Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review

Research in Progress

Sameera Mubarak
School of Information Technology & Mathematical Sciences
University of South Australia
Mawson Lakes Campus, Adelaide
E mail Sameera.Mubarak@.unisa.edu.au

Haneen Heyasat
School of Information Technology & Mathematical Sciences
University of South Australia
Mawson Lakes Campus, Adelaide
E mail Haneen.Heyasat@unisa.edu.au

Santoso Wibowo
School of Engineering and Technology
Higher Education Division
CQUniversity Australia
120 Spencer Street,
Melbourne VIC 3000
Email s.wibowo1@cqu.edu.au

Abstract

Effective information security management is necessary in the success of any organisation, including Small-and-Medium-Sized Enterprises (SMEs). Nonetheless, keeping their security needs met is always a challenge for SMEs. One of the proven ways to manage information security is through applying available international standards, frameworks and best practices. However, choosing a suitable model that addresses the SMEs holistic needs may be an overwhelming task. This systematic literature review formed the initial phase of a larger analytical project of existing models in three categories: risk management models, standards-based models and 'other' models. The review showed that most of models are theoretically conceived but have not been further tested empirically. Hence, their usability is unknown. More in-depth research is required to find a suitable model that may be applicable to all SMEs.

Keywords information security, information security models, information security frameworks, SMEs, information security standards.

1 INTRODUCTION

Protecting SMEs from security breaches is necessary. Like large organisations, SMEs generate and store large amount of customer and supply chain information (Clout, 2018). However, they lack relevant resources to protect their important information like their counter parts. The information security risks for SMEs are similar as large organisations. As pointed out by Montenegro and Moncayo (2016), SMEs are particularly appealing to hackers because of their size. At the same time, they often lack the resources such as technology, staff training, and specialist knowledge that promotes resilience. As a result, hackers pick them off as easy targets. The challenge for SMEs is due to the fact that they lack budget and obtain less support from the senior management (Brodin 2017). Further, convincing the management has been a great hurdle as consequences of attacks are hard to prove with numbers. A recent study by Clout (2018) states that 64% of organisations were unable to handle the cloud security adequately when they were faced with several security challenges including 681 million cyber-attacks on their 1,200 clients.

Although studies tend to emphasis standards and best practice guidelines to overcome information security challenges, the rising number of cyber-attacks and information security breaches on SMEs encouraged us instead to review the existing research on this area. With regard to SMEs, there are only a few studies that focus on various aspects of information security such as threats and challenges, risk management, and information security standards. Standards in general provide uniformity that would ease the understanding and management of concerned areas. In addition, standards help to establish effective governance and suitable risk management. Thus, considering the nature and limitations of SMEs, choosing a right standard or framework that serves their needs has not been explicitly addressed in such models. This paper begins to address that gap by comparing models and frameworks in a systematic review of existing literature. The main research question is: *"What is the main emphasis of existing information security models and frameworks for SME, the specific areas they discuss, the outcomes of those models and the limitations as explained in the paper?"*. Finally, in this paper, we identify overall gaps and future direction for research. In the following sections, we present the methodology of the systematic literature review, its findings, and the direction for future research.

The scope of this systematic research is to conduct an in-depth analysis of literature available on the area of information security and SMEs. This will also help to identify practical application of a model to real scenario and formulate the evaluation. There are no studies available for evaluating information security models in SMEs. Hence this will serve a literature review on the niche area.

2 METHODOLOGY

This section describes the customised guidelines used to perform systematic reviews developed by (Kitchenham, 2004). Kitchenham (2004) proposes four steps to carry out a literature review: (a) identification of resources, (b) selection of studies, (c) data extraction and synthesis and (d) data analysis.

