Evaluation of Cloud Business Intelligence Prior to Adoption: The Voice of Small Business Enterprises in a South African Township

Moses Moyo(✉) and Marianne Loock

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

Abstract. The purpose of this qualitative study was to provide an insight into how small business enterprises from a South African township evaluated cloud business intelligence solutions and the challenges faced. The study found that despite limited knowledge in security evaluation and lack of easy-to-use techniques for small business enterprise, decision makers conducted basic and unsystematic evaluation of cloud business intelligence prior to adoption. Unsystematic security evaluation was mainly on data security, access control functionalities such as authentication, cloud service providers' security, trust and reliability and financial risks. The study concluded that an easy-to-use security evaluation framework for cloud business intelligence solution tailored for small business enterprises was a necessity to overcome challenges among enterprises in South African townships in order to enhance good security practices when adopting cloud services.

Keywords: Security evaluation · Data security · Cloud business intelligence · Small business enterprises

1 Introduction

The acceptance and use of cloud business intelligence solutions (CBIs) are not yet consolidated in South Africa, therefore, it is relevant to question their adoption by small business enterprises (SBEs). CBIs can be used as some decision support systems to strategically increase business viability by reducing operational disruptions and competition among (SBEs) [1, 2]. However, several security challenges deprive SBEs of the benefits these technologies, particularly in townships where there is scarce information technology (IT) specialists [3]. With the growing awareness and acceptance of cloud services among South African SBEs, the need for security evaluation becomes a vital process to undertake when adopting CBI [4]. Without conducting security evaluation, there is a possibility that SBEs can adopt and use CBIs without evaluating security risks, a practice that may expose the enterprise information system to cyber security threats and risks. Apparently, the problem is that, many CBIs are still novel to SBEs who have limited knowledge of inherent security vulnerabilities, threats and risks that need to be assessed [5]. This is worsened when CBIs depend on cloud computing technologies that are prone to several security threats and breaches which compromise

M. Themistocleous et al. (Eds.): EMCIS 2020, LNBIP 402, pp. 449–460, 2020.
https://doi.org/10.1007/978-3-030-63396-7_30

information systems and potentially jeopardise enterprise operations, viability and competitiveness [6]. With several South African SBEs adopting and using cloud services, data breaches also increase exponential resulting in the loss of millions of Rands in revenue annually [7, 8]. A report by [9] shows that, close to 60% of the cyber-attacks in South Africa target SBEs. These reports underscore that SBEs migrating data to the cloud cannot be spared of data breaches and therefore, the need for these enterprise to be cautious when adopting CBIs.

The problem is that whenever SBEs in townships decide to adopt and use any new technologies the owners and managers of these enterprises, who are not security specialists, assume responsibilities in security evaluation. Consequently, basic knowledge in security evaluation among decision makers becomes a crucial requirement for selecting appropriate and secure CBIs. Currently, there is scarce information about how SBEs select the CBIs they use to support business activities.

The purpose of this study is to contribute to existing knowledge on the security evaluation of CBIs among disadvantaged SBEs in South African townships by critically examining the practices of these enterprises when adopting cloud services. This qualitative study was designed to answer the following research questions:

a. *What security evaluation techniques do SBEs use when selecting cloud business intelligence prior to adoption?*
b. *What challenges do SBEs face in implementing the evaluation techniques?*
c. *What do SBEs consider to be important aspects in security evaluation of CBIs?*

The structure of the article is as follows: Sect. 2: Review of related works; Sect. 3: Research design and methods, Sect. 4: Analysis of results and interpretations; Sect. 5: Discussions of findings and Sect. 6: Conclusions and limitations.

