Journal of Contemporary Management
Volume 13

Integrated business model for mitigating e-retail information security risks

B OKANGA *

Department of Business Management, University of Johannesburg

*boniokanga@gmail.com * corresponding author*

A DROTSKI

Department of Business Management, University of Johannesburg

adrid@uj.ac.za

Abstract

Dynamic nature and sources of information security risks render largely reactive and inflexible approaches less effective for managing e-retail information security risks. This research examines the effectiveness of the strategies used for mitigating e-retail information security risks by the modern e-retail enterprises. It entailed the application of a meta-synthesis as a qualitative research technique to socially construct and triangulate theories on e-retail information security risks with the empirical findings on the approach used by the e-retailers for managing e-retail information security risks in South Africa. The motive of the study was to identify the major paradoxes and the remedial e-retail information security risk management model that can be suggested.

Despite wider application of a six steps' framework (assets' analysis, identification of the sources and symptoms of risks, vulnerability analysis, intervention and evaluation) for e-retail information security risk management, lack of accompanying change and transformation of employees' information security behaviours, culture and practices were still reiterated to constrain the emergence and evolution of a dynamic proactive approach for managing the usually dynamic e-retail information security risks. The interpretation of the findings revealed such deficiencies are also often further exacerbated by poor synchronisation of e-retail information security management systems with enterprise-wide risk management frameworks.

The study concludes with the suggestion of the e-retail information security risk management model integrating the six steps' framework with the measures for changing and transforming the employees' information security behaviours, culture and practices to enhance the creation of a coherent dynamic proactive approach for effective management of e-retail information security risks as part of the enterprise-wide risk management system.

Key phrases

e-retail; information security risks; integrated business model

1. INTRODUCTION

E-retail is a branch of e-commerce that entails the selling of goods in smaller quantities to the larger electronic markets (Fernie, Fernie & Moore 2013:6: Soto & Merono 2008:49). In e-retail, all activities such as enquiries, ordering and payment of goods are accomplished electronically until the actual physical goods are delivered to the specified e-customers' addresses (Fernie *et al.* 2013:6: Soto & Merono 2008:49).

The overall functionality and efficient performance of the e-retail information system are therefore prerequisites for effective performance of the contemporary e-retail enterprises (Al-Somali, Clegg & Gholami 2010:6). To edify the effective functionality and efficient performance of the e-retail enterprises, most of the contemporary e-retail executives often opt to invest in one or a combination of the e-retail technological platforms such as on-premise-e-commerce, software as a service (SaaS) e-commerce or open source e-commerce (Al-Somali *et al.* 2010:6; Soto & Merono 2008:49).

However, the installation of more efficient and reliable e-retail technological platforms like on-premise-e-commerce software is often preferred as the appropriate strategies that edify the efficiency of the e-retail enterprises (Al-Somali *et al.* 2010:6). Unless the investment in such superior and efficient e-retail technologies is accompanied by a dynamic proactive initiative for effective identification and mitigation of information security risks, the overall efficiency of the e-retail enterprise may still be undermined (Forrester 2010:16; KPMG 2011:7).

Information security risks are internal risks linked to employees' activities and external threats arising from cybercrimes that can interfere with or damage a firm's information system (Citrix 2014:66; Saleh & Alfantookh 2011:107). This can affect the smooth flow of activities and information along the e-retail value chain (Citrix 2014:66).

Less efficient e-retail operation can affect customer satisfaction with the quality of online services, and the competitiveness of the e-retail enterprise (Citrix 2014:66). So far, Fichardt (2015:2) highlights recent statistics to indicate South Africa loses about R2.2billion annually to cybercrimes linked to internet fraud and phishing attacks. This is attributable to the fact that besides the direct effects of cybercrimes, several studies on information security risks in South Africa also herald information security risk is increasingly turning into a multidimensional vice with sources linked to among others the actual internal employees and partners in the supply chain (Dagada, Eloff, Venter & Meraka 2013:9; Jordan 2014:21; Mobius 2014:5). Combined with a largely underdeveloped policy on information security threats in South Africa, all these imply e-retail enterprises therefore have to adopt the appropriate proactive measures to identify and diffuse all sources of information security risks before they turn into irreversible costly threats (Belayneh 2014:10; Jordan 2014:21; Pricewaterhouse Coopers 2015).

However, the question as to the appropriate business model that can be adopted without necessarily interfering with the efficiency and quality of online customer services seems yet a paradox that most of the e-retail enterprises still grapple with (Belayneh 2014:10; Jordan 2014:21). Even if the question as to the most suitable electronic information security management model remains a puzzle, epistemological trends highlight most studies to have focused on the evaluation of the sources of information security risks rather than proposing comprehensive solutions on the business models that can be replicated. Such a trend has created a gap that this research deals with by evaluating the nature of e-retail information security risks vis-a-vis the effectiveness of the approach that the e-retail enterprises use for mitigating their exposure to such risks. Through this analysis, the study aims to develop an integrated business model that the e-retailers can replicate for managing and mitigating e-retail information security risks.

