 2011; Devece, 2013). Thus an information architecture model should be a customised one, keeping in view specific business functions and processes. An information architecture integrating business functions and processes is critical for business continuity, so its security management needs the participation of managers from all the business functions.

Cloud-based computing also presents own challenges for managers. On the one hand it promises opportunities to save costs but on the other hand it can possess many legal, ethical and security challenges. Data security is the major issue with cloud computing which reduces the growth of cloud-based computing (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010; Subashini & Kavitha, 2011). The existing literature is very rich on security issues of cloud-based computing, as 33% of cloud computing related articles from 2008 to 11 discuss the security issues, but mostly discuss security from the technical perspective and the technical solutions suggested (Yang & Tate, 2012). Albeit decisions regarding having in-house computing or switching to cloud-based activities seem to be technical, managers from other areas of business have a critical role, given that it includes regulatory implications, information security cultural changes, information security audit implications (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011) ethical and legal issues (Dutta, Peng, & Choudhary, 2013), information audit, information security control and many other business management issues (Marston et al., 2011). Marston et al. (2011) declares an urgent need to understand business related issues surrounding cloud computing. Referring to the role of senior management in information security management, Rebollo et al. (2012) suggest that senior management should define a clear strategy regard-

Table 10
Summary of management, managerial activities and cited work on each.

Author	Management/managerial practices											
	Overall management role	IS security policy making	Human factor/HRM	IS security as a board level issue	IS security awareness and compliance training	Top management support	Integration of technical and managerial activities	IS security as a business issue	Business IT/IS alignment	Information architecture	IS security risk assessment	Cloud computing and security management issues
Whitman (2004)					✓							
Bergeron et al. (2004)									✓			
Alter and Sherer (2004)											✓	
Goles et al. (2005)								✓				
Loster (2005)		✓										
Von Solms and von Solms (2005)				✓				✓				
Chang and Ho (2006)	✓											
Knapp et al. (2006)						✓						
Anthony et al. (2006)									✓			
Chang and Lin (2007)		✓										
Ezingeard and Bowen-Schrire (2007)	✓											
Ji et al. (2007)							✓					
Trcek et al. (2007)			✓									
Hicks (2007)									✓			
Pulkkinen et al. (2007)										✓		
Johnson et al. (2007)										✓		
Hagen et al. (2008)					✓							
Chen et al. (2008)									✓			
Bodin et al. (2008)											✓	
Salmela (2008)											✓	
Doherty et al. (2009)					✓							
Johnston and Hale (2009)						✓						
Ma et al. (2009)					✓	✓						
Siponen et al. (2009)					✓							
Werlinger et al. (2009)					✓	✓						
Albrechtsen and Hovden (2010)					✓							
Kayworth and Whitten (2010)							✓					
Puhakainen and Siponen (2010)					✓							
Young and Windsor (2010)							✓					
Hamlen et al. (2010)												✓
Yeniman et al. (2011)			✓			✓						
Feng and Li (2011)									✓		✓	
Subashini and Kavitha (2011)									✓			✓
Marston et al. (2011)									✓			✓
Hu et al. (2012)						✓						
Rhee, Ryu, and Kim (2012)			✓									
Whitman and Mattord (2012)						✓						
Ryan et al. (2012)											✓	
Yang and Tate (2012)												✓
Rebollo et al. (2012)												✓
Atkins (2013)				✓								
Jaeger (2013)			✓									
Alaeddini and Salekfard (2013)									✓			
Kwon et al. (2012)						✓		✓				
Phillips (2013)	✓											
Rubenstein and Francis (2008)		✓										
Singh et al. (2013)	✓	✓										
Vance et al. (2013)			✓									
Alaeddini and Salekfard (2013)										✓		
Dutta et al. (2013)												✓
Chabinsky (2014)				✓								
Parsons et al. (2014)			✓		✓							
Siponen et al. (2014)					✓							
Dutot, Bergeron, and Raymond (2014)									✓			
Zang (2014)											✓	

ing security of information assets before switching to cloud-based computing.