2.1 Identification of Resources

The first step towards resource identification was recognising the relevant keywords. As the research aim was to be detailed in coverage, this search mainly depends on databases and grey literature. To perform a systematic literature review, the initial search of databases yielded four different databases as potential sources of publications: 1) Emerald Insight, 2) Science Direct, 3) Engineering Village, 4) IEEE Xplore and Google Scholar. The 'grey literature area' was addressed in using Google Scholar and the university's library catalogue as data sources to avoid omitting any additional publications. For the initial screening, only titles, abstracts, and keywords were considered and the search was limited to studies published between the years 2008 and 2018, both inclusive. The search strategy depends on the search keywords that were used in the literature review, these key words include the combination of: 'information security management', 'information security models', 'information security standards' and 'SMEs'.

2.2 Selection of Studies

The first iteration involved searching for the selected keywords over four databases and excluding papers based on titles, keywords, abstracts and full texts. This removed articles have one of the following exclusion criteria: (a) did not include the defined key words, (b) were in languages other than English, (c) publication date not within the selected range, and (d) were not peer reviewed.

After a careful observation of the exclusion criteria, 272 papers were removed. The papers selected contain at least one keyword in their title or abstract followed by excluding the publications not belonged

to the criteria. The first iteration ensured substantive reading of abstracts. The second iteration was done to further ensure relevance by skimming the whole article.

2.3 Data Extraction and Synthesis

In the data extraction and synthesis step, the key details from the selected papers were obtained. In this review, the information extracted was divided into the content of the articles discussing information security models in SMEs. In order to obtain and include relevant and important publications to concentrate on, the selection and evaluation depend on a set of inclusion and exclusion criteria. The research was narrowed down through these criteria: (a) papers are published between 2008 to 2018, (b) papers are obtained from peer-reviewed articles, and (c) papers are published in English.

2.4 Data Analysis

PRISMA flow diagram (PRISMA, 2015), in Figure 1 below, shows the final number of selected publications, how many publications were identified and screened for eligibility, how many publications were excluded and why. After the initial search process, 547 publications were found. Removing the duplication with EndNote software reduced the total number to be 292 publications. After checking the titles and abstracts to identify and remove irrelevant publications, there were 120 publications.

In the first eligibility iteration, 172 articles were excluded because of the title and the abstract. In the second eligibility iteration, 100 articles were excluded after full scanning, the researcher found that these articles were not related directly to the topic and will not enrich the research focus. After checking and analysing the full publications, 148 publications were removed and twenty publications remained.

