Small and Medium-Sized Enterprises' Understanding of Security Evaluation of Cloud-Based Business Intelligence Systems and Its Challenges

Moses Moyo(✉) and Marianne Loock

University of South Africa (UNISA), Pretoria, South Africa
mosesm50@gmail.com, loockm@unisa.ac.za

Abstract. Although small and medium-sized enterprises (SMEs) are encouraged to seek new business opportunities by adopting and utilising cloud-based services, their understanding of threats, vulnerabilities and risk evaluation in the cloud environment, which is crucial in the success of cloud-based business intelligence (BI) adoption, is hardly known. The purpose of this study was to investigate SMEs' understanding of security evaluation of cloud-based BI and associated challenges. A cross-sectional survey was conducted among 109 SME owners/managers from selected South African provinces in which data was collected by means of an electronic and postal questionnaire. The study found that SME owners/managers were aware of conventional security challenges in the cloud-based services including BIs, had a basic understanding of security evaluation in general, understood the need to evaluate cloud-based BIs in terms of physically checking for vulnerabilities and data security and were not proficient in performing security evaluations of cloud-based BIs and relied on experts. SMEs face predicaments in evaluating cloud-based BI due to a lack of appropriate tools they can use. The study concluded that SME owners/managers have a basic understanding of security evaluation and challenges it poses.

Keywords: Cloud-based business intelligence · Security evaluation
Small and medium-sized enterprises

1 Introduction

The availability of many types of cloud-based services such as e-mails, online backup storage, online accounting, customer relations management and cloud-based business intelligence (BI) on the open web is a good development for small and medium-sized enterprises (SMEs) intending to adopt and use these technologies. Cloud-based BI is a concept that describes the components of a BI system delivered as services and data used by the BI system or stored in the cloud [1]. Cloud-based BI or BI in the cloud is the combination of two major cloud computing architectures as a flexible and cost-effective computing platform and BI technology as a support for swift organisational decision making [2]. A survey by Forest Technologies [3] found that the adoption of cloud-based services by South African SMEs was on the rise from 29% in 2014 to 39%

H. Venter et al. (Eds.): ISSA 2018, CCIS 973, pp. 133–148, 2019.
https://doi.org/10.1007/978-3-030-11407-7_10

in 2015 and to 50% in 2016. However, the cloud is an environment attractive for business opportunities to both unsuspecting SMEs and cyber criminals [4] and this requires SMEs to understand how to deal with cyber security challenges when migrating sensitive data, applications and transactions to the cloud [5]. According to Toesland [6], SMEs are a major target of cyber threats because their data are becoming increasingly valuable to cyber criminals and are also potentially easy routes to attacks on large enterprises which conduct transactions on the web. Literature also shows that a growing number of SMEs experience relentless cyber attacks by various threats that can breach data and application security by utilising vulnerabilities in cloud technologies used to offer services [6, 7]. Security breaches in cloud-based services compromise data confidentiality, integrity and availability [8] and this is likely to make SMEs reluctant to adopt and utilise cloud-based BIs.

SMEs are always encouraged to seek new business opportunities by adopting and utilising cloud-based services, despite the fact that their understanding of security evaluation of threats, vulnerabilities and risks in the cloud environment is hardly known. Chances are high that SMEs could end up selecting wrong cloud-based BIs, leading to business failure. According to Moore [9], the prospects of SME owners/managers selecting wrong BIs is usually increased by the presence of many cloud-based technologies as well as the lack of understanding of the technology to be adopted. Empirical studies on the adoption of cloud-based BI by South African SMEs explore the affordability of the technology, awareness and how it has been received among different types of SMEs [10, 11]. SME owners/managers' understanding of security evaluation of cloud-based services is very important for the adoption of cloud-based BIs by South African SMEs. SMEs need to work independently, without the influence of cloud technology vendors or cloud service providers (CSPs) when deciding on the cloud-based BIs and service providers most suitable for their business needs. Therefore, the purpose of this study was to evaluate SME owners/managers' understanding of security evaluation in cloud-based services, particularly BIs, they intended to adopt or had already adopted and challenges associated with the evaluation processes.

The study was guided by the following research questions (RQs):

RQ1: What is the state of adoption of cloud-based services by SMEs in South Africa?
RQ2: What is the level of awareness of security challenges associated with cloud-based services among South African SMEs?
RQ3: How do SMEs evaluate security in cloud-based services prior to adoption?
RQ4: How do SMEs understand security evaluation in cloud-based services?
RQ5: What challenges do SMEs face in evaluating cloud-based services, particularly BI?

The article is organised as follows: introduction, literature review, research methodology, results and analysis, findings and discussion, conclusions and limitations.