The decisions regarding adoption of proprietary or open source software depends upon the strategic business needs, particularly confidentiality and security requirements. There are mixed arguments about the comparative security levels of open source and proprietary software (Heron, Hanson, & Ricketts, 2013). In favour of open source software, Bouras, Kokkinos, and Tseliou (2013) conclude that hiding the source code for a system does not provide any additional security and an open code system has an advantage of adjustments for enhanced security measures based upon suggestions by expert reviewers. In contrast, Hoepman and Jacobs (2007) debate that keeping the source closed prevents attackers from having easy access to the information. King, Smith, and Williams (2012) in an empirical study on the security audit of medical software concluded that open source software satisfied 62.5% and proprietary only 19% during security audit. The research regarding open source or proprietary being more secure is still ongoing, so it cannot be decided which one is more secure. Regarding adoption of open source or proprietary software, Caulkins et al. (2013) conclude that open source or proprietary software need multiple considerations, so management from diversified fields should participate in such decision making.

Information security risk assessment is a critical part of risk management, which includes assessing risk using qualitative and quantitative approaches and incorporating means to counter these vulnerabilities (Zang, 2014). The quantitative approaches consider risk exposure on the probability of threat and expected loss on account of the vulnerability of the organisation to the threat (Bodin, Gordon, & Loeb, 2008), whereas qualitative approaches are based on experts' estimated potential losses (Feng & Li, 2011). Keeping in view the complexities of businesses, Feng and Li (2011) suggest that both approaches should be used while assessing the information security risk (Alter & Sherer, 2004; Salmela, 2008). Ryan, Mazzuchi, Ryan, Lopez de la Cruz, & Cooke (2012) argue that each approach has some weaknesses, so management has greater responsibility to develop or adopt either approach or a mixed one and to make adjustments in view of the information infrastructure. Management has also to develop strategies to counter those vulnerabilities, through technical and social means. Management decisions regarding access control, security policy, hardware security, financial provision, security awareness, training and human resources management have a critical impact on the effectiveness of the measures, which is only possible through a holistic approach to information security management.

4.8. Social media and security management

The growth of social media in corporations has opened many opportunities and concerns. The major concern in social media is security of information and privacy. Social media promotes openness and unrestricted information sharing which may not be consistent with an organisation's culture, policies and practices (Fagnot & Paquette, 2010). In lieu of insider threats Fagnot and Paquette (2010) argue that practices on social media and the desired culture of information security in organisations are not compatible. On the contrary, Patel and Jasani (2010) argue that social media presents business with many advantages, particularly their employees, because they can have an open environment in which to discuss ideas, collaborate and interact and exemplify the social media use of IBM. There are many theories on whether or not corporate policies should control the use of social media by employees (Patel & Jasani, 2010). Formulation and execution of policies regarding controlling social media is one of the prime deals of management, so a holistic approach to information security management is recommended.

5. Summary of the literature

Management, with its specialised activities directed toward information security, plays a critical role in the success of information security management. Table 10 represents a summary of various activities of management and exploration studies on their effectiveness in information security.

Table 10 shows activities of management which have a positive role in information security along with a list of researchers who explored these activities. Management's role in information security is gaining importance and increasing the attention of researchers in this area. The literature gives importance to the critical role of management in developing and implementing an effective information security policy to mitigate information security risks. The strategic alignment of business and IT/IS is emphasised by various researchers, concerning its criticality to information security management. The other information security management related issues such as cloud computing, business information architecture management; information infrastructure and vulnerability assessment mechanisms also need cross functional managerial coordination. The human factor in information security is given more space in the literature on account of its significant role in data breach and information security policy compliance. Information security awareness creation and training are also suggested for their significance to the effectiveness of security policy. The other activities discussed in the literature are top management support and the integration of technical and managerial activities for a successful information security policy. These activities have a significant impact on information security and management is responsible for all these aspects. Therefore, it may be suggested to adopt a more holistic approach to information security management that should include all those managerial activities that have a significant impact on the security of information sources.

6. Conclusion

The extant literature in management shows that previously, the management role was explored in relation to organisational performance, productivity and human resource perspectives. The introduction of information technology in businesses and the emergence of online business markets have broadened the scope of management. Current research is more concerned with management's role in information security. The trend of considering IT professionals being responsible for information security has changed and now management is believed to be responsible for information security. Various practices of management are being explored concerning having significance in information security management. As per our information, no such study is available in the literature which has presented all activities in one place, so this is the first study of its nature and thus makes an important theoretical contribution. This study suggests that information security issues should be considered as a responsibility of management, as it has an impact on the market position of a firm (Von Solms & von Solms, 2005).