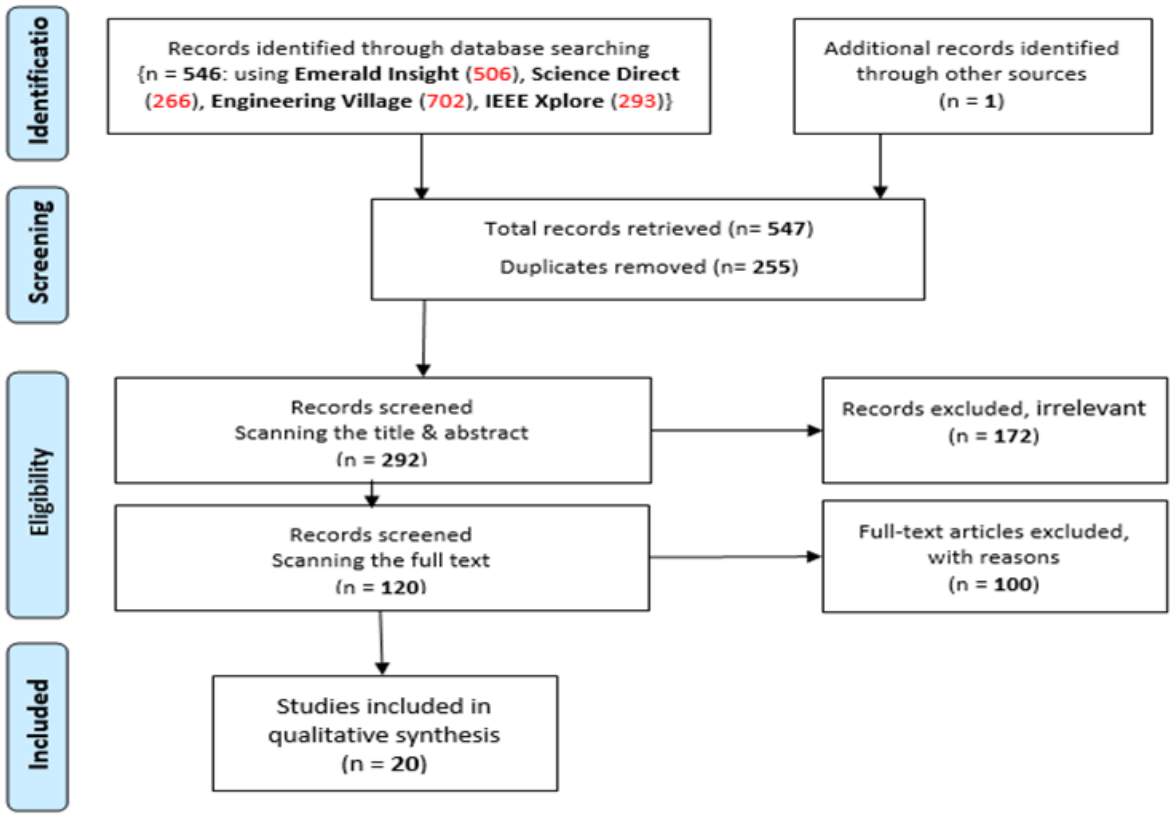

Figure 1: PRISMA Flow Diagram for Systematic Review

2.5 Risk Management Related Models

Table 1 summaries twenty articles selected after going through above mentioned PRISMA flow diagram method. The models listed in Table 1 specifically integrates various risks and their management.

It is evident that there are eight studies that focus on the risk management of SMEs. According to Bayaga and Flowerday (2010), Information Communication Technology (ICT) risk failure in an SME is directly dependent on operational risk management. This conceptual model, however, is yet to be tested. Montenegro and Moncayo (2016) developed a model that formalises the concepts involved in risk

reduction and further developed a metric summarising best practices of OCTAVE-S, MAGERIT and ISO 27005. This framework needs to be tested in real-world situations.

An important finding is revealed by Mayadunne and Park (2016) that the risk taker will invest a larger amount than the risk-neutral enterprise would when protecting the high-risk sets in the group. The results guide information security vendors when tailoring products to suit small businesses. The risk-neutral decision maker will diversify security investment to a greater extent than the risk taker.

Risk Management Models	
Author and Year	Findings of the Model/Framework
Bayaga and Flowerday (2010)	The model shows the relationship between IT operational risk management, causes of IT failure, and performances of SMEs.
Montenegro and Moncayo (2016)	Model for assessment and reduction of information security risks.
Mayadunne and Park (2016)	Information security investment decisions using the expected utility approach.
Santos-Olmo et al. (2012)	The risk taker will invest a larger amount than the risk-neutral enterprises.
Santos Olmo Parra et al. (2016)	MARISMA, a model aimed at risk analysis.
Javaid and Iqbal (2017)	A risk management application model for small enterprises.
Ntouskas et al. (2012)	Open, collaborative environment STORM in order to offer a cost-efficient tool to SMEs for self-managing their security.
Michelberger Jr and Lábodi (2012)	Process-centred enterprise security model handles risk factors.

Table 1. Summary of Risk Management Related Models

Santos-Olmo (2012) have conducted a systematic review of the models for risk analysis and management. It was concluded that most of the models cater to the needs of the large organisations and difficult to apply to SMEs. Santos-Olmo et al. (2016) developed a new methodology, called MARIANA, aimed at carrying out a risk analysis simplified and dynamic, which is valid for SMEs. Javaid and Iqbal (2017) proposed the People, Process and Technology model for the application of risk management frameworks, which offers a chance to small enterprises to integrate appropriate risk management activity in their business operations. The model has been validated through two case studies and could next be tested with a larger sample. Ntouskas et al. (2012) presented a cost-efficient tool (STORM) for SMEs to self-manage their security. However, there is no evidence available about the implementation of this model. Michelberger Jr and Lábodi (2012) proposed an enterprise security model that aims to focus on security requirements in a holistic manner.