2 Review of Related Works

CBI combines a cloud computing platform and BI technology in a user-friendly, flexible and cost-effective manner to support fast decision making in an enterprise [10]. SBEs in South African townships with weak financial resources and limited IT knowledge to acquire and implement traditional business intelligence (BI) can benefit from CBIs. Dashboards and reports present results in formats that are easy to interpret and facilitate actionable decision-making without involving expensive data analytics experts [11]. However, security vulnerabilities, threats and risks in the cloud environments pose as main challenges [3, 6]. Cloud computing security should be the core reason to inspire SBEs to adopt the use of cloud services [6, 11]. Ideally, CBIs should be more secure than on-premise information systems because CSPs are supposed to be specialised in providing security in the cloud [12]. Conversely, literature by [13] and [14] shows that security in cloud environments is difficult to attain due to vulnerabilities in the technologies used and increasing cyber threats. With SBEs gradually realising the importance of CBIs as decision support systems, adopting these technologies without proper security evaluation defeats the intended purposes.

Adopting CBIs and migrating data to the cloud is a big decision that requires SBEs to evaluate a range of security aspects and other functionalities that are crucial to the

enterprise operations [1]. Security evaluation entails analysis of a solution to determine its degree of compliance with a stated security model, security standard, or specification [15]. Similarly, [16] posits that security evaluation plays an important role in identifying existing threats and potential vulnerabilities of the system so as to avoid them in future systems. SBEs need to perform security evaluation in order to verify that security measures and functionalities are in place accurately and effectively comply with the individual user's security requirements. Furthermore, CBIs security evaluation can be used to verify CSPs security trust, assurance and reliability in service provision [10]. Presently, there is very thin literature on security evaluation of cloud services by SBEs particularly in South Africa. This study is vital in providing knowledge and insights on personal experiences of SBEs decision making on CBIs evaluation prior to adoption. Findings from the empirical study will narrow the knowledge gap of security evaluation by SBEs in township that public and academic researcher could have been taking for granted.

3 Research Design and Data Collection Method

This study utilised a qualitative design for the researcher to interact with participants in their natural settings where they were free to express their experiences about the phenomenon being studied [17], security evaluation in CBIs. A purposive sample of five decision makers from SBEs already using ITs to support business operations was used. Participants with experience in IT systems and basic knowledge in cloud services were regarded as rich source of information relevant to CBIs being investigated [18]. The use of a purposive sample was supported by [19] who argues that it was effective in attaining data saturation with a few participants. The inclusion criteria were based on the knowledge of CBIs and the intention to adopt by SBEs already using IT systems to support business operations.

Face-to-face semi-structured interviews were done to collect data from the selected participants. The use of semi-structured interview guide provided the researcher with an opportunity to understand the security evaluation from the point of view of decision makers. The interview sessions lasted an average of 30 min.

3.1 Ethical Issues

An ethical clearance was obtained from the relevant institution before data collection. Prior to the interview, each participant signed the consent form which stipulated ethical issues such as privacy of identity, anonymity and confidentiality of participants, protection of participants and other researchers from harm, voluntary participation and withdrawal and avoiding the use of deception. Participants were identified as P1, P2, P3, P4 and P4.

3.2 Trustworthiness

In ensuring trustworthiness and credibility, we followed recommendations by [20] of asking interviewees to confirm at the end of the interview and data transcriptions that they agreed with the transcripts.

4 Analysis and Interpretation of Results

Qualitative data analysis was conducted using Atlas ti 8 following thematic analysis method [21]. Themes and sub-themes important to this article were those that related to the evaluation of CBIs and the challenges that decision makers faced.

4.1 Evaluation Strategies Used by Decision Makers in Selecting Cloud Business Intelligence Solutions

The attestations highlight how decision makers assessed CBIs to be adopted. The evaluation strategies used included active assessment of security features in CBIs, asking for information from friends and CSPs, searching for information about CBIs from internet and using trial versions.

Assessing Data Security in Cloud Business Intelligence Solutions. Although participants were non-IT specialists, the need to assess data security in CBIs was regarded as very important to decision makers:

> *'I do my own evaluation bit by bit, comparing different solutions looking for possible security weaknesses in the interface, data conversions, data retrieval',* [P1].
> *'I use trial or free versions to check if security features work and also to find out if the system support data migration easily. I do not want to struggle when moving data to the cloud',* [P3].
> *'I check how secure the systems is in terms of interface used, particularly what takes place during logging-in and logging-out. Ideally, I would want to check how many users can access my account if I leave the app without logging out',* [P5].