2. LITERATURE REVIEW

Information security risks refer to incidents and events that interfere with the effective and efficient performance of the e-retail information systems (Forrester 2010:16). Information security risks also often cause damage or loss of information that can cause further loss or

damage of other information. All these can affect the effective performance of e-retails as business entities. To minimise or mitigate information security risks, Easttom (2011:29) heralds the use of the basic principle of CIA triad (confidentiality, integrity and availability) to be critical for diffusing risks of information security risks.

Confidentiality is often upheld by classifying information and ensuring that such information is not availed to unauthorised persons, entities and processes (Easttom 2011:29). Integrity is a prerequisite for the prevention and detection of whether information or data has been tampered with (Easttom 2011:29).

Availability is a principle that edifies the extent to which an enterprise is able to ensure that all its information system apparatus are securely available and functional for accomplishing different business activities (Easttom 2011:29; Cherdantseva & Hilton 2013:66). The use of these three principles enhance the improvement of the process for managing and mitigating information security risks (Cherdantseva & Hilton 2013:66; Easttom 2011:29). However, Almeida and Portela (2013:16) and Howarth (2014:11) argue that the effective management of information security risks cannot be achieved by mere adherence to principles.

Instead, alternative views indicate it is critical that the use of the CIA triad is accompanied by the use of an effective framework for information security risk identification and management (Almeida & Portela 2013:16; CEB 2015:16; Howarth 2014:11). The views of Almeida and Portela (2013:16) and Howarth (2014:11) are echoed in the opinions of different authors that highlight different views on the critical logical steps required for the identification and mitigation of information security risks (Almeida & Portela 2013:16; Forrester 2010:16; Kamaraju 2012:16; KMPG 2011:7).

In such theories, different authors share similar views that the effective identification and management of information security risks is often predicted by the application of certain six chronological steps that include (Almeida & Portela 2013:16; Forrester 2010:16; Kamaraju 2012:16; KMPG 2011:7):

Step 1: In the context of the illustration in Figure 1, *the first step* in such a framework requires the identification and analysis of the values of the available assets as well as their associated inherent vulnerability to risks.