2.6 Industry Standards Related Models

Some of the models selected from the literature review that focus on industry standards as their main foundation are included in Table 2. Shojaie et al. (2015) conclude that cultural dimensions can significantly affect organisational administration and achievements such as decision-making, innovation and new practices, work motivation, negotiation, human resource practices, and leadership. The paper highlights that cultural dimensions have a high impact on the success and effectiveness of the ISO 27001 development phases. Al-Ahmad and Mohammad (2012) present the challenges faced by the enterprises when adopting international standards and frameworks. The authors suggest some selection criteria to choose an appropriate model and proper implementation. Although the paper highlights cultural dimensions internationally, this model has yet to be tested with empirical data.

Barlette and Fomin (2008) present the adoption process of the newly published ISO 27001. They state that the legislative environment can play a crucial role in the further growth of security standards adoption. Lewis et al. (2014) focus on information security and supply chains of SMEs. Their findings conclude that the types of information that could be shared among SMEs in a supply chain network when faced with a specific cyber-attack scenario are significant factors. By contrast, Garengo and Biazzo (2013) investigate the process characterising the effective implementation of an integrated management system (IMS) in a leading SME and the main factors enabling the changeover from the adoption of ISO quality standards to the implementation of an IMS. They claim that the new synthesised framework can support the understanding and the implementation of an IMS in SMEs. The study was validated in only one SME and the authors do not claim the generalisability of the framework. In addition, Valdevit et al.

(2009) argue that it remains a challenge for SMEs to maintain the requirements of ISO/IEC 27001. However, the authors propose that the ISO/IEC 27001 certifications for SMEs would be very beneficial.

Industry Standards Related Models	
Author and Year	Findings of the Model/Framework
Barlette and Fomin (2008)	The adoption ISO 27001 standards.
Shojaie et al. (2015)	The effects of cultural dimensions on the development of an ISMS Based on the ISO 27001.
Lewis et al.(2014)	The supply chain and cyber-attack scenario.
Al-Ahmad and Mohammad (2012)	Analysis of the most popular and widely used standards.
Garengo and Biazzo (2013)	A framework for Integrated Management Systems in SMEs.
Valdevit et al. (2009)	An implementation guide for deploying an Information Security Management System.

Table 2. Summary of Industry Standards Related Models

2.7 Other Models

Some of the models or frameworks are unique to specific areas like, cloud computing or digital forensics have been listed under Table 3. Although these models do not fit in the above categories, they contribute in overall information security management.

Brodin (2017) states that a framework used for a large system is not an option for SME, but that the right choice of the model solely depends on the security needs of a company. Sanchez et al. (2008) conclude that the application of the maturity model for SMEs allows them to adapt to change with a minimum of cost, guaranteeing the security and stability of their IS. Browne et al. (2015) suggest that a deficiency exists in the IS security literature because of the tendency to regard IT threat avoidance and IT security adoption as separate behaviours. Barske et al. proposed a Digital Forensic Readiness Framework, which is yet to be tested. Sun and Wang (2013) developed a data security model for cloud computing. The theoretical model adopts efficient encryption mechanisms to protect users' data. Agarkar et al. (2012) designed a Document Management System with certain 'enhanced' features regarding security, compression, abstraction and file versioning for SMEs.

