Improving information security in SMEs to protect customer’s personal identifiable information

Small and medium enterprises (SMEs) are increasingly making use of e-commerce to increase profitability. SMEs often do not have the necessary internal controls in place to secure the personal identifiable information (PII) that is collected from customers during e-commerce transactions because the size and nature of an SME prevent it from addressing these risks. This article explores the critical success factors (CSFs) that must be considered by an SME to protect the PII of customers collected on their e-commerce site. A literature review was performed to identify possible barriers for the implementation of information security in SMEs. Furthermore, the Confidentiality-Integrity-Availability triad and ISO/IEC 27002 standards were used to group the identified barriers, and from this process CSFs were formulated for consideration. There are six CSFs that were identified to improve the information security in SMEs, which include management commitment, information security training, access control, infrastructure security, security policies and periodic audits. The recommendation of this paper is that these six CSFs must be considered to improve the information security of SMEs in South Africa.

Introduction

Small and medium enterprises (SMEs) are crucial to the economic stability of developing countries (Duan et al. 2002). In South Africa, SMEs contribute to 35% of the national gross domestic product (GDP), which therefore plays a vital role in job creation, investment, income generation and poverty alleviation (Abor & Quartey 2010). For an SME to be sustainable there are many opportunities for the owner to consider. One such opportunity includes the use of e-commerce to expand the customer base in the global market. However, because of the implementation of new technologies, some problems can be expected. SMEs in South Africa are characterised by poor information and communications technology utilisation and limited human and financial resources, which expose the SMEs to new risks (Parida, Westerberg & Ylinenpaa 2009). Typical problems that SMEs will encounter in the area of e-commerce include changes in technology, innovation of products and customer demands (Abor & Quartey 2010). One of the main risks associated with e-commerce is the security of customer information, also called personally identifiable information (PII). Although there are legislations in place to protect the customer, SMEs are known not to comply with these information security standards (Campbell & Hartcher 2015; Jiang & Li 2010; Ju Xiang 2009). SMEs either do not understand the privacy risks associated with the loss of customer information or, if they do, are overwhelmed by the security standards and regulations that must be implemented (Campbell & Hartcher 2015). This problem is further compounded as the SME typically has limited human and financial resources available to implement information security controls (Powell 2011).

This article explores the critical success factors (CSFs) that must be considered by an SME to protect the PII of customers collected on its e-commerce site. To accomplish this goal, a qualitative literature search was conducted. Relevant papers reflecting the purpose of the study were identified from four databases: ACM, EBSCO, ProQuest and JSTOR. A search strategy was used to identify articles with ‘small and medium enterprises’, ‘information security’, ‘privacy’ and ‘personal identifiable information’ as keywords. Papers published between January 2000 and October 2015 were considered, without language restriction. The literature search identified 53 references. The reference titles and abstracts were reviewed by one author for relevance to the study. The identified articles were analysed, making use of an inductive approach to contribute to the argument and CSFs presented in the paper. The purpose of the search was to identify relevant, high-quality studies that documented the barriers that prevent SMEs from implementing internal information security controls to protect the PII of their customers. The rest of the paper is structured as follows: the next section provides a definition for SMEs, as well as an explanation of what PII entails. This is followed by a discussion of the risks that are associated with both SMEs and the collection of PII. Subsequently, an overview of the Confidentiality-Integrity-Availability
(CIA) triad, ISO/IEC 27002 Security Standard and the four pillars of information security will be provided, and finally the CSFs to enable an SME to protect the PII of customers on its e-commerce site will be discussed.

**Literature review**

The characteristics of an SME are most commonly used to determine if a business falls into this category. The characteristics include the number of employees that the business employs, the annual turnover, capital assets and the SME’s contribution towards the GDP (Abor & Quartey 2010). In South Africa, an SME is recognised by the *National Small Business Amendment Act* (2003) as an organisation that employs no more than 250 employees with a turnover of less than R4 million and a total gross asset value of less than R2 million. Recently, SMEs have started to use e-commerce to improve the geographical reach of their business and attract new customers (Cheng 2009). Beckinsale, Levy and Powell (2006) found that there are three drivers that determine if an SME will adopt e-commerce, which include the perceived benefits, organisational readiness and external pressures. The perceived benefits of e-commerce for an SME include a reduction in operation costs and an increase in market share because of increased visibility in the global market (Jahanshahi et al. 2012). The flexibility of SMEs enables the business to quickly respond to new business needs, such as e-commerce, as decisions can be taken quickly by the owner (Karahanna et al. 2013).