This study also advises organisations to adopt a more holistic approach to information security management to include: management participation from top level management; human resources management; information security policy development and execution; information security awareness and training; and the involvement of strategic decision makers.

7. Limitations and future research

Although we used a rigorous approach to search related literature, there are still some limitations regarding the used search terms and identified articles. Firstly, only English terms were used and publications in other languages were not included for this study. Secondly, a list of predefined search terms was used which may cause some literature to remain unspotted. An alternative search process with search terms gathered during the analysis of literature should be conducted to find further literature relevant to this review. Empirically testing the findings of this research using quantitative surveys and qualitative case studies could also enhance our understanding of the issues highlighted in this paper. This paper also suggests looking at security related issues in enterprise architecture, information infrastructure and cloud-based computing from the management perspective.

References

Alaeddini, M., & Salekfard, S. (2013). Investigating the role of an enterprise architecture project in the business-IT alignment in Iran. *Information Systems Frontiers*, *15*(1), 67–88.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432–445.

Alter, S., & Sherer, S. A. (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems*, *14*(1), 1.

Anthony, B., Terry Lewis, B. R., & Bryan, R. W. (2006). The leveraging influence of strategic alignment on IT investment: an empirical examination. *Information & Management*, *43*(3), 308–321.

Atkins, B. (2013). Board focus on cyber security: a director's perspective. *Corporate Governance Advisor*, *21*(4), 24–26.

Bergeron, F., Raymond, L., & Rivard, S. (2004). Ideal patterns of strategic alignment and business performance. *Information & Management*, *41*(8), 1003–1020.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164.

Bouras, C., Kokkinos, V., & Tseliou, G. (2013). Methodology for public administrators for selecting between open source and proprietary software. *Telematics and Informatics*, *30*(2), 100–110.

Caulkins, J. P., Feichtinger, G., Grass, D., Hartl, R. F., Kort, P. M., & Seidl, A. (2013). When to make proprietary software open source. *Journal of Economic Dynamics and Control*, *37*(6), 1182–1194.

Chabinsky, S. (2014). The business necessity of cybersecurity: It's not an IT issue. *Security: Solutions for Enterprise Security Leaders*, *51*(3), 56.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361.

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458.

Chen, R., Sun, C., Helms, M. M., & Jih, W. (2008). Aligning information technology and business strategy with a dynamic capabilities perspective: a longitudinal study of a taiwanese semiconductor company. *International Journal of Information Management*, *28*(5), 366–378.

Computer Weekly, (2007). Companies ignore reputation threat from data breaches. Retrieved from http://www.computerweekly.com/news/2240082499/Companies-ignore-reputation-threat-from-data-breaches.

Cortada, J. W. (2010). *How societies embrace information technology: lessons for management and the rest of us*. Hoboken, NJ, USA: John Wiley & Sons, Inc. http://dx.doi.org/10.1002/9780470643938, ch4

Da Xu, L. (2011). Enterprise systems: state-of-the-art and future trends. *Industrial Informatics, IEEE Transactions on*, *7*(4), 630–640.

Devece, C. (2013). The value of business managers" information technology'competence. *The Service Industries Journal*, *33*(7–8), 720–733.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: a critical study of the content of university policies. *International Journal of Information Management*, *29*(6), 449–457.

Dutot, V., Bergeron, F., & Raymond, L. (2014). Information management for the internationalization of SMEs: an exploratory study based on a strategic alignment perspective. *International Journal of Information Management*, *34*(5), 672–681.

Dutta, A., Peng, G., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39–48.

Ernst, Young, (2012). Fighting to close the gap. Retrieved from 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.

Ezingeard, J., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*, *32*(4), 53–72.

Fagnot, I., Paquette, S., (2010). Social media use and employee attitudes towards information security.

Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, *11*(7), 4332–4340.

Frenkel, K. A. (2014). What to do after a security breach. *CIO Insight*, 1.

Goles, T., White, G. B., & Dietrich, G. (2005). Dark screen: An exercise in cyber security. *MIS Quarterly Executive*, *4*(2), 303–318.

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). 'Risky business': perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, *34*(2), 99–122.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397.

Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP)*, *4*(2), 36–48.

Heron, M., Hanson, V. L., & Ricketts, I. (2013). Open source and accessibility: advantages and limitations. *Journal of Interaction Science*, *1*(1), 1–10.

Hoepman, J., & Jacobs, B. (2007). Increased security through open source. *Communications of the ACM*, *50*(1), 79–83.