2 Literature Review

2.1 SMEs' Awareness of Security Challenges Associated with Cloud-Based Services

Of the three major cloud service models available, i.e. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), in community or public clouds, SaaS is highly recommended for adoption and utilisation by SMEs that have constrained human and financial capacity to purchase and maintain substantial information technology (IT) resources [12]. Unlike in private clouds, low-cost or free-of-charge public clouds present serious security challenges for hosting BIs and sensitive data. Narayanan [13] argues that SMEs using SaaS face security threats related to scam e-mails, online malware, identity scams, misuse of company files on employees' own devices as well as insecure wireless networks. By hosting BIs in SaaS, SMEs lose control over their data and applications to CSPs and this makes it difficult for SMEs to ensure that correct security mechanisms are in place [14] and to ensure application availability when needed [15]. SaaS as a multi-tenant service allows different clients to store their sensitive data in the same location, although it is not intelligent enough to separate that data [16]. By exploiting security vulnerabilities in SaaS, hackers use less sophisticated means to bypass security controls and breach data security for many clients. The implication is that SMEs storing customer data in SaaS could eventually suffer financial loss and face legal liabilities related to data security breaches [17].

In SMEs the importance of security can be undermined by users who are ignorant of security threats and always judge security based mainly on their uninterrupted availability of the respective cloud service [18]. A study by Lacey and James [19] on SMEs as IT service users concludes that SMEs tend to view security as not their problem and therefore always seek to minimise their commitment and involvement in securing their information systems. Separate studies by Moyo and Loock [5] and Toesland [6] conclude that South African SME owners/managers are aware of security challenges associated with the adoption and utilisation of cloud-based BIs and this influences their disposition to adopt the technology. However, it is still not clear how SME owners/managers understand security evaluation in cloud-based BI and how they conduct the evaluations.

2.2 Techniques Used by SMEs to Evaluate Security in Cloud-Based BIs Prior to Adoption

Information system evaluation refers to a systematic process which involves data collection and analysis, making judgements and finally providing useful feedback about the worth or merit of the product or service being evaluated [20]. With regard to SMEs, evaluating cloud-based BIs can provide information on security needed to assist decision making on the most appropriate cloud-based BI for a particular enterprise [21]. The two types of evaluation employed in IT are prior-operational use evaluation (POUE), known as strategic, pre-implementation or formative evaluation, and operational use evaluation (OUE), referred to as post-implementation or summative evaluation [22]. POUE serves to support IT investment justification by predicting estimated

costs and benefits, return on investment and management [22]. On the other hand, OUE is used to establish the impact of the system, providing a better understanding of system performance, and what it has accomplished in terms of its stated objectives [23]. SMEs should conduct POUE on cloud-based BIs in order to establish the security threats, vulnerabilities and risks associated with the adoption of the technology. Using POUE enables SMEs to gather required data to determine whether the cloud-based BIs they intend to adopt meet their needs and expectations in terms of data and application security. Heller [24] encourages SMEs to conduct their own evaluations when selecting cloud-based BIs to check whether most of the features the vendors claim to have are of real benefit to the enterprise.

Currently, there is no literature specific to cloud-based BI evaluation techniques for SMEs besides traditional technical evaluation techniques such as vulnerability scanning and testing, which are suitable for large business organisations with sound finance and IT security personnel [25]. Although the Cloud Security White Paper [26] outlines areas that potential cloud users need to evaluate in order to successfully adopt and use cloud-based services, it does not specify how this evaluation should be done. The White Paper also overlooks the fact that most potential adopters of cloud-based services may not be able to access CSPs due to different geographical locations and legislation. Heiser [27] argues that effective cloud-based services security evaluation processes need pragmatic and flexible use of multiple forms of CSP security posture information. In this regard, SMEs face increasing challenges to obtain that information.

2.3 Challenges SMEs Face in Evaluating Cloud-Based BIs

The existence of different cloud-based BI products in the market presents SMEs with selection challenges because they raise different security issues to be dealt with [28]. Unlike on-premises BIs where enterprises have to evaluate only technical and procedural aspects, evaluating cloud-based BIs requires enterprises to evaluate more areas of the clouds [29]. According to Willcocks [30], evaluation raises the issues of costs, benefits, risk and value of an IT system to an organisation and these could be assessed through an informal or formal evaluation process. CSPs are responsible for technical information infrastructure security whereas client enterprises are responsible for configuration and procedural security. This implies that SME owners/managers should be able to check whether CSP infrastructure is based on commonly used manufacturers that produce patches to deal with identified security vulnerabilities, and documentations of the vulnerabilities and patches are always available [31]. According to Moghe [32], lack of standardisation in cloud-based BIs presents a challenge to SMEs because they would have to devise a variety of strategies in evaluating cloud-based BIs.

3 Research Methodology

The study utilised a descriptive cross-sectional survey design because it enabled easy collection of data from a large sample over a large geographical area at low cost and without the influence of the researcher on respondents. The target population was all SMEs utilising the Internet/web-based systems for business transactions across the

Western Cape, Limpopo, Gauteng, Mpumalanga and Eastern Cape. The network sampling technique was used to select a sample of decision makers/owners/managers in SMEs already using or considering adopting cloud-based services. The information about suitable SMEs was obtained through owners/managers who had knowledge about other SMEs' utilisation of ITs in various provinces/districts. E-mails and phone calls were used to access all potential SME owners/managers, after which the questionnaires were sent either electronically or by post.