Organisational readiness refers to the aptitude of the owner to take risks and the availability of appropriate information technology (IT) infrastructure (Alghamdi, Nguyen & Jones 2013). Olatokun and Kebonye (2010) stated that SMEs tended to be labour-intensive rather than capital-intensive as the business cannot afford the IT equipment to automate tasks and services. The degree of formalisation in an SME refers to the extent to which a business’s work is standardised (Robbins 2006). Most SMEs are family-orientated businesses and are dependent on the interaction of a small number of people employed by the business. The size of SMEs means that there is a low degree of formalisation with no clear hierarchical structures or policies and procedures about how the company operates as the owner is responsible for most of the decision-making (Nicolescu 2009). Often there is also an informal environment in the SME, which deters the owner to establish effective governance systems to promote accountability amongst employees (Jiang & Li 2010; Nicolescu 2009). The importance of IT governance in the SME will depend on the knowledge and skill of the owner. If the owner does not consider the protection of the PII of their customers as a priority, or does not have the necessary skills to manage the information security of the website, it is unlikely that proper security controls will be put in place (Nicolescu 2009). In addition, Abor and Quartey (2010) stated that the employees of an SME usually did not possess any specialised skills and that SMEs also tended not to invest in their employees’ training and development because of insufficient funds. This means that it is highly unlikely that the employees will be able to develop or maintain an e-commerce site for the business (Shemi & Procter 2013).

External pressure refers to the needs of the customers of the SME to make use of e-commerce as a convenient tool. The literature reports that customers need the be assured that their information that is provided on the websites will be protected (Jiang & Li 2010; Teketel & Berhanu 2009). This lack of information security controls for an SME can undermine consumer trust, as the software and security measures, such as third party assurance seals, are too expensive for the SME to purchase (Olatokun & Kebonye 2010).

**Personal identifiable information**

PII is commonly referred to as any form of information that can be used to identify, locate and contact an individual (Narayanan & Shmatikov 2009). The information collected could include an individual’s demographics, address, financial details, educational status or employment history (Jessup & Neal 2009). Hackers often steal this information with the goal to combine the pieces of personal information, which in itself appears innocuous, in order to compromise an individual’s identity (McCallister, Grance & Scarfone 2010). PII can be compromised in two ways: when data are transmitted across an e-commerce network or because of the physical theft of devices that store sensitive information. The latter is possible in an SME because of poorly understood data and security practices. If there are no internal controls in place to secure PII, the SME will not even be aware that sensitive data are taken from the system (Jiang & Li 2010). Because of the lack of financial and technical resources, SMEs are often unable to observe good governance practices in the business. An information security policy is an effective means of defining, describing and documenting security principles that are based upon SMEs’ core beliefs. The policy should also establish a standardised baseline of expectation for the behaviour of all personnel as to comply with regulatory mandates and governance principles. Therefore, the policy will minimise or prevent any form of risk in order to protect the company assets and PII of customers (Ihovbhere 2010; Tittel 2008). Security and privacy policies are often not considered to be important in an SME, as it does not contribute directly to the profit margin of the business (Glynn 2012; Park et al. 2008). The lack of information security controls leaves the SME susceptible to possible instances of fraudulent activities, whether from an external or internal threat (Campbell & Hatcher 2015; Jiang & Li 2010). It is therefore important that the information security standards of the business are either in place or improved. This is achievable through the implementation and utilisation of internal controls within the SME. If these are in place, it will improve the trustworthiness of the e-commerce site of the SME, which in turn will improve the profitability of the business (Michel 2012).

**CIA triad – Model of security**

The CIA triad is in an information systems security term that relates to the important aspect of data protection. This security model was developed as a tool to put in place...
measures relating to information security. The main objective of information security is to assure the confidentiality, integrity and availability of PII that is crucial for the continuity of a business’s operations and functionalities (Ihonvbere 2010; Tittel 2008). The following section discusses the confidentiality, integrity and availability triad as can be seen in Figure 1.

Confidentiality of data: The purpose of confidentiality is to ensure that PII is only accessible by authorised individuals. Confidentiality also relates to the broader concept of data privacy, thus limiting the access to PII within an SME (Whitman & Mattord 2009). The next section of the CIA triad relates to data integrity.

