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

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).

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