To account for questionnaire validity and reliability at the design stage Segars and Gover [33] and Chang et al. [34] encourage researchers to avoid or reduce any potential common method variance (CMV), a common source of bias. CMV bias was reduced by adopting constructs from different sources and mixing the ordering structure of the questions in order to reduce the likelihood of bias towards the theory-in-use. Respondents were assured of the anonymity and confidentiality of the study, and were informed that there were no right or wrong answers but were encouraged to answer questions as honestly as possible [34]. The questionnaire was tested and piloted to eliminate ambiguity of questions among local SME owners who volunteered to test the questionnaire. The reliability of the questionnaire was measured using SPSS and Cronbach's alpha was found to be 0.929. A copy of the survey questionnaire was distributed to a network sample of 380 respondents, in the form of 150 online Google forms and 230 copies posted. The questionnaire response rate was very low with only 113 (29.7%) returned; 109 (28.7%) of the respondents' questionnaires were analysed. Data were then processed using SPSS to generate frequency tables, graphs and descriptive statistics.

4 Results and Analysis

This section presents an analysis of the results of the study. Table 1 shows the distribution of respondents by type of enterprise.

Table 1. Distribution of respondents by enterprise

No. of employees	Frequency f (%)	Combined f (%)	Type of enterprise
10 to 20	21 (19.3)	67 (61.5)	Small enterprise (SE)
21 to 50	46 (42.2)		
51 to 100	25 (22.9)	42 (38.5)	Medium enterprise (ME)
101 to 150	11 (10.1)		
151 to 200	6 (5.5)		
Total	**109 (100)**	**109 (100)**	

The majority of the respondents in this survey, 67 (61.5%), were from small enterprises (SEs), 21 (19.3%) of which employed 10 to 20 workers and 46 (42.2%) employed 21 to 50 workers. The minority of the respondents, 42 (38.5%), were from medium enterprises (MEs), 25 (22.9%) of which employed 51 to 100 employees,

11 (10.1%) employed 101 to 150 employees and 6 (5.5%) employed 151 to 200 employees. In SMEs, the owners/managers are usually responsible for the day-to-day operations of the enterprise and make all the decisions in the adoption and use of cloud-based services in the organisation and may be the ones who use it most.

The results in Table 2 show the distribution of decision makers from which data were collected. 61 (56.0%) respondents were owners responsible for decision making in 16 (14.7%) MEs and 45 (41.3%) SEs; 48 (44.0%) respondents were hired managers who made decisions in 26 (23.9%) MEs and 22 (20.2%) SEs.

Table 2. Distribution of decision makers of cloud-based service adoption in SMEs

	Person in charge of decision making to adopt cloud-based services (n = 109)		
Type of SME	Owner f (%)	Hired manager f (%)	Total f (%)
ME	16 (14.7)	26 (23.9)	42 (38.5)
SE	45 (41.3)	22 (20.2)	67 (61.5)
Total	61 (56.0)	48 (44.0)	109 (100)

In this study, there were more owners than hired managers who were involved in decision making regarding the adoption and use of cloud-based services and other ITs.

4.1 RQ1: What Is the State of Adoption of Cloud-Based Services by SMEs in South Africa?

Responses regarding the state of adoption and use of cloud-based services, including cloud-based BIs, are shown in Fig. 1.

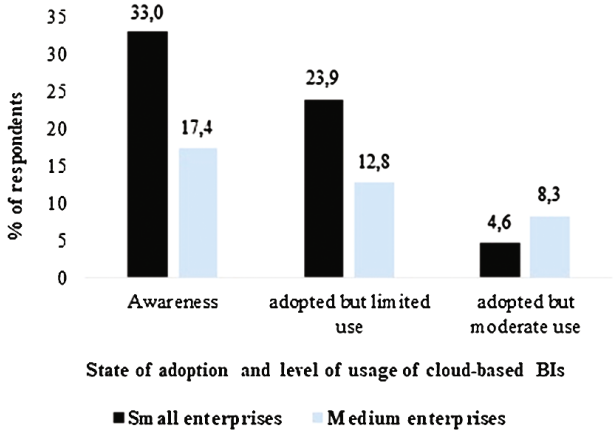

Fig. 1. State of adoption and use of cloud-based services

The results show that 36 (33.0%) of the respondents from SEs and 19 (17.4%) from MEs, overall 55 (50.5%) of the respondents, indicated that their enterprises were at the awareness stage of adopting cloud-based services. 40 (37%) respondents, consisting of 26 (23.8%) from SEs and 14 (12.8%) from MEs, indicated that their enterprises had adopted cloud-based technologies but put them to limited use. A minority, 14 (13.0%) respondents, 5 (4.6%) from SEs and 9 (8.3%) from MEs, had adopted cloud-based services and used them moderately.

4.2 RQ2: What Is the Level of Awareness of Security Challenges Associated with Cloud-Based Services Among South African SMEs?

Table 3 shows respondents' rating of their awareness of security challenges that affect the adoption of cloud-based services, particularly cloud BIs. A 4-point Likert-type rating scale from very much aware (4) to not aware (1) was used.