Integrity of data: Data integrity relates to the assurance as well as the trustworthiness of information that data have not been altered inappropriately, either accidentally or deliberately (Whitman & Mattord 2009). Any information that is transmitted or recorded and entered into the system should reflect actual, reliable and correct records or instances, without corruption (Ihonvbere 2010; Whitman & Mattord 2009). The following section discusses the final aspect of the CIA triad: availability of data.

Availability of data: The last aspect of the CIA triad, availability, guarantees that PII is readily available to authorised users because modern businesses are highly dependent on a functioning information system (Whitman & Mattord 2009).

Confidentiality, integrity and availability are often taken for granted by SME owners. Information security is often associated with services that engage with sensitive information, such as financial, legal, human resources or business documentation. SMEs question the need for security controls in their business as this type of information exposure is limited (Campbell & Hartcher 2015). The following section will discuss the ISO/IEC 27002 security standard.

ISO/IEC 27002 standard

The International Organization for Standardization (ISO/IEC) is the world’s largest developer of voluntary International Standards (ISO/IEC 27000 2014). The ISO/IEC 27002 standard provides a ‘code of practice’ that can be used for high-level security management that is intended as a common basis and practical guideline for SMEs to develop security standards and effective security management practices. The standard is based on 11 sections but cannot be used for certification purposes. Instead, the ISO/IEC 27001 standard was developed as an information security management system (ISO/IEC 27000 2014). The objective of these standards is to ensure compliance with all statutory, regulatory, certificatory or contractual obligations, and these requirements should be explicitly defined, documented and kept up to date (ISO/IEC 27000 2014). The following section introduces the CSF developed to ensure that internal control in the SME will provide for the secure collection and storage of PII.

Critical success factors

The focus of this paper was to identify CSFs that are necessary to ensure that internal information security controls are in place in SMEs to protect the PII of their customers. The CIA triad provides the general foundations for the development of the CSF. Additionally, the ISO/IEC 27002 Security Standard was discussed as it provides a code of practice for information security management. A CSF refers to the specific activities, procedures or areas that a business depends upon for success or survival and is unique for each SME. The CSFs that are recommended for an SME to make sure that there are internal controls in place to protect the PII of customers are discussed in the following sections.

CSF01 – Management commitment

The owner of an SME has a commitment and responsibility to ensure that an information security policy is in place. As discussed earlier, the knowledge of the owner will determine the level of attention that is given to security controls in the SME. In addition, the owner should ensure that the policy is enforced and managed in accordance with ISO/IEC 27001 and 27002 security standards (Binder et al. 2010; Shanmugam, CheHaat & Ali 2012). Once the policy is in place, the next step is to provide user training and awareness programme.

CSF02 – Information security training

The second CSF relates to employee or user awareness and training. It is important that all employees of an SME should receive some form of training with regard to the security policies of the SME, as this training will encourage compliance (Mendes 2012). Furthermore, if the information security knowledge of employees increases, they will be able to help the SME recover from undesirable situations, as

Source: Bhaiji, Y., 2008, Chapter 1 – Overview of network security, Cisco Academy, Indianapolis.

FIGURE 1: CIA triad.
well as be able to detect situations that can lead to adverse situations (de Vos & Willemse 2011; Kelly 2011; Mendes 2012; Shanmugam et al. 2012). Following the implementation of employee or user awareness and training, it is essential that an access control system is placed within the business.

CSF03 – Access control
Access control relates to the appropriate physical access controls, guards and surveillance systems that are implemented within an SME. The goal of this CSF is to ensure the protection of the work environment, as well as any other areas that contain sensitive information assets (Kelly 2011; Park et al. 2008). The following CSF relates to the Infrastructure Security Standards that must govern the information security policies in the SME.

CSF04 – Infrastructure security
Infrastructure security relates to computer and network security procedures and methods. As such, the IT staff or IT vendors are able to securely manage the technological infrastructure in a defined and documented manner that adheres to effective information security practices. This ensures the compliance of regulatory standards for the protection of sensitive organisational information, as well as the prevention of unauthorised access to this information (Kelly 2011; Park et al. 2008). With an effective and efficient security infrastructure in place, the next CSF relates to the implementation of security policies to ensure that a secure environment is possible through regulations and standards.