Other Models	
Author and Year	Findings of the Model/Framework
Agarkar et al. (2012)	Document Management System with certain 'enhanced' features regarding security.
Brodin (2017)	Security of mobile devices used in SMEs.
Sanchez et al.(2008)	Information security maturity model to minimise cost.
Sun and Wang (2013)	Data Security Model for cloud computing platform.
Browne (2015)	Synthesises elements of theories into a holistic model on 'Threat Avoidance'.
Barske et al. (2010)	Digital Forensic Readiness Framework.

Table 3. Summary of SMEs Other Models

3 DISCUSSION AND IMPLICATIONS

The above systematic literature analysis reviews twenty articles on information security models, frameworks and best practice guides for SMEs. The finding indicates that there are more in-depth empirical studies needed to test the proposed models. In many of the research papers, there are no follow up studies published to implement and test those models further. The absence of follow-up studies means no conclusions can be drawn regarding the model/framework's successful implementation. Hence, further research is needed to apply and evaluate those models.

The eight articles categorised under 'Risk Management Model' focus on several important factors including the role of ICT in preventing risk factors, investment analysis, and characteristics of risk-taking firms (Bayaga and Flowerday 2010; Mayadunne and Park 2016). However, there is no evidence of the applications of those models and their usability to other SMEs. Hence, an in-depth research is required to conclude the benefits of those theoretical models. There are already available ISO standards

such as ISO for SMEs in Europe, however, little data exists on their experiences of using those models/standards and suggestions for their improvement.

There are six articles listed under the 'Industry Standards Related Models' section. The themes of that section include several factors including the influence of cultural factors while adopting standards, preventing a cyber attack in the supply chain process, and an effective implementation of the integrated management system. We noted that there are no studies available discussing the application of NIST (National Institute of Standards Technology) or COBIT in recent years. This indicates that knowledge of all available standards and their pros and cons for SMEs would be a great resource.

There are six articles grouped under the 'Other Models' category. The range of themes included an evaluation of maturity, cloud security of SMEs and Digital Forensic readiness. By observing several models in different areas, information security might be an overwhelming exercise for SMEs in the selection of the right one. Having one generic model that rules the basic security components may be an ideal step to establish. In addition, some articles focus on security models whereas others focus on frameworks or best practice. These notations can be a puzzle for some SMEs to make the right selection.

4 CONCLUSION AND FUTURE DIRECTION

To answer the research question formulated at the beginning of the paper, we undertook a systematic literature review of existing information security models, standards and frameworks available for SMEs from the year 2008-2018. The articles are categorised in major groups namely: risk management models, Industry standards-based models and 'other' models. The findings show that further research is required to develop a general framework that applies to all SMEs and then to adopt a model based on the specific needs of the organisation.

Since there is a lack of studies on information security management on specific sectors of SMEs, there is a dire need for in-depth studies with empirical data to generate conclusive knowledge. In the next phase of our research, empirical data will be collected through in-depth case studies to understand the needs of SMEs to develop and implement a generalised framework suitable for all SMEs to address fundamental security needs.

5 REFERENCES

Agarkar, M., Borle, A., Deshmukh, A., and Bhagat, M. 2012. "An Enhanced Document Management System for SME," The 2012 IEEE 8th World Congress on Services, 24-29 June 2012, Honolulu, HI, United states.

Al-Ahmad, W., and Mohammad, B. 2012." Can A Single Security Framework Address Information Security Risks Adequately?" International Journal of Digital Information and Wireless Communications (2:3), pp. 222-231.

Barlette, Y., and Fomin, V.V. 2008. "Exploring the Suitability of IS Security Management Standards for SMEs," The 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA.

Barske, D., Stander, A., and Jordaan, J. 2010. "A Digital Forensic Readiness Framework for South African SME's," The Information Security for South Africa (ISSA).

Bayaga, A., and Flowerday, S. 2010. "A Conceptual Operational Risk Model for SMEs: Impact on Organisational Information Technology," The 2010 Information Security for South Africa (ISSA 2010), 2-4 Aug. 2010, Piscataway, NJ, USA.