Table 3. Ratings of awareness in security challenges in cloud-based services

Security challenges	Ratings of selected security challenges in cloud services n = 109					
	Very much aware n (%)	Moderately aware n (%)	Little aware-ness n (%)	Not aware n (%)	Mean	Std. Dev
Hacking activities on web	62 (56.9)	36 (33.0)	7 (6.4)	4 (3.7)	3.4	0.9
Data theft	46 (42.2)	45 (41.3)	7 (6.4)	11 (10.1)	3.2	0.9
Data unavailability	48 (44.0)	34 (31.3)	7 (6.4)	20 (18.3)	3.0	1.1
Competitors sharing same data storage	46 (42.2)	25 (22.9)	18 (16.5)	20 (18.3)	2.9	1.1
Privacy breaches	36 (33.0)	35 (32.1)	27 (24.8)	11 (10.1)	2.9	1.0
Data confidentiality breaches	46 (42.2)	43 (39.4)	9 (8.3)	11 (10.1)	2.8	1.1
Information leakage in cloud	35 (32.1)	38 (34.9)	22 (20.2)	14 (12.8)	2.8	1.1
Loss of control of data to CSP	30 (27.5)	39 (35.8)	31 (28.4)	9 (8.3)	2.8	0.9
Difficulties in data migration to other providers	32 (29.4)	25 (22.9)	41 (37.6)	11 (10.1)	2.7	1.0
Ransomware effects	20 (18.3)	14 (12.8)	46 (42.2)	29 (26.6)	2.5	1.2
CSP closing down without notice	21 (19.3)	25 (22.9)	34 (31.2)	29 (26.6)	2.3	1.1

The results reveal that respondents' awareness of all key security challenges was rated as moderate (mean of 3.4), with hacking activities on the web topping the list, down to 2.7 for difficulties in data migration to other providers. The two least rated security challenges were awareness of the possibility of CSP closing down without

notice (mean of 2.5) and ignorance of ransomware effects (mean of 2.3), which indicated respondents having very little awareness. An overall average mean score of 2.8 indicates that the majority of the respondents had nearly moderate awareness of most challenges being investigated.

4.3 RQ3: How Do SMEs Evaluate Security in Cloud-Based BIs Prior to Adoption?

To answer this question, respondents were asked how they selected cloud-based services they were currently using or intended to use, as seen in Fig. 2. The results show that 28 (25.7%) of the respondents from SEs and 6 (5.5%) respondents from MEs, with an overall minority of 34 (31.2%), searched for cloud-based services possibly for adoption from the web on their own. On the other hand, 39 (35.8%) of the respondents from SEs and 36 (33.0%) from MEs, i.e. the majority of 75 (68.8%) of the respondents, indicated that the cloud-based services they adopted or intended to adopt were recommended to them by experts in cloud technology. These results show that SMEs were also able to use the web to search for cloud-based services that met their needs.

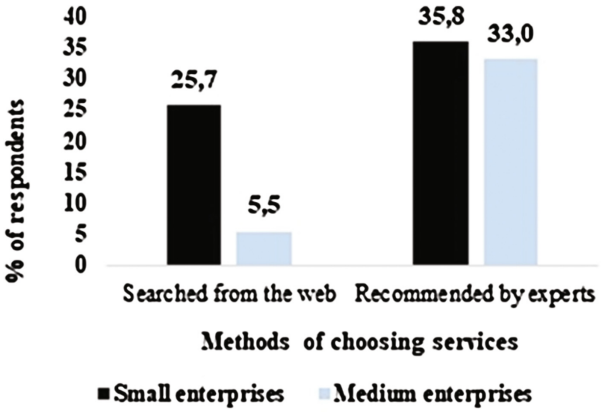

Fig. 2. Methods used to select cloud-based services by SMEs

Respondents were asked to rate the importance of evaluating a number of key aspects of security in the cloud. The results are shown in Table 4.

Based on the Likert scale of 4 (very important) to 1 (not important), the majority of the respondents, 102 (93.6%), rated password protection as the most important security aspect that must be evaluated, and 7 (6.4%) rated it as important, with a mean score of 3.9. Application programming interfaces were rated the second most important, with a mean of 2.6, with 32 (29.4%) respondents rating it very important, 70 (64.2%) as important and 7 (6.4%) as less important. The average mean of 3.1 shows that respondents regarded all the aspects as important to consider when evaluating cloud-based services.