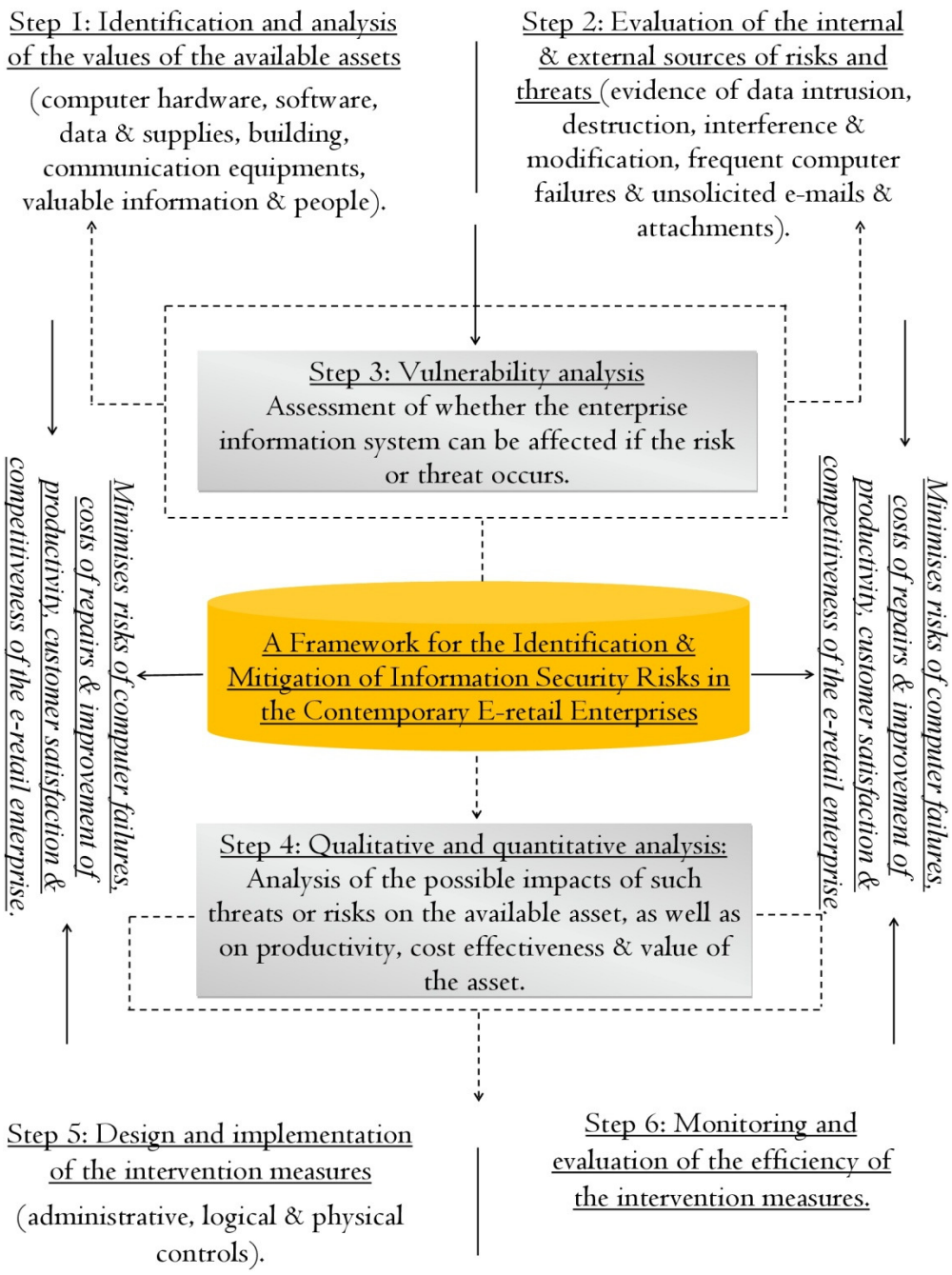

FIGURE 1: A framework for the identification and mitigation of information security risks in the contemporary e-retail enterprises

Source: As derived from the information security frameworks of authors such as Almeida & Portela 2013:16, Forrester 2010:16 and KMPG 2011:7

Such assets may include computer hardware, software, data, supplies, building, people and valuable company information (Forrester 2010:16).

Step 2: Requires evaluation of the existing and probable internal and external sources of risks and threats (CEB 2015:16; Howarth 2014:11). The internal sources of risks may include theft of company information, visiting unauthorised sites, flouting of company policies and procedures on the usage of information system and unauthorised disclosure of information (Notenboom 2008:5).

The other internal sources of information security risks may require the analysis of the risks associated with over-trusting third parties in the supply chain, and unethical practices among employees and those in the supply chain (Forrester 2010:16). Risks may also arise from the use of information system equipment for personal purposes and negligence linked to lending company computers or memory sticks to unauthorised persons (Harnish 2015:11).

The external sources of information security risks are often linked to theft of intellectual property, identity theft, software attacks, theft of information equipment such as computers and memory sticks, acts of sabotage or information extortion, software attacks using viruses, worms, phishing and trojan horses and hacking (Notenboom 2008:5). Symptoms of eminent information security risks are often exhibited in the evidence of intrusion, data destruction, data interference, computer interference, information modification, false use of data, unauthorised transactions, frequent computer failures, and e-mails from unsolicited sites or respondents (Almeida & Portela 2013:16).

Step 3: The effective isolation of the potential sources of information security risks leads to the *third step* that involves vulnerability analysis that requires assessment of how the enterprise information system can be affected if the risk or threat occurs (Almeida & Portela 2013:16). Vulnerability analysis often focuses on the assessment of the effectiveness of the enterprise's existing information security policies, procedures, standards, training, physical security, quality control and technical security (Fariborz, Navathe, Gunter & Enslow 2014:5; Forrester 2010:16).

Step 4: Entails qualitative and quantitative analysis of the magnitude of the impact of the identified threats to facilitate the determining of the intervention and response measures that must be undertaken in step 5. (Forrester 2010:16).

Step 5: The intervention measures often requires the establishment of administrative controls (written policies, procedures and standards), logical controls (passwords, network intrusion detection systems, and data encryption) and physical controls (the use of human guards and door locks) (Forrester 2010:16; KPMG 2011:7).

Step 6: ınvolves monitoring and evaluation of the effectiveness of the intervention measures undertaken in terms of their costs and productivity implications (Almeida & Portela 2013:16). This is attributable to the fact that in certain cases, the adoption of certain intervention measures has been undertaken at the expense of the efficiency and effectiveness of the functionality of the information system. The evaluation in step 6 therefore facilitates the improvement of the compatibility of the adopted systems with the established systems or the undertaken changes to ensure that the efficiency of the systems in place is not affected.

In other words, the framework in Figure 1 reflects the kind of frameworks that are often relied on by most of the e-retail enterprises in South Africa as the accurate steps for the identification and mitigation of information security risks in the contemporary e-retail enterprises.

However, such frameworks often lack the accompanying critical aspects through which the overall organisational practice and cultures can be changed and transformed to support the development and evolution of the dynamic initiatives for the identification and mitigation of information security risks (ISACA 2015:5). In the widely used ISACA (2015:5) integrated business model, the essence for changing and transforming organisational behaviours and practices to create an effective culture is strongly emphasised.

However, a challenge still arises from the fact that ISACA's (2015:5) integrated business model also strongly emphasises the need for cultural change and transformation at the expense of the critical steps that enterprises can replicate to ensure effective identification

and mitigation of information security risks. It is such incoherency in the existing theories that motivates this research.

3. PROBLEM INVESTIGATED

Investment in superior IT systems without undertaking corresponding initiatives to change and transform the employees' information security behaviours and practices affect the development and application of a dynamic framework for identification and mitigation of e-retail information security risks in most of the contemporary e-retail enterprises in South Africa.

4. PURPOSE OF THE RESEARCH

The purpose of this research is to evaluate the overall effectiveness of the strategies used for mitigating information security risks by the e-retail enterprises in South Africa, so as to develop a business model that edifies the e-retail enterprises' capabilities to identify and mitigate all e-retail information security risks.