Hicks, B. (2007). Lean information management: understanding and eliminating waste. *International Journal of Information Management*, *27*(4), 233–249.

Hong, I. B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management*, *33*(6), 927–939.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Jaeger, J. (2013). Human error, not hackers, cause most data breaches. *Compliance Week*, *10*(110), 56–57.

Ji, S., Wang, J., Min, Q., Smith-Chao, S., (2007). Systems plan for combating identity theft-A theoretical framework. *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, 6402–6405.

Johnson, P., Lagerström, R., Närman, P., & Simonsson, M. (2007). Enterprise architecture analysis with extended influence diagrams. *Information Systems Frontiers*, *9*(2–3), 163–180.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129.

Jung, Y., & Joo, M. (2011). Building information modelling (BIM) framework for practical implementation. *Automation in Construction*, *20*(2), 126–133.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 163–175.

Khansa, L., & Liginlal, D. (2009). Quantifying the benefits of investing in information security. *Communications of the ACM*, *52*(11), 113–117.

King, J., Smith, B., & Williams, L. (2012). Audit mechanisms in electronic health record systems: protected health information may remain vulnerable to undetected misuse. *International Journal of Computational Models and Algorithms in Medicine (IJCMAM)*, *3*(2), 23–42.

Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Morrow, D. W. (2006). The top information security issues facing organizations: what can government do to help? *Network Security*, *1*, 327.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219–236.

Loster, P. C. (2005). Managing e-business risk to mitigate loss. *Financial Executive*, *21*(5), 43–45.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business*, *30*(1), 58–69.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—the business perspective. *Decision Support Systems*, *51*(1), 176–189.

Martin, A., Dmitriev, D., & Akeroyd, J. (2010). A resurgence of interest in information architecture. *International Journal of Information Management*, *30*(1), 6–12.

McKendrick, J. (2013). A lesson in risk management. *Insurance Networking News*, *16*(5), 24–26.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176.

Patel, N., & Jasani, H. (2010). Social media security policies: Guidelines for organizations. *Issues in Information Systems*, *11*(1), 628–634.

Phillips, B. (2013). Information technology management practice: impacts upon effectiveness. *Journal of Organizational & End User Computing*, *25*(4), 50–74. http://dx.doi.org/10.4018/joeuc.2013100103

Poneman Institute, (2012). 2011 cost of data breach study: United states. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, *34*(4), 757–778.

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services

business-enterprise architecture as a coordination tool. *Journal of Systems and Software*, *80*(10), 1607–1620.
Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A systematic review of information security governance frameworks in the cloud computing environment. *J.UCS*, *18*(6), 798–815.
Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221–232.
Riley, M., Elgin, B., Lawrence, D., Matlack, C., (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Retrieved from http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p2.
Ring, T. (2013). A breach too far? *Computer Fraud & Security*, *2013*(6), 5–9.
Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? *Wall Street Journal—Eastern Edition*, *251*(100), D1–D2.
Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., Lopez de la Cruz, Juliana, & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*(4), 774–784.
Salmela, H. (2008). Analysing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology*, *23*(3), 185–202.
Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from india and germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. http://dx.doi.org/10.1007/s40171-013-0047-4
Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145–147.
Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: an exploratory field study. *Information & Management*, *51*(2), 217–224.
Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database*, *38*(1), 60–80.
Sposito, S. (2013). In wake of data breaches, banks face huge losses: survey. *American Banker*, *178*(122), 17.
Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.
Trcek, D., Trobec, R., Pavesic, N., & Tasic, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113–118.
Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–290.
Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376.
Von Solms, B., & von Solms, R. (2005). From information security to business security? *Computers & Security*, *24*(4), 271–273.
Warwick Ashford, (2012). Many UK firms underestimate cost of data breaches, study finds. Retrieved from http://www.computerweekly.com/news/2240171040/Many-UK-firms-underestimate-cost-of-data-breaches-study-finds.
Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19.
Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43–57.
Whitman, M. E., & Mattord, H. J. (2012). Information security governance for the non-security business executive. *Journal of Executive Education*, *11*(1), 97–111.
Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, *31*(2), 35–60.
Yeniman, Y., Ebru 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*, *31*(4), 360–365.
Young, R., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, *26*(1), 245–266.
Zang, W. L. (2014). Research of information security quantitative evaluation method. *Applied Mechanics and Materials*, *513*, 369–372.