Table 4. Ratings of the importance of evaluating selected security aspects

Security aspect evaluated	Ratings of importance of evaluation of security aspects n = 109					
	Very important f (%)	Important f (%)	Less important f (%)	Not important f (%)	Mean	Std. Dev
Password protection	102 (93.6)	7 (6.4)	0 (0)	0 (0)	3.9	0.5
Security management services	91 (83.5)	11 (10.1)	7 (6.4)	0 (0)	3.7	0.7
Firewall configurations	82 (75.2)	27 (24.8)	0 (0)	0 (0)	3.5	0.9
Software security	75 (68.8)	34 (31.2)	0 (0)	0 (0)	3.4	0.9
Up-to-date security patches	73 (67.0)	36 (33.0)	0 (0)	0 (0)	3.3	0.9
Contingencies and backups	73 (67.0)	29 (26.6)	7 (6.4)	0 (0)	3.3	0.9
Vendor or provider reliability	68 (62.4)	41 (37.6)	0 (0)	0 (0)	3.2	1.0
Organisational security and risk management	62 (56.9)	31 (28.4)	16 (14.7)	0 (0)	3.1	1.0
Human resources security	41 (37.6)	39 (35.8)	29 (26.6)	0 (0)	2.8	1.0
Physical security of provider	41 (37.6)	41 (37.6)	27 (24.8)	0 (0)	2.8	1.0
Security guideline by provider	48 (44.0)	41 (37.6)	11 (10.1)	9 (8.3)	2.8	1.1
Interoperability and portability	39 (35.8)	34 (31.2)	36 (33)	0 (0)	2.7	1.0
Application programming interfaces security	32 (29.4)	70 (64.2)	7 (6.4)	0 (0)	2.6	0.9

4.4 RQ4: How Do SMEs Understand Security Evaluation in Cloud-Based Services?

To determine the respondents' understanding of security evaluation in cloud-based BIs and related services, respondents were asked to rate a given number of statements on a Likert scale of 5 (strongly agree) to 1 (strongly disagree) (Table 5). The mean scores ranged between 4.6 and 3.8, close to strongly agree and agree, and the average overall mean was 4.2 for all items. This shows that respondents understood security evaluation in cloud-based services in terms of a variety of aspects indicated. The overall average mean rating score of 4.2 shows that respondents had a generic understanding of what each aspect meant with regard to cloud-based BIs.

As a follow-up, respondents were asked to indicate how they understood evaluation of cloud-based BI and other services, as seen in Table 6 below.

The majority of the respondents understood security evaluation of cloud-based services as assessing the effectiveness of the following security controls: data security - 91 (83.5%) strongly agreed and 18 (16.5%) agreed, with a mean of 4.8; application

Table 5. Understanding of security evaluation in cloud services

Aspect	Ratings of security evaluation understanding n = 109					
	Strongly agree f (%)	Agree f (%)	Not sure f (%)	Disagree f (%)	Mean	Std. Dev
Checking information asset accessibility publicly by unauthorised cloud users	64 (58.7)	45 (41.3)	0 (0)	0 (0)	4.6	0.5
Checking the chances of being tricked into signing a contract by a poor-performing CSPs	64 (58.7)	36 (33)	0	6 (5.5)	4.4	0.9
Checking that expected results match CSPs' claims	55 (50.5)	45 (41.3)	6 (5.5)	3 (2.8)	4.4	0.6
Checking whether CSP employees can access and manipulate enterprise data without permission	47 (43.1)	46 (42.2)	16 (14.7)	0 (0)	4.3	0.7
Checking the level of control of data in the cloud I will have	48 (44)	47 (43.1)	13 (11.9)	3 (2.8)	4.3	0.7
Identifying and understanding exposure to risk and capability of managing it	35 (32.1)	65 (59.6)	6 (5.5)	3 (2.8)	4.2	0.6
Checking reported cases on whether unexpected changes to data/information in a particular cloud once occurred	46 (42.2)	36 (33)	18 (16.5)	9 (8.3)	4.1	1.0
Checking whether processes or functions on clouds can be manipulated by outsiders	28 (25.7)	56 (51.4)	18 (16.5)	7 (6.4)	4.0	0.7
Identifying the possible sources of conflict with the cloud provider in terms of SLAs	26 (23.9)	51 (46.8)	22 (20.2)	10 (9.2)	3.9	0.7
Checking reports on periods of time when the cloud was unavailable to the users	26 (23.9)	42 (38.5)	32 (29.4)	9 (8.3)	3.8	0.9

security - 84 (77.1%) strongly agreed and 25 (22.9%) agreed, with a mean of 4.8; system security - 73 (67.0%) strongly agreed and 36 (33.0%) agreed, with a mean of 4.7; network security - 84 (77.1%) strongly agreed, 18 (16.5%) agreed and 7 (6.4%) were not sure, with a mean of 4.7, and physical security of data centres from cloud providers - 36 (33.0%) strongly agreed, 53 (48.6%) agreed, 11 (10.1%) were not sure and 9 (8.3%) disagreed. From these results, it could be deduced that SME owners/managers had a clear understanding of what security evaluation entailed and the critical areas of the cloud to be evaluated.

Table 6. Meaning of evaluation of cloud-based services and BIs

Aspect	Ratings of what security evaluation means for each control n = 109					
	Strongly agree f (%)	Agree f (%)	Not sure f (%)	Disagree f (%)	Mean	Std. Dev
Data security	91 (83.5)	18 (16.5)	0	0 (0)	4.8	0.4
Application security	84 (77.1)	25 (22.9)	0	0 (0)	4.8	0.4
System security	73 (67.0)	36 (33.0)	0	0 (0)	4.7	0.5
Network security	84 (77.1)	18 (16.5)	7 (6.4)	0 (0)	4.7	0.6
Physical security of data centres for cloud providers	36 (33.0)	53 (48.6)	11 (10.1)	9 (8.3)	4.1	0.9

4.5 RQ5: What Challenges Do SMEs Face in Evaluating Cloud-Based Services, Particularly BIs?

Respondents indicated the extent to which common security challenges were likely to affect their effort in evaluating cloud-based services they intended to adopt and use, as seen in Table 7. The results are arranged with regard to their mean score of the Likert rating scale from very serious (4) to not serious (1).