The extracts show that security evaluation centres on vital information about data security in the application. It is also clear that decision makers make effort to check applications for security weaknesses. These findings show that decision makers evaluating data security in CBIs was a key strategy which should be done to protect business assets.

Using Information About Cloud Service Providers to Assess Security, Trust and Reliability in Service Provision. CSPs play a crucial role in providing CBIs as service hence the need to evaluate CBIs by examining the history of security, trust and reliability of the providers. The extracts confirm this:

> *'I make background checks of a providers to see how reliable they are in providing the services and how they performed in terms of security. I also use discussion forums to check what is being said about the app I am interested in',* [P2].
> *'I look for formation on previous data breaches which occurred with provider…how they were dealt with…. I request information from providers on how safety of data storages',* [P4].

Consulting colleagues to get information and advice on new IT solutions and what to do was another strategy suggested by partipcants:

'I prefer to consult my colleagues whenever there is new technology I want to use then I decide from what they say…I compare what my colleagues tell me with what I find from the internet concerning the new technologies. I visit web sites of service providers to familiarise myself with their product', [P5].

The four attestations show a growing need for decision makers to be initiative in the evaluation of IT solutions to support their decision making process for the adoption. Easy access to information about CBIs and CSPs can make it feasible for decision makers to find and learn much about the solutions they intend to adopt.

Using Checklists to Evaluate Cloud Business Intelligence Solutions. The use of checklists in the evaluation of CBIs prior to adoption was raised by two participants only. This shows that decision makers were not aware of existing tools that could be used to guide them when evaluating CBIs:

'I use checklists from the Web to assess how secure the app is and how to use it. Checklist guides me on those vital aspects of the cloud I should evaluate. At least I get an idea of what should be done although some of the guidelines are too difficult to follow', [P3].
'There are many checklists one can use to evaluate cloud services, the problem is that they are specific to certain product and not others. All the same they are important as a starting point. It is different from adopting a solution without assessing it', [P5].

The use of checklists by some of the decision makers in evaluating CBIs highlighted the importance of having an easy-to-use evaluation tool for non-IT end users. This would encourage them to try things out on their own or with minimum assistance from specialists.

Inspecting Physical Security of Data Centres Participants indicated that decision makers preferred to ascertain how secure the physical infrastructure was against various natural disasters, burglary and unauthorised access.

'I am not confident with cloud technologies; I cannot take any chance without assessing physical security of the place where the data will be stored. It is my desire to check whether the service provider has the capabilities of protecting the computers where data will be kept', [P1].
The situation becomes difficult when it comes to physical security in the cloud as it is difficult to access the place where data is stored and check how secure it. All now depends on how trustworthy the provider is. I would like to visit the site where data is stored so that I see how secure it is and who access the data [P2].

Assessing of physical security of data centres was viewed as an important aspect of security evaluations in CBIs which decision makers could conduct to ascertain the security of their data.

4.2 Description of Challenges Faced in the Evaluation of Cloud Business Intelligence

Although decision makers were forthcoming which strategies in evaluating CBIs, challenges faced were counterproductive to their efforts. Three main challenges were identified from the interviews with participant as presented.

Limited Knowledge on How to Evaluate Security in Cloud Business Intelligence Solutions. Excerpts from participants show that limited knowledge in assessing CBIs by decision makers was a major challenge that stifled their effort to recommend the adoption of cloud services. The two excerpts below support this finding;

> *Without the know-how of cloud technologies, it's difficult to tell which cloud business intelligence is safe to adopt. I have little technical knowledge about security and how to evaluate IT solutions. Something may appear appealing but hiding threats,* [P2].
> *Lack of evaluative skills of emerging information technologies is detrimental to the enterprise as we continue to rely on old methods of data management. In my opinion, being able to use an app is much easier than evaluating it. With people like me, if the app is working everything is fine*, [P4].

This finding shows that decision makers value knowledge and skills for evaluating IT solutions for business use, but they acknowledge having limited knowledge to accurately assess CBI security measures as setback. Without basic knowledge in security evaluation of CBIs, decision makers would not be able to select the appropriate application.