Brodin, M. 2017. "Security Strategies for Managing Mobile Devices in SMEs: A Theoretical Evaluation," The 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), 27-30 Aug. 2017, Piscataway, NJ, USA.

Browne, S., Lang, M., & Golden, W. 2015. "Linking Threat Avoidance and Security Adoption: A Theoretical Model for SMEs," The 28th Bled eConference: #eWellbeing, 7-10 June 2015, Bled, Slovenia.

Clout, J. 2018. "More Needs to be Done by SMEs on Cyber Security: Angus Taylor. Retrieved from https://www.afr.com/technology/technology-companies/more-needs-to-be-done-by-smes-on-cyber-security--angus-taylor-20180809-h13qh3 Retrieved 10 April, 2019.

Garengo, P., and Biazzo, S. 2013. "From ISO Quality Standards to an Integrated Management System: An Implementation Process in SME," Total Quality Management & Business Excellence (24:3), pp. 310-335.

Javaid, M.I., and Iqbal, M.M.W. 2017. "A Comprehensive People, Process and Technology Application Model for Information Systems Risk Management in Small/Medium Enterprises (SME)," The International Conference on Communication Technologies, 19-21 April 2017, Piscataway, USA.

Kitchenham, B. 2004. "Procedures for Performing Systematic Reviews," Keele, UK, Keele University, (33:1), pp. 1-26.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., and Jones, K. 2014. "Cybersecurity Information Sharing: A Framework for Information Security Management in UK SME Supply Chains," The 22nd European Conference on Information Systems, 9-11 June 2014, Tel Aviv, Israel.

Mayadunne, S., and Park, S. 2016. "An Economic Model to Evaluate Information Security Investment of Risk-Taking Small and Medium Enterprises," International Journal of Production Economics (182:1), pp. 519-530.

Michelberger Jr, P., and Lábodi, C. 2012. "After Information Security–Before A Paradigm Change (A Complex Enterprise Security Model)," Acta Polytechnica Hungarica (9:4), p. 101.

Montenegro, C., and Moncayo, D. 2016. "Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS: Evaluation in Two Ecuadorian SMEs of Automotive Sector," The 6th International Conference on Information Communication and Management, 29-31 October 2016, Hatfield, Hertfordshire, United Kingdom.

Ntouskas, T., Papanikas, D., and Polemi, N. 2012. "A collaborative system offering security management services for SMEs/MEs," The Joint 7th International Conference on Global Security, Safety and Sustainability, 24-26 August 2011, Thessaloniki, Greece.

PRISMA. 2015. "PRISMA Flow Diagram." R http://www.prisma-statement.org/ Retrieved 3 March 2019.

Sanchez, L. E., Villafranca, D., Fernandez-Medina, E., and Piattini, M. 2008. "Practical Application of a Security Management Maturity Model for SMES Based on Predefined Schemas," The International Conference on Security and Cryptography, 26-29 July 2008, Porto, Portugal.

Santos-Olmo, A., Sanchez, L. E., Fernandez-Medina, E., and Piattini, M. 2012. "Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs," The 9th International Workshop on Security in Information Systems, 28 June-1 July 2012, Setubal, Portugal.

Santos Olmo Parra, A., Sanchez Crespo, L.E., Alvarez, E., Huerta, M., and Fernandez Medina Paton, E. 2016. "Methodology for Dynamic Analysis and Risk Management on ISO27001," IEEE Latin America Transactions (14:6), pp. 2897-2911.

Shojaie, B., Federrath, H., and Saberi, I. 2015. "The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001," The 2015 10th International Conference on Availability, Reliability and Security, 24-27 August 2015, Toulouse, France.

Sun, T., and Wang, X. 2013. "Research of Data Security Model in Cloud Computing Platform for SMEs," International Journal of Security and its Applications, 7(6), pp. 97-108.

Valdevit, T., Mayer, N., and Barafort, B. 2009. *Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings*. Berlin: Heidelberg.