5. METHODOLOGY

In line with the articulations of Blanchette (2012:5) and Boghossian (2011:488) on the notion of conceptual analysis, this study uses conceptual analysis, and specifically a meta-synthesis as a qualitative research technique. The process for the accomplishment of a meta-synthesis was guided by four critical research questions, namely:

- What are the major sources of information security risks in the contemporary South African e-retail enterprises?
- How effective are the strategies used for the identification and mitigation of information security risks in the contemporary South African e-retail enterprises?

- What are the major inhibitors of the effectiveness of the strategies used for the identification and mitigation of information security risks in the contemporary South African e-retail enterprises?

- Which integrated business model can be adopted for improving the ability of the contemporary South Africa e-retail enterprises to identify and mitigate all information security risks?

In a bid to seek answers to these research questions, a meta-synthesis of different theories and prior empirical studies were undertaken using four main steps that include:

- Critical analysis of the contemporary theories on the identification and mitigation of e-retail information security risks.

- Evaluation of prior empirical studies on the identification and mitigation of e-retail information security risks in South Africa in the period between 2010 and 2015.

- Comparison and contrasting of theories and empirical findings on the inhibitors of the strategies for identification and mitigation of e-retail information security risks in South Africa.

- Identification and mapping of themes highlighting the major sources of e-retail information security risks, the strategies and inhibitors linked to managing information security risks.

The identification of such themes and the process of mapping led to the development of a dynamic e-retail information security management model that can be emulated for improving the ability of the contemporary e-retail enterprises to identify and mitigate all information security risks. The details of the results of meta-synthesis are as presented in the next section.

6. FINDINGS

This section provides the evaluation of the results of the meta-synthesis according to two subsections:

- Contemporary theories: integrated business model for managing information security risks
- Empirical facts: e-retail information security risks in South Africa

The details of the analysis are as follows:

6.1 Contemporary theories: integrated business model for managing information security risks

A rather comprehensive approach enunciated in ISACA's (2015:5) integrated business model seems to offer views consonant with the opinions of most of the authors in different theories for managing information security risks (Bediako 2014:119; Bojanc & Blazic 2013:25; Ekelhart Fenz & Neubaur 2009:3). ISACA's (2015:5) model posits the effective management of information security in the contemporary complex enterprises to be predicted by certain four elements and six dynamic interconnections (DIs).

The four elements are highlighted in ISACA's (2015:5) model to constitute of the organisation, process, people and technology.

The six dynamic interconnections (DIs) include culture, governance, architecture, emergence, enabling and support, and human factors (ISACA 2015:5).

For an enterprise to effectively manage its information security, it is critical a balance of all these four elements and six dynamic interconnections are maintained at all the time (ISACA 2015:5).

The details of all these are illustrated in the theoretical framework in Figure 2.

6.1.1 BMIS' four elements for information security

In line with the illustration in Figure 2, the details of the BMIS' four elements for information security are evaluated as follows.