Inadequate Knowledge of Existing Tools Used in the Evaluation of the Cloud Business Intelligence Solutions by Decision Makers. Extracts from participants 3 and 5 reveal that decision makers faced challenges related ignorance of tools suitable for use in evaluating CBIs.

> *I am not sure if we have simple techniques to guide small business in selecting cloud services. I think small businesses are treated like large businesses in IT solutions. It is difficult for use to assess cloud business intelligence advanced techniques and tools for big companies*, [P3].
> *It is difficult for us small businesses to select cloud services because we cannot systematically evaluate them properly due to lack of tools for that purpose. .... everyone thinks we should follow the big businesses even if there are very clear differences in our needs*, [P5].

From these attestations, participants were aware of differences between SBEs and large business needs and that the existing evaluation tools are designed for latter. The assertions confirm that SBEs expect to have evaluation tools tailored for these enterprises.

Difficult in Getting Relevant Information from the Cloud Service Providers About the Cloud Business Intelligence Solutions. Although participants alleged that they used information from various sources to evaluate CBIs, finding such information from CSPs and vendors was difficult. Some of the information was misrepresenting the solutions and outdated. The extracts illustrate the claims:

> *It is difficult to find the right information about cloud apps from the Web because providers do not cooperate. Some attract customers with fancy marketing language but offering service with deplorable results*, [P1].
> *I realised that some of the sites offering business intelligence are never updated for a long time. I doubt if they still offer the solutions. ... I avoid such providers, ... the trend is noticeable in many situations where the offers are exaggerated making it difficult to tell the appropriateness of the services from the little information available*, [P2].

The finding shows the importance of historical and current information about CBIs and CSP in the evaluation process. However, the inability of CSPs to provide such

information makes it difficult for decision makers to evaluate CBIs on their own. Information from outdated web sites and challenges in accessing current information deterred decision makers from conducting proper evaluation of CBIs.

4.3 Important Aspects Considered When Evaluating Cloud Business Intelligence Solutions

Participants suggested four aspects that should be considered when decision makers decided to evaluate CBIs.

Examining the Level of Knowledge and Skill Needed to Operate or Use the Application. The level of knowledge and skills needed to use CBIs was an important area to evaluate so that decision makers avoid making mistakes that lead to breach security procedures in the applications.

> *It is important to check how easy it is to use or learn to use the apps before I make costly mistakes. I would avoid any apps difficult to use or subscribe. I do not want to spend much time learning to use new apps…I do not want to make mistakes that corrupt information…,* [P2].
> *I want to maintain my business in good working condition…so any solution I want to use should be perfect and should not provide glitches, the time I take to learn the solution is important…. it tells me how difficult it is. …skills needed to use the application without making blunders is important to consider in this case*, [P4].

These two utterances illustrate that decision makers regarded knowledge about how CBIs worked crucial in the evaluation process. The amount of effort needed to use or learn how to use the solution was very important in the evaluation process.

Data Security, Portability and Application Interoperability in the Clouds. Some participants expressed that decision makers should prioritise data security, portability and application interoperability when evaluating CBIs.

> *I look at how sensitive the data is and decide which one to put on the cloud… I make sure that it is safe to use and that my information and data will be protected especially when it is on the Web where the chances of information being corrupted or stolen is always high*, [P2].
> *The first thing I may consider is checking whether data can be uploaded to the cloud storage without being converted to another format and … the new system can open the data files without corrupting it…. data remains unchanged during migration for future use*, [P4].

These assertions show that data security and portability should be major considerations when migrating sensitive data to the cloud. There was need to consider how data integrity was maintained during migration to the cloud.

Security Functionalities and Compliance of Cloud Business Intelligence Solutions. Some excerpts conveyed the notion that decision makers should expected certain security functionalities to be available in CBIs and should consider checking their deployment and effectiveness prior to adoption.

> *I will be interested in features used to protect data during migration and while being stored in the cloud*, [P3].
> *I will consider the functionality in the app, how they are deployed and used by end users. …I expect cloud service providers to comply with security regulations but some can flout these regulations as they wish*, [P4].