CSF05 – Security policies
Security policies relate to how an SME has defined and documented its management approach to security and legal compliances. More importantly, these security policies must be implemented in a manner that complies with the SMEs’ responsibilities and duties to protect confidential and sensitive information, as well as prevent any access, exposure or distribution of such information (Binder et al. 2010; Park et al. 2008). Subsequently, with an efficient security policy in place, it is important to continuously assess the various policies and regulations in place. This therefore leads to the final CSF.

CSF06 – Periodic assessment
The final CSF relates to periodic assessment. This factor aims to ensure that an SME pertains to an assessment or review of its security programme and policies, dealing with managerial and technical aspects. It is important that this assessment is conducted annually to further ensure security and reliability of an SME. With the integration of periodic assessments within the SMEs, information and data loss or theft prevention can be dealt with effectively and sufficiently, furthermore contributing to the importance of security and regulatory policies (Binder et al. 2010; Shanmugam et al. 2012). The following section provides an overview of how each of the CSFs can be mapped to the four pillars as discussed in the previous section.

Critical success factors and the four pillars of information security
The four pillars of information security refer to the different aspects that an SME should take into consideration to assist in ensuring that sufficient security standards are met. The four pillars are based on data protection and recovery, the detection of unwanted states of access and furthermore the compliance with regulation, standards and policies. These pillars focus on an SMEs’ perspective in ensuring organisational and customer security:

- **Protection**: protecting confidential and sensitive information;
- **Detection**: detecting or preventing of unwanted states or programmes from unauthorised access;
- **Recovery**: making initiatives in the case of an emergency or unexpected, unwanted situation; and
- **Compliance**: ensuring that policies, standards and legal regulations or requirements are organisationally met (Shanmugam et al. 2012).

It is essential that the CSFs identified above are able to ensure the enforcement of regulations and policies, as well as the protection of PII. Table 1 provides an illustration of how each CSF aligns with the four pillars in assisting with the security concerns of SMEs previously discussed previously.

From Table 1 it is noted that the CSF will assist an SME to be compliant with various security standards, policies or regulations. Compliance is one of the key aspects that will determine the successful protection of PII. SMEs are often overwhelmed by the volume of security standards and regulations that must be complied with. Additionally, SMEs do not comprehend the potential risks associated with not having to comply with such standards and regulations, which result in the ignorance of security measures. The identified CSFs will provide the SME with a specific security framework that it can use to make sure that the necessary internal controls are in place to protect and detect potential harmful situations during the collection of PII.

Conclusion
This article explored the CSFs that are considered by an SME to improve the protection of the PII of customers collected on e-commerce sites. This was done through an in-depth literature review of experts in the field of information security and internal controls as well as PII collection, resulting in

<table>
<thead>
<tr>
<th>TABLE 1: CSFs and four pillars.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success factors</td>
</tr>
<tr>
<td>Top management commitment</td>
</tr>
<tr>
<td>Employee and user awareness/training</td>
</tr>
<tr>
<td>Access control</td>
</tr>
<tr>
<td>Infrastructure security</td>
</tr>
<tr>
<td>Third-party assurance</td>
</tr>
<tr>
<td>Security policies</td>
</tr>
<tr>
<td>Periodic assessment</td>
</tr>
</tbody>
</table>

http://www.icbmd.org  
do:10.4102/jbmd.v5i1.7
the CSFs. These CSFs were created through the utilisation and understanding of the CIA triad and ISO/IEC 27002 Security Standards. The CIA triad provided a foundation of information confidentiality, integrity and availability, whilst the ISO/IEC 27002 provided a more in-depth observation of information security. Therefore, the CSFs can be utilised in an SME to ensure that any PII that is collected is effectively and efficiently secured and managed, in addition to creating a more secure working environment. Once a secure environment is achieved through the implementation of these CSFs, the mitigation of the risks discussed in the research is possible.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationship(s) that may have inappropriately influenced them in writing this article.

Authors’ contributions

F.E. (University of Fort Hare) and L.C. (University of Fort Hare) contributed equally to the writing of this article.

References


Bhaiji, Y., 2008, Chapter 1 – Overview of network security, Cisco Academy, Indianapolis.


De Vos, A. & Willemsen, I., 2011, Leveraging training skills development in SMEs, OECD.


Tittel, E., 2008, ABCs of IT security for CPAs, American Institute of Certified Public Accountants, Washington.