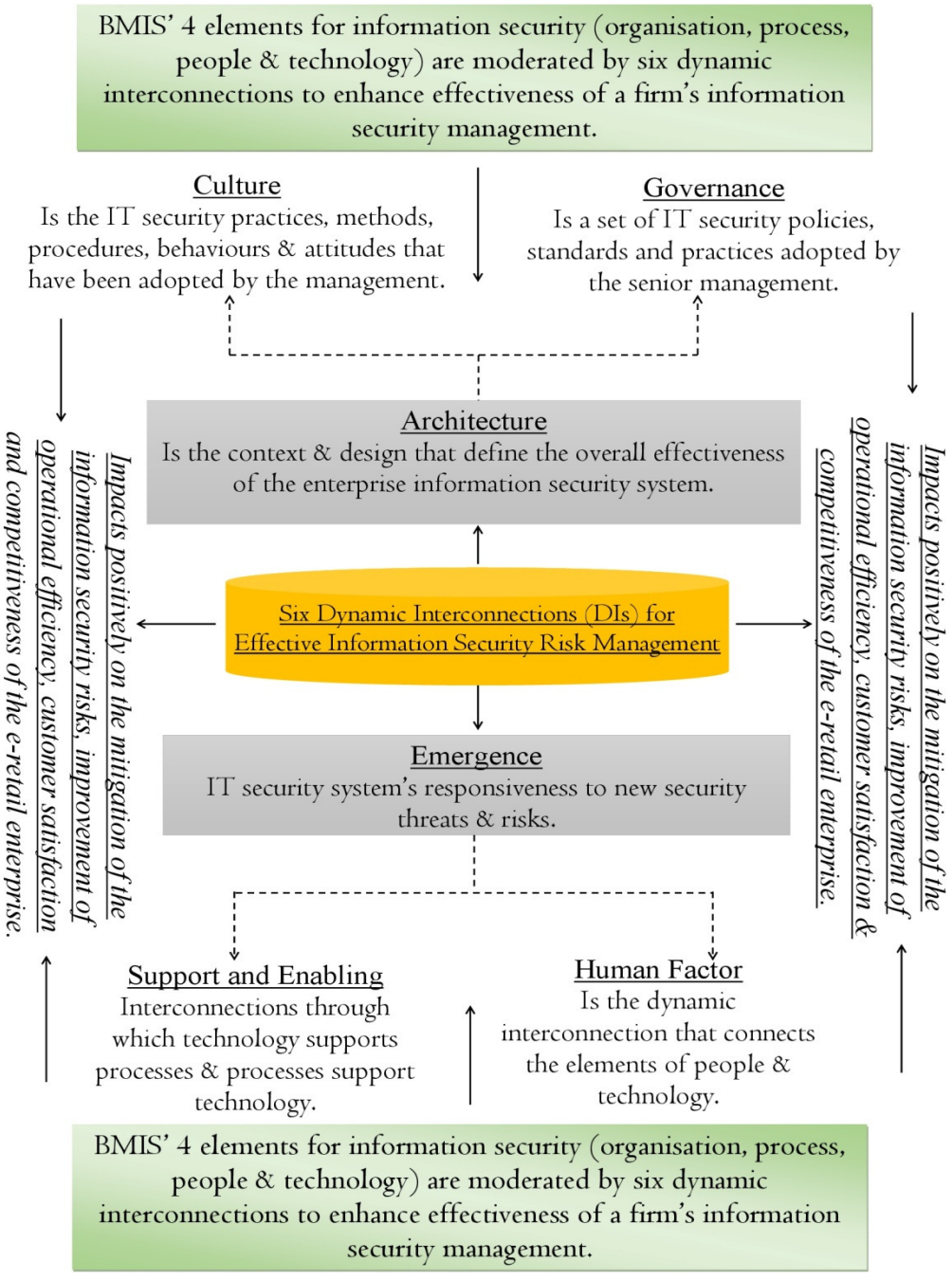

FIGURE 2: ISACA's (2015) moderating effects of the six (6) dynamic interconnections on the four (4) elements of a business model for effective information security management

Source: ISACA 2015:5

- ***Organisational***

Organisational element enables security experts gain enterprise-wide view to assess how the existing structures and strategy enhance or inhibit information security measures (ISACA 2015:5).

In terms of the evaluation of the existing structures, the analysis of the existing divisions of the organisational structures is often undertaken by assessing the extent to which the degree of activities' coordination and control influence effectiveness of information security management (Bediako 2014:119).

In such analysis, it is often of essence to note that disintegrated and silo-based structures are more vulnerable to information security risks than more centralised structural systems (Bojanc & Blazic 2013:25; Ekelhart *et al.* 2009:3). It also extends to the evaluation of the extent of the supportiveness of the organisational culture, procedures and policies as well as the formal and informal organisations (Bojanc & Blazic 2013:25; Ekelhart *et al.* 2009:3).

Effective analysis of the organisational dimension of an enterprise enables relevant mapping of security fundamentals of confidentiality, availability and integrity to be undertaken (Bojanc & Blazic 2013:25).

- ***Process***

Process is a set of repetitive tasks and activities systematically accomplished in the context of the defined methods, procedures and policies (ISACA 2015:5). It predicts the effectiveness of the enterprise's information security system. Process analysis is therefore critical for an enterprise to identify the major impediments and determine the necessary intervention measures that can be adopted to improve the overall effectiveness of e-retail information security management (Iglesias, Pascual, Hernandez & Chaparro 2013:314).

Process effectiveness is predicted by the extent to which it either facilitates effective feedback or induces delay. This enhances the analysis of the loop between the period that the feedback is received and the time that intervention measures are undertaken (Iglesias *et al.* 2013:314). If there is significant delay, it is in that loop that the information security of an

enterprise may tend to become more vulnerable. In effect, solutions to such circumstances are often latent in the undertaking of the appropriate technological intervention measures.

- ***Technology***

Technology deals with the implementation and utilisation of technical skills and knowledge as well as equipments in the management and enhancement of e-retail information security (ISACA 2015:5). Technology requires the use of personal computers and the associated software, a pager, mobile phone, voice-over IP (VoIP), smartphones and tablets and mainframe computers (Ekelhart *et al.* 2009:3).

Other technological applications may also require the building of solid physical locks on the door of the biometric access management devices, PC camera, video surveillance system and fire button alarm (ISACA 2015:5). It also entails the adoption of the applications that exceed the intra-enterprise applications and web-based applications to encompass data storage and control of access via public networks, peer-to-peer infrastructures and darknets (ISACA 2015:5).

- ***People***

The people dimension of information security risk management encompasses human resources or employees of the enterprise, and those working in partner enterprises such as suppliers, customers or subcontractors (ISACA 2015:5). Ensuring the balance of these four critical factors is a prerequisite for ensuring effective management of e-retail information security (Ekelhart *et al.* 2009:3).

The overall effectiveness of the people dimension of information security is often determined by training and developing all employees on the matters of information security (Ekelhart *et al.* 2009:3). Besides designing reward strategies to motivate employees' behaviours and practices, the other strategy may require the adoption of a culture that enhances the information security of an enterprise.

In other words, the people's dimension of information security risk management entails the analysis of the nature of interactions and relationships between the enterprise and its

external stakeholders such as partners and strategic alliances, third-party vendors, consultants, customers and other stakeholders (Department for Business, Innovation and Skills 2014:11).

However, ISACA's (2015) model cautions that unless such a balance is linked to the six dynamic interconnections (DIs), their overall positive effects on enhancing the effectiveness of the enterprise information security risk management may only be minimal.