This finding confirms that decision makers should be concerned with key security features, functionalities and how secure they were. Decision makers were also supposed to consider providers compliant to security standards.

Financial Risks Associated with the Cloud Business Intelligence Solution. Financial benefits than risks arising from security data breaches and system unavailability were very important considerations recommended in the evaluation process. The extracts illustrate the need for such considerations:

> *It is wise to look at financial benefits of the app to the enterprises first and then look at the pitfalls. At times, one can be blinded by many benefits and overlooks risks which surface when using the application,* [P1].
> *I will consider financial risks of using cloud business intelligence…if I am to subscribe to a service provider, I want assurance that service disruptions will not prejudiced the enterprise in any way,* [P4].

Financial risks that arise from additional subscription fees imposed on the enterprise on supposedly free app were important considerations.

> *I am sceptical of financial risks incurred from supposedly free product that demands payment when in use or one is locked out. …evaluation should check for such payments to avoid disruptions,* [P5].

Decision makers were supposed to take into account financial risks due to losing control of sensitive data to CSPs and litigations.

> S*toring data in the cloud is giving up control to providers who can do whatever they want with it. … financial loses arise if the provider's employees access and leak sensitive data to the public. Paying for legal costs is one thing we cannot afford,* [P3].

The findings show a multiple of aspects that led to potential financial risks should be considered during the evaluation process of CBIs. Possible unethical practice by some service providers and their employees were financial risks with negatively impact profits that SBEs would avert. Ligations arising from leakages of sensitive enterprise by CSPs and their employees compelled SBE to consider assurance from the CSP on the security financial responsibilities.

5 Discussion of Findings

In this section, discussions of findings are made for each research question.

5.1 What Security Evaluation Techniques Did SBEs Use When Selecting Cloud Business Intelligence Prior to Adoption?

The findings show that decision makers conducted unsystematic security evaluation in cloud services as a managerial obligation to safeguard enterprise information assets. The key strategies involved assessing access control, authentication and security functionalities using interfaces of CBIs, as recommended by [5]. Similarly, [2] suggest that SBE should use of trial versions to verify the claims made by CSPs in providing secure applications. Decision makers used CSPs' history information in providing

security, trust and honouring contracts in the evaluation process. This finding was consistent with existing literature by [22] who emphasise the importance of getting reports about security posture of CSPs. Decision makers consulted friends and at times IT specialist for advice on the security of CBIs they were interested in before adoption. Consultation during the evaluation of new technologies is a good practice within social network of business persons and makes it easy for decision makers to have up-to-date information [23]. However, information shared in networks by friends may not flow to others out of the network thereby delaying the evaluation process. Another danger is circulating inaccurate information among SBEs facing similar problems and the may not be applicable to needs of other enterprises. The use of checklists in security evaluation is a standard practice [24], increasingly used for self-sustenance among SBEs. These findings show basic unsystematic security evaluating of CBIs prior to adoption by SBEs was a good initiative is security good practice.

5.2 What Challenges Did SBEs Face in Implementing the Evaluation Techniques?

Decision makers face three major challenges in security evaluation of CBIs namely: 1) limited knowledge to systematically evaluate CBI; 2) lack of knowledge about appropriate tools for evaluating CBIs for SBEs; and 3) difficulties in getting relevant information from the CSPs about the CBIs. These findings showed that decision makers appreciated the importance of basic knowledge in security evaluation for them to be actively involved in the selection of CBI solutions. According to [2] posit that knowledge about security evaluation of IT solutions is crucial in assisting users in selecting appropriate solutions for their enterprises. Existing evaluation tools were difficult for decision makers to use as they required technical knowledge in security evaluation. SBEs require CBIs which are easy-to-use without requiring much training [5]. A difficult-to-use CBI was construed as a security challenge which led users to make mistakes that result to security breaches. Decision makers found it difficult to get current information about CBIs from CSPs who did not respond to enquiries, or provided outdated information on their web sites. Previous studies in IT solution evaluations emphasise on the importance of accurate information needed when evaluating new technologies [23]. Without correct up-to-date information about CBIs, it was difficult for decision makers to proceed with evaluations.