Table 7. Ratings of the common security challenges in evaluating cloud-based services

Security aspect	Ratings of security evaluation challenges n = 109					
	Very serious f (%)	Serious f (%)	Less serious f (%)	Not serious f (%)	Mean	Std. Dev
Evaluating vulnerabilities in interface of applications	82 (75.2)	27 (24.8)	0	0	3.8	0.4
Security that cloud providers claim they give	68 (62.4)	32 (29.4)	9 (8.3)	0	3.5	0.6
Getting information from cloud providers	71 (65.1)	18 (16.5)	20 (18.3)	0	3.5	0.8
Ability of provider to meet requirements	48 (44)	52 (47.7)	9 (8.3)	0	3.4	0.6
Authentication of users/applications/processes	58 (53.2)	40 (36.7)	11 (10.1)	0	3.4	0.7
Robustness of separation between data belonging to different customers	64 (58.7)	25 (22.9)	20 (18.3)	0	3.4	0.8
Lack of tools to evaluate cloud-based BIs	46 (42.2)	54 (49.5)	9 (8.3)	0	3.3	0.6
History of data breaches in a particular cloud	48 (44.0)	43 (39.4)	18 (16.5)	0	3.3	0.7

(*continued*)

Table 7. (*continued*)

Security aspect	Ratings of security evaluation challenges n = 109					
	Very serious f (%)	Serious f (%)	Less serious f (%)	Not serious f (%)	Mean	Std. Dev
Certainty about survival of cloud provider	61 (56.0)	30 (27.5)	9 (8.3)	9 (8.3)	3.3	0.9
Establishing the physical location of the cloud provider	47 (43.1)	46 (42.2)	7 (6.4)	9 (8.3)	3.2	0.9
Physical security evaluation of provider	46 (42.2)	34 (31.2)	18 (16.5)	9 (8.3)	3.1	1.0
Trust of provider and employees	55 (50.5)	18 (16.5)	27 (24.8)	9 (8.3)	3.1	1.0
Enterprises with which the cloud was shared	48 (44.0)	41 (37.6)	20 (18.3)	0	3.1	1.1

The results show that respondents rated all items as challenges to the evaluation of security in cloud-based services as serious to nearly very serious, with mean scores ranging from 3.1 to 3.8. Evaluating vulnerabilities in the cloud-based application interfaces posed the most serious challenges as indicated by the majority of the respondents: 82 (75.2%) rated this very serious and 27 (24.8%) rated it serious, with a mean score of 3.8. The security challenge rated the least serious was evaluating the enterprises with which the cloud-based services were shared: 48 (44%) respondents rated it as very serious, 41 (37.6%) rated it as serious and 20 (18.3%) as less serious, with a mean of 3.1. With the majority of the respondents regarding these challenges as serious, this affects the manner in which SMEs evaluate cloud-based services and eventually adopt and use the services. The overall mean score of 3.4 indicates that respondents considered the majority of the security aspects as serious.

5 Findings and Discussions

This subsection presents the findings of the study based on the research questions.

5.1 State of Adoption of Cloud-Based BI by SMEs in South Africa

The state of adoption of cloud-based services such as BI by SMEs has been found to be in three stages: awareness (50.4%), adoption with limited use (36.2%) and adopted with extensive use (12.9%). These findings are consistent with the projections made independently by Forest Technologies [3]. As a new technology for SMEs, the level of awareness of its existence is generally high among SME owners/managers.

5.2 Level of Awareness of Security Challenges Associated with Cloud-Based Services Among South African SMEs

Hacking activities on the web, data confidentiality breaches in the cloud, data availability issues, various forms of data theft, sharing of the same data storage with competitors and data privacy breaches were commonly known by the majority of respondents, whereas challenges related to ransomware and possibility of the provider closing down without notice were least known by most of the respondents. Technical paper by Muntean [1] and Boonsiritomachai et al. [11] allude to a number of security challenges that SMEs face in their quest to adopt cloud-based services. A study by Moyo and Loock [5] also attributes the poor adoption and use of cloud-based services, particularly BIs, to several security challenges that SMEs have to overcome if they are to successfully adopt and utilise these services. SMEs are aware of the devastating effects of various threats in cyber space on their business profitability if they risk adopting cloud-based BI without due evaluation [26].

5.3 SMEs' Evaluation of Security in Cloud-Based BIs Prior to Adoption

The majority (68.8%) of the SME owners/managers relied on experts' opinions regarding which service to adopt and were not able to perform security evaluations themselves. However, 31.2% of the owners/managers were able to perform searches for cloud-based services on the web and evaluate the services before adoption and use. The majority of respondents were aware of the importance of evaluating cloud services before adopting them. The majority (75% to 94%) of the owners/managers thought that password protection, security management services and firewall configurations were very important areas to be evaluated in cloud-based BIs. Although a number of studies encourage SMEs to evaluate the cloud before adoption, they provide piece-meal suggestions on what and how to evaluate envisaged security challenges [26].