In effect, BMIS' four elements for information security management (organisation, process, people & technology) are often moderated by six dynamic interconnections to enhance the effectiveness of a firm's information security management.

6.1.2 Six dynamic interconnections (DIs)

In the context of the illustration in Figure 2, the six dynamic interconnections (DIs) are explained as follows (ISACA 2015:5).

- ***Culture***

Culture is the practice, methods, procedures, behaviours and attitudes that have been adopted by the management, supervisors and ordinary employees to enhance the overall effective management of an enterprise's information security systems (ISACA 2015:5; Notenboom 2008:5). Information security culture is influenced by effective training and transformation, and use of rewards and de-motivators to change peoples' behaviours (Citrix 2014:19; Saleh & Alfantookh 2011:107).

It also entails the creation of effective information security culture that may require establishing a strong information security programme, establishing and communicating clear information security policies, and the elimination of silos through encouragement of greater collaboration across different departments and units (Bojanc & Blazic 2013:25).

Besides providing knowledge, tools and skills that people need to effectively handle information security risks, the development of consistent processes for information handling and sharing in conjunction with scenario training to influence change in beliefs and attitudes

are the other strategies for developing a culture that facilitates effective information security risk management (ISACA 2015:5). For such ensures to be effective, they must be accompanied by the development and establishment of an effective governance system.

- ***Governance***

Governance is the application of policies, standards and practices adopted by the senior management to influence the form that an organisation takes (ISACA 2015:5). Governance also influences the change of people, process and technology to support the overall initiative for enhancing the effectiveness of the e-retail information security system.

This enhances the overall effectiveness of information security risk management (Citrix 2014:19; Saleh & Alfantookh 2011:107). It also deals with the commitment of the senior managers towards enhancing compliance and allocation of sufficient resources for the implementation of different security measures (Citrix 2014:19; Saleh & Alfantookh 2011:107).

- ***Architecture***

Architecture is the context and the design that define the overall effectiveness of the enterprise information security system (ISACA 2015:5). The effectiveness of the architecture of an enterprise's information system is measured by the extent of its scalability and adaptability (Alqatawna 2014:883). Scalability and adaptability are measured by the extent to which the existing information security system allows space for evolution and improvement, and reaction to changes in the external context, fitness for purpose, effectiveness and efficiency (Alqatawna 2014:883).

Other critical determinants of scalability and adaptability of the architecture of the enterprise information security system include its overall consistency with policy and standards as well as maintainability and usability (Alqatawna 2014:883). The design of the architecture of an enterprise's information security system is also often influenced by the scope and charter of the technology security, and whether the capacity is static and dynamic, centralised or decentralised (Hartono, Holsapple, Kim & Simpson 2014:11).

- ***Emergence***

Emergence refers to the new circumstance that arise from new opportunities for businesses, new behaviours, new processes and other relevant security elements as the subsystems between people and processes evolve (ISACA 2015:5). It examines the extent to which the improvement of the information security systems is constantly undertaken to support such changes and identify and diffuse all the new emerging information security risks (ISACA 2015:5).

- ***Support and enabling***

Support and enabling provide the interconnections through which technology supports processes that in turn support technology (ISACA 2015:5). Ensuring a strong enabling and support is attained through balancing processes and quick adjustment to a new equilibrium state. Besides the adherence to appropriate standards, it also requires the use of controls, a strong security focus and recognition of compliance requirements (Hartono *et al.* 2014:11).

The key components of the enabling and support offer the physical and tangibles platforms that support the design and implementation of different information security features and systems. It often aids the achievement of strategically high-level business objectives that may facilitate the reduction of costs, improvement of productivity and the detailed business requirements. It may also require the adoption of an effective architecture and process frameworks and facilitation of cross-functional groups to improve the effective management of information security risks (Hartono *et al.* 2014:11).

- ***Human factor***

Human factor is often linked to the dynamic interconnection that connects the elements of people and technology (ISACA 2015:15). It facilitates the evaluation of the extent to which the behaviours, practices and cultures adopted by the employees and other users of information support the consistent identification and diffusion of all sources of information security risks (ISACA 2015:15).

However, the analysis of the empirical studies conducted on e-retail information security risks in South Africa in the period between 2010 and 2015 would suggest that the adoption of such a comprehensive strategy seems to be lacking in the approach adopted by most of the e-retail enterprises (Bedi & Warden 2010:144; Hansen 2013:122; Jordan 2014:21; Nyoni & Mthulisi 2015:6).

6.2 Empirical facts: e-retail information security risks in South Africa

As indicated in Figure 3, studies conducted on e-retail information security risks in South Africa in the period between 2010 and 2015 indicated the initiatives of most of the e-retail enterprises to enhance the effective identification and mitigation of all internal and external sources of e-retail information security risks are still inhibited by a combination of different factors (Bedi & Warden 2010:144; Hansen 2013:122; Jordan 2014:21; Mobius 2014:5; Nyoni & Mthulisi 2015:6).