5.3 What Did SBEs Consider to Be Important Aspects in Security Evaluation of CBIs?

Several considerations were recommended for successful CBIs evaluating by SBEs. Decision makers were aware that the cloud was prevalent of data security breaches and therefore prioritised evaluation of CBIs vulnerabilities and threats that would affect data portability and application interoperability. A study by [23] encourages potential cloud service users to evaluate data security, portability and application interoperability to avoid frustrations of data and vendor lock-in. CSPs fail to provide tools, techniques and standard data formats, services or interfaces for clients to manage data and service

portability due differences in technologies used [10]. This consideration was important for decision makers to make beforehand, to ensure data integrity and availability.

Operational security functionalities, features and ratings of CBIs can be used in the evaluation process. These aspects intended to show decision makers how secure the CBIs behaved when in use [3]. Poor-quality CBIs can be very costly and difficult to rectify once the contract is operational. Consequently, decision makers needed to evaluate this aspect prior to the adoption of CBIs. This shows the extent to which decision makers mistrusted CSPs in providing quality and secure CBIs.

The evaluation of cloud deployment model particularly public clouds was another important consideration that should be made. CSPs provide different public clouds that pose data and application portability challenges that SMEs might find it difficult to resolve by themselves [25]. CSP security, trust and reliability were considered important for evaluation because these were part of contractual obligations. One of the major expectations of enterprises from CSPs is the trust in keeping data safe and providing services as stipulated in the contracts [1]. Decision makers could assess reliability by checking the performance of a CSP against the service level agreement over a duration of a year using information from publications or requested by clients [26]. Adopting CBIs from untrusted and unreliable CSPs can lead to financial loss which SBEs seek to avoid.

Financial risks were found to be important aspect that should be evaluated. Different CSPs use their own pricing models which the SBEs should check to avoid running into unnecessary costly financial risks that may lead to unforeseen financial risks [27]. This would assist decision makers to select reliable CSPs with competitive pricing schemes. The level of knowledge and skills needed to operate or use the applications was also considered important when evaluating CBIs because it ultimately affected data security when the user accidentally used the application wrongly. This finding is supported by [4] who posit that an easy to learn and use application tends to lead to fewer security breaches by users compared to a difficult one.

6 Conclusions and Limitations

The study concluded that: 1) the security evaluation strategies used by SBEs were unsystematic and were characterised by the use of unorthodox means; 2) decision makers faced challenges of limited knowledge in security evaluation, lacked knowledge of tools for evaluating CBIs; inability to get correct and up-to-date information from the CSPs needed for CBIs evaluation; and 3) decision makers considered data security, portability and interoperability in the clouds; operational and security functionalities and ratings of CBIs; environment where CBIs were used, financial benefits and risks of the CBIs and CSP trust and reliability as the most important areas to evaluate. The study also concluded that security evaluation of CBIs by SBEs was very important and the enterprises required assistance to overcome challenges in evaluation tools and increase in basic security knowledge need to conduct basic evaluations.

Limitations of the study were that of the sample used was too small to generalise to a large population of other townships in South Africa. Based on the findings of this study, a security evaluation framework for CBIs tailored for SBEs was needed to

improve good practice among these enterprises. The findings of this study have implications on the future design and developing security evaluation tools appropriate for use by SBEs intending to adopt different cloud applications. The study recommended similar study with a bigger sample from SBEs across south Africa in order to formulate a security evaluation framework suitable for these enterprises.