5.4 SMEs' Understanding of Security Evaluations in Cloud-Based BIs

SME owners/managers understood security evaluation in cloud-based services from a practical perspective in which they preferred checking information assets for vulnerabilities that could possibly be accessed publicly by unauthorised cloud users, guarding against being tricked into signing a contract by a poor-performing cloud provider and verifying that the process or function provided the expected results as claimed by the cloud provider. Literature emphasises that cloud clients such as SMEs have an obligation to understand technical infrastructure security, data security, standards and procedures pertaining to the cloud-based service they want to adopt [31]. Similarly, Antoo et al. [4] point out that SMEs should understand the evaluation of cloud-based services in terms of security vulnerabilities, threats and risks in internal network controls, data storage and service level agreements (SLAs) of their CSPs with regard to their requirements and security policies. The Cloud Security White Paper [26] emphasises the importance of having a clear understanding of how to evaluate the physical infrastructure in the data centre, applications hosted by CSPs that manage clients' data, and the policies and procedures used to continuously maintain security in

the cloud environment. The findings of this study suggest that SME owners/managers should be actively involved in the process of evaluating cloud-based BIs to make correct decisions about services to be adopted.

5.5 Challenges that SMEs Face in Evaluating Cloud-Based Services, Particularly BIs

While SME owners/managers may have some understanding of security evaluation in cloud-based services, they also face serious challenges in evaluating the identified areas due to complications that range from accessibility to legal issues [5]. The major obstacle is a lack of proper tools to evaluate cloud-based services to determine how secure the services and CSP are [26]. SME owners/managers lack technical skills in evaluating IT systems and they tend to rely on expertise from outside the organisation, which is also too expensive for them [29]. It is difficult for SME owners/managers to force CSPs to divulge every detail about the service they provide, although legally they should do so. Not all CSPs can provide a totally secure service as they are unable to vet their clients who use a virtual space. Due to different geographical locations, SME owners/managers are unable to evaluate the physical security of data centres and also to monitor unauthorised access to their data by the provider's employees [9]. Generally, studies which encourage the adoption of cloud-based services by SMEs do so on the strength of benefits that adopters may derive from the technology while overlooking or downplaying the security challenges that come with the cloud [15]. On the other hand, SME owners/managers are not prepared to risk their businesses by adopting services they are not certain about.

6 Conclusions

The majority of the SME owners/managers surveyed understood security evaluations in terms of physically checking for vulnerabilities in cloud-based BIs and the security of data that were likely to be accessed publicly by unauthorised cloud users, guarding against being tricked into signing contracts by a poor-performing and unreliable cloud provider and verifying whether the process or function was capable of providing the expected results as claimed by the CSP. Although the majority of SME owners/managers were not able to perform security evaluations, their level of understanding of the need for these evaluations was fair. SME owners were also aware of the areas of cloud-based BIs that needed to be evaluated. A number of SME owners/managers conducted their own search of cloud-based services on the web, deviating from the traditional practice of depending on expertise from outside their businesses. The ability of SME owners/managers to evaluate cloud-based services was affected by a number of factors beyond the control and comprehension of the adopters.

7 Limitations and Further Research

The findings of this study cannot be generalised to all SMEs in South Africa due to the fact that it was a cross-sectional study whose results may change within the foreseeable future as more easy-to-use technology emerges and the adopters improve their understanding of security issues. Secondly, the use of postal/online questionnaires have their own strengths and shortfalls, resulting in a very low response rate which constrains generalisation. Further studies are in progress in using the findings of longitudinal research in developing a security framework to evaluate cloud-based BIs by SMEs in South Africa.