The common inhibitors of the initiatives to ensure effectiveness of e-retail information security in South Africa are noted in most of the empirical studies to be linked to (Bedi & Warden 2010:144; Hansen 2013:122; Jordan 2014:21; Nyoni & Mthulisi 2015:6):

6.2.1 E-retail's executive support

The overall buy-in of the top managers is one of the factors that either inhibit or influence the effectiveness of the strategies for mitigating information security risks in the contemporary business enterprises (Dagada *et al.* 2013:9; Mobius 2014:5). Top managers are often interested in the values of the information security measure to be adopted. If they find the overall values of enhancing operational efficiency and significant financial returns to be only minimal, they may be less interested in pursuing such a strategy (Dagada *et al.* 2013:9). Such a decision may also affect the commitment of the senior managers and the allocation of the resources necessary for the undertaking of such investments (Jordan 2014:21; Mobius 2014:5).

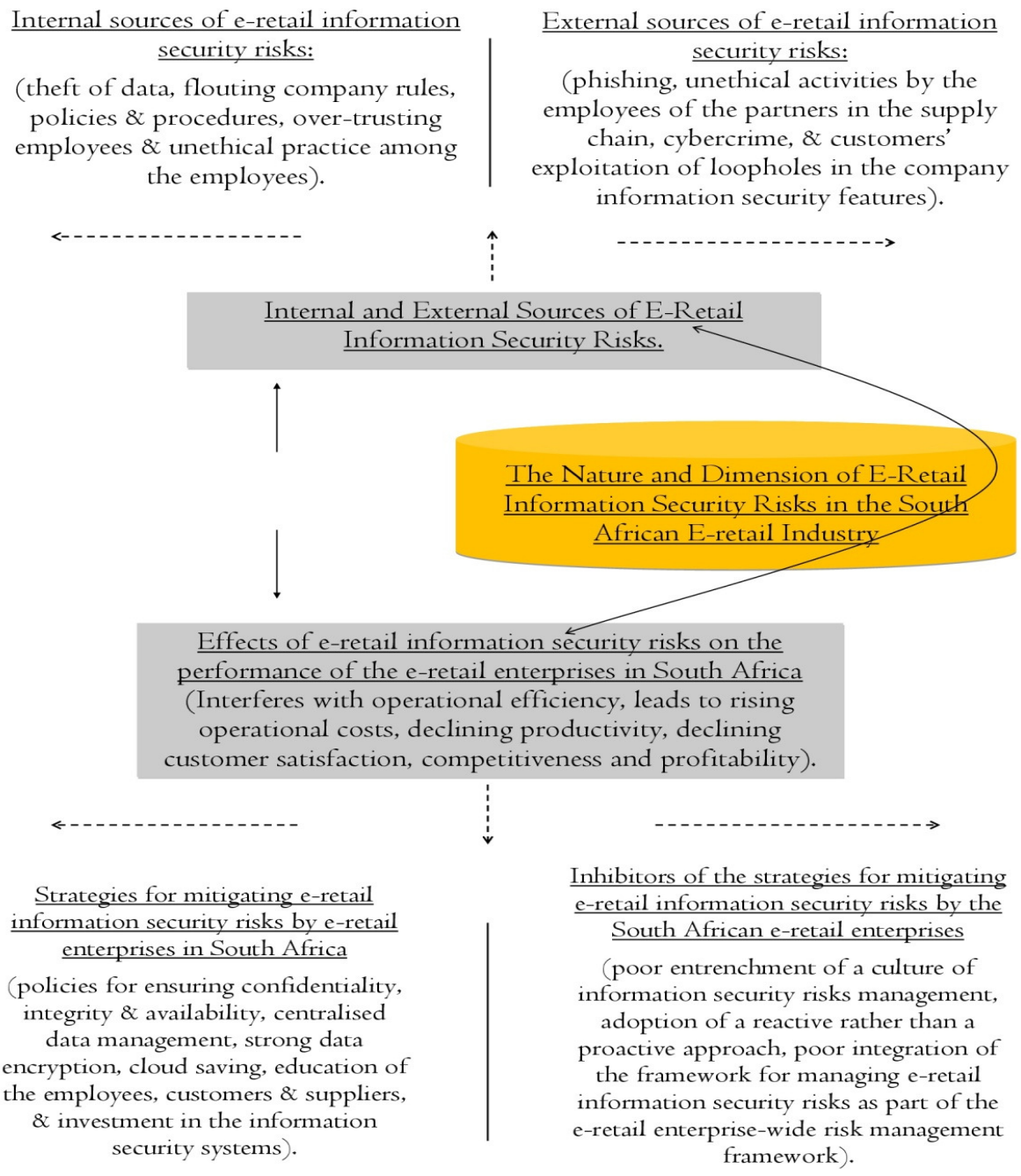

FIGURE 3: Empirical facts: e-retail information security risks in South Africa

Source: Researcher's construct as derived from the thematic content analysis and interpretation of the results of empirical studies conducted on e-retail information security risks in South Africa in the period between 2010 and 2015 (Bedi & Warden 2010:144; Jordan 2014:21; Mobius 2014:5; Nyoni & Mthulisi 2015:6).

Since the implementation of the information security measures can affect the normal workflow and productivity, most of the e-retail enterprises also tend to only go half way without completing all the essential security essentials and specifications (Jordan 2014:21). This leaves the information system vulnerable to risks and threats (Jordan 2014:21).

This is exacerbated by the fact that most of the enterprises tend to implement and adopt information security measures without necessarily training the ordinary employees (Mobius 2014:5). The implications are latent in the fact that even in the midst of the existence of effective information security measures, ordinary employees may still tend to engage in activities that affect the security of the enterprise information system. Such a situation breeds a culture that does not support the initiative for improving the effectiveness of e-retail information security management (Dagada *et al.* 2013:9).

6.2.2 Culture

The development of an effective information security culture is a challenge that mars the ability of most of the e-retailers to successfully implement information security measures (Bedi & Warden 2010:144). Poor change and transformation in the behaviours and practices of managers and employees affect the effectiveness of information security policies and measures that could have been adopted (Bedi & Warden 2010:144).

Most e-retailers tend to adopt new information security measures without constant evaluation of the extent to which the overall organisational practices and behaviours have changed and transformed to support such initiatives (Bedi & Warden 2010:144). Even in cases where the accompanying measures for changing and transforming behaviours have been undertaken, major focus has often only been directed towards the internal employees and managers (Kgopa 2013:580).

Yet, in actual practice, the networks of the transactions involved in the accomplishment of e-retail operational activities and transactions often span beyond the nature of the interactions that often take place between the employees and managers (Kgopa 2013:580).

In an effective e-retail operation, the web of the online activities that must be managed to enhance identification and mitigation of information security risks include customer and

supplier related users. Other users include the transporters and third party firms involved in the deliveries of the ordered online goods to e-customers (Kgopa 2013:580). By concentrating only on the internal users such as employees and managers, the organisational culture for information security is only partly changed and transformed (Fichard 2015:2; Jordan 2014:116).

As the internal users therefore undertake the necessary measures to limit the vulnerability of the e-retail information system to risks, most of the information systems of the e-retailers are left vulnerable to risks (Jordan 2014:116; Nyoni & Mthulisi 2015:6). Such a circumstance is further exacerbated by poor enforcement that creates the situation where most of the employees tend to continue engaging in activities such as visiting dangerous sites and being caught through phishing that put the entire system at threat and risks (Jordan 2014:116; Nyoni & Mthulisi 2015:6).

6.2.3 Reactive approach

The reactive rather than proactive approach undertaken by most of the e-retailers for managing information security is one of the other limitations of the effectiveness of the approach that most e-retailers use to enhance the overall effectiveness of their information systems (Hansen 2013:16; KPMG 2011:10). Unless the information security problem becomes quite acute, most e-retail executives are often reluctant to invest in the appropriate information security system.

Most of the e-retail enterprises are largely small scale enterprises that do not have enormous capital finance (KPMG 2011:10). This implies although there could be willingness to take proactive approach to information security management, the impetus to do so is often constrained by the need to optimise the limited resources by only focusing on the areas of acute challenges (Dlodlo & Dhurup 2003:164). In effect, most e-retail enterprises tend to continue using the system as it is, even if it is widely evident from the symptoms that their information systems are under attack (Hansen 2013:12).

Just like the traditional retail enterprises, e-retailers operate in cohort and concert with other businesses and partners (Mobius 2014:5; KPMG 2011:10). This signifies the e-retail

enterprise that does not take the necessary precautionary measures turns to be the source through which the information systems in partner and sister businesses are attacked or infected (KPMG 2011:10). Unless addressed across all the web of interactions among the related e-retailers, the problem may become cyclical to thereby endanger the enterprise's information security risks (Hansen 2013:16).

Even in circumstances that the e-retail executives opt to invest in superior systems, constant monitoring and evaluation is often not undertaken to ensure that the security features are upgraded to respond and thwart the likely information security risks before they occur (Hansen 2013:16). Sources of information security risks are constantly evolving and changing. Without constant update, most of the protection mechanisms put in place tend to become obsolete and vulnerable to modified forms of contemporary attacks (Hansen 2013:16; KPMG 2011:10; Mobius 2014:5). Such a challenge is often further exacerbated by the less prioritisation of information security risk management.

6.2.4 Enterprise risks

In most of the e-retail enterprises, information security risks does not feature among the top 10 strategic risks that include business continuity risks, capital project risks, regulatory risks, productivity efficiency risks, environmental management, commercial risks, safety management, supply chain risks, reputational risks and human capital risks (Michalson 2014:1; Pick n Pay 2013:44; PM&A 2014:5; Woolworths 2014:67). Information security risks would have been clustered under productivity efficiency risks or reputational risks (Mobius 2014:5). Productivity efficiency risks are the events that cause failure to achieve a quantum leap improvement in operational efficiency and asset utilisation.

The same ambiguity is also latent in the description of reputational risks that are the events that can affect the reputation of the enterprise (Mobius 2014:5). In the midst of the increasing information security threats in the South African business environment, such approach undermines the extent to which e-retail enterprises are able to take the necessary proactive measures that can lead to the minimisation of the vulnerability of their information systems to risks (Hansen 2013:12).

Following the outsourcing of information security services to third party professional IT contractors, most e-retail executives are often a little reluctant to constantly conduct analysis and upgrade information security system (Nyoni & Mthulisi 2015:1). The implications are manifested in the fact that if events or incidents occur, it is often not easy to undertake immediate