References

1. Wise, L.: Evaluating business intelligence in the cloud (2016). http://www.cio.com/article/3041639/business-intelligence/evaluating-business-intelligence-in-the-cloud.html
2. Herwig, V., Friess, K.: Integrating business intelligence services in the cloud: a conceptual model. In: Khosrow-pour, M.H. (ed.) Business Intelligence: Concepts, Methodologies, Tools and Applications, pp. 572–584. IGC Global (2016)
3. Llave, M.R.: Business intelligence and analytics in small and medium-sized enterprises: a systematic literature review. Int. J. Bus. Intell. Res. **10**(1), 19–41 (2019)
4. Moyo, M., Loock, M.: Small and medium-sized enterprises' understanding of security evaluation of cloud-based business intelligence systems and its challenges. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (eds.) ISSA 2018. CCIS, vol. 973, pp. 133–148. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11407-7_10
5. Indriasari, E., Prabowo, H., Meyliana, K., Hidayanto, A.N.: Key benefits of cloud business intelligence: a systematic literature review. Int. J. Mech. Eng. Technol. **9**(13), 819–831 (2018)
6. Patil, S.S., Chavan, R.: Cloud business intelligence: an empirical study. Stud. Indian Place Names UGC Care J. **27**, 747–754 (2020)
7. Niekerk, B.V.: An analysis of cyber-incidents in South Africa. African J. Inf. Commun. **20** (2017), 113–132 (2017)
8. IBM Security, Cost of a Data Breach Report 2020 (2020). https://www.ibm.com/security/digital-assets/cost-data-breach-report/
9. TechCentral, South Africa's vulnerability to cyberattacks (2019). https://techcentral.co.za/south-africas-vulnerability-to-cyberattacks/90051/
10. Cloud Security Alliance, Cloud Computing Top Threats in 2016 (2016). http://oemhub.bitdefender.com/top-threats-to-securing-the-cloud
11. Elmalah, K., Nasr, M.: Cloud business intelligence. Int. J. Adv. Netw. Appl. **10**(6), 4120–4124 (2019)
12. Alia, M., Khana, S., Vasilakos, A.: Security in cloud computing: Opportunities and challenges. Inf. Sci. (NY) **2015**(305), 357–384 (2015)
13. Khan, N., Al-Yasiri, A.: Framework for cloud computing adoption: a roadmap for SMEs to cloud migration. Int. J. Cloud Comput. Serv. Archit. **5**(56), 258–269 (2015)
14. Dresner, H.: Cloud Computing and Business Intelligence Market Study Licensed to Domo (2017). https://www.domo.com/blog/wp-content/uploads/2018/04/2018-Wisdom-of-Crowds-Cloud-Computing-BI-Market-Study-Licensed-to-Do.pdf
15. Encyclopedia.com, Security Evaluation (2020). https://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/security-evaluation
16. Heyszl, J., Schütte, J.: Security Evaluation (2018). https://www.aisec.fraunhofer.de/en/fields-of-expertise/security-evaluation.html
17. Bradshaw, C., Atkinson, S., Doody, O.: Employing a qualitative description approach in health care. Res. Glob. Qual. Nurs. Res. **4**(1–8) (2017)

18. Vasileiou, K., Barnett, J., Thorpe, S., Young, T.: Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. BMC Med. Res. Methodol. **18**(148), 125–136 (2018)
19. Kaushik, V., Walsh, C.A.: Pragmatism as a research paradigm and its implications for Social Work research. Soc. Sci. **8**(9) (2019)
20. Polit, D., Beck, T.: Nursing research, generating and assessing evidence for nursing practice, 10th edn. Lippincott Williams and Wilkins, Philadelphia (2017)
21. Clarke, V., Braun, V.: Teaching thematic analysis: overcoming challenges and developing strategies for effective learning. Psychology **26**(2), 120–123 (2013)
22. Majhi, S.K., Dhal, S.K.: A study on security vulnerability on cloud platforms. Phys. Procedia **78**(2016), 55–60 (2016)
23. Salim, S., Sedera, D., Sawang, S., Alarifi, A., Atapattu, M.: Moving from evaluation to trial: how do SMEs start adopting Cloud ERP? Australas. J. Inf. Syst. **2015**(19), S219–S254 (2015)
24. 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)
25. Bach, M.P., Celjo, A., Zoroja, J.: Technology acceptance model for business intelligence systems: preliminary research. Procedia Comput. Sci. **100**(2016), 995–1001 (2016)
26. Cloud Industry Forum: 8 criteria to ensure you select the right cloud service provider (2019). https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider
27. Chaudhari, N., Al-Yasiri, A.: A cloud security approach for data at rest. Int. J. Cloud Comput. Serv. Archit. **5**(1), 11–16 (2015)