References

1. Muntean, M.: Considerations regarding business intelligence in cloud context. Informatica Economica **19**(4), 55–67 (2015)
2. Tamer, C., Kiley, N., Ashrafi, N., Kuilboer, J.: Risks and benefits of business intelligence in the cloud. In: Proceedings of the Northeast Decision Sciences Institute Annual Meeting, p. 86 (2013)
3. Forest Technologies: SME Survey 2015: The Greening of the SME Sector (2015). http://www.smesurvey.co.za/press.html
4. Antoo, M., Cadersaib, Z., Gobin, B.: PEST framework for analysing cloud computing adoption by Mauritian SMEs. Lect. Notes Softw. Eng. **3**(2), 107–112 (2015)
5. Moyo, M., Loock, M.: South African small and medium-sized enterprises' reluctance to adopt and use cloud-based business intelligence systems: a literature review. In: The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016), pp. 250–254 (2016)
6. Toesland, F.: Why SMEs are big targets for cybercrime (2016). https://www.raconteur.net/technology/why-smes-are-big-targets-for-cyber-crime
7. Madzima, K., Moyo, M., Dzawo, G., Mbodila, M.: Mobile security threats: a survey of how mobile device users are protecting themselves from new forms of cybercrimes. In: Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015, pp. 123–133 (2015)
8. Akinola, K.E., Odumosu, A.A.: Threat handling and security issue in cloud computing. Int. J. Sci. Eng. Res. **6**(11), 1371–1385 (2015)
9. Moore, J.: Business Intelligence Takes to Cloud for Small Businesses (2014). https://www.cio.com/article/3237786/business-intelligence/9-ways-youre-failing-at-business-intelligence.html#tk.drr_mlt
10. Mohlameane, M.J., Ruxwana, N.L.: The potential of cloud computing as an alternative technology for SMEs in South Africa. J. Econ. Bus. Manage. **1**(4), 396–400 (2014)
11. Boonsiritomachai, W., McGrath, M., Burgess, S.: A research framework for the adoption of business intelligence by small and medium-sized enterprises. In: 27th Annual SEAANZ Proceedings for Small Enterprise Association of Australia and New Zealand Conference, 16–18 July 2014, pp. 16–28 (2014)
12. Chang, V., Kuob, Y., Ramachandrana, M.: Cloud computing adoption framework: a security framework for business clouds. Future Gener. **57**(2015), 24–41 (2015)
13. Narayanan, S.: Tackling the cyber security challenges faced by SMEs (2013). http://www.cisoplatform.com/profiles/blogs/tackling-the-cyber-security-challenges-by-smes

14. European Union Agency for Network and Information Security. Security framework for governmental clouds (2015). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds
15. Chou, T.: Security threats on cloud computing vulnerabilities. Int. J. Comput. Sci. Inf. Technol. (IJCSIT) **5**(3), 79–88 (2013)
16. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V.M., Freire, M., Inacio, P.R.M.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. (IJIS) **2013**(1), 1–62 (2013)
17. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
18. Oza, N., Karppinen, K., Savola, R.: User experience and security in the cloud – an empirical study in the Finnish Cloud Consortium. In: The 2nd IEEE International Conference on Cloud Computing Technology and Science, pp. 621–628 (2010)
19. Lacey, D., James, B.E.: Review of Availability of Advice on Security for Small/Medium Sized Organisations (2010). https://ico.org.uk/media/about-the-ico/documents/1042344/review-availablility-of-security-advice-for-sme.pdf
20. Mussa, M., Kipanyula, M.J., Angello, C., Sanga, C.A.: Evaluation of Livestock Information Network Knowledge System (LINKS) based on user satisfaction definition of information system evaluation. Int. J. Inf. Commun. Technol. Res. **6**(8), 115–130 (2016)
21. Wise, L.: Evaluating business intelligence in the cloud (2016). http://www.cio.com/article/3041639/business-intelligence/evaluating-business-intelligence-in-the-cloud.html
22. Al-yaseen, H.M.: Challenges of implementing healthcare information systems in developing countries: using a mixed method research. J. Emerg. Trends Comput. Inf. Sci. **3**(11), 1521–1529 (2012)
23. Al-Yaseen, H., Al-Jaghoub, S., Al-Shorbaji, M., Salim, M.: Post-implementation evaluation of healthcare information systems in developing countries. Inf. Syst. J. **13**(1), 9–16 (2010)
24. Heller, M.: How to Select the Best Self-service BI Tool for Your Business (2017). https://www.cio.com/article/3235394/business-intelligence/how-to-select-the-best-self-service-bi-tool-for-your-business.html#tk.cio_rs
25. Kazim, M., Zhu, S.Y.: A survey on top security threats in cloud computing. Int. J. Appl. Comput. Sci. Appl. **6**(3), 10495–10500 (2015)
26. Cloud Security White Paper.: How to Evaluate the Data Security Capabilities of Cloud-Based Services (2011). http://www.carestream.com/WhitePaper_Cloud-Security.pdf
27. Heiser, J.: How to Evaluate Cloud Service Provider Security (2016). https://www.gartner.com/doc/3275117/evaluate-cloud-service-provider-security
28. Agostino, A., Soilen, S.K., Gerritsen, B.: Cloud solution in business intelligence for SMEs – vendor and customer perspectives. J. Intell. Stud. Bus. **3**(2013), 5–28 (2013)
29. Vacca, J.R.: Security in the Private Cloud. Taylor and Francis, Denver (2017)
30. Willcocks, L.: Evaluating information technology investments: research findings and reappraisal. J. Inf. Syst. **2**(1992), 243–268 (1992)
31. Shimamoto, CD.: How to Evaluate Cloud Security? (2015) https://www.techsoup.org/support/articles-and-how-tos/how-to-evaluate-cloud-security
32. Moghe, P.: 6 Hidden Challenges of using the Cloud for Big Data and How to Overcome Them (2016). https://thenextweb.com/insider/2016/04/12/6-challenges-cloud-overcome
33. Segars, A.H., Grover, V.: Strategic information systems planning success: an investigation of the construct and its measurement. MIS Q. **22**(2), 139–163 (1998)
34. Chang, S.J., Van Witteloostuijn, A., Eden, L.: From the editors: common method variance in international business research. Int. J. Bus. Stud. **41**(2), 178–184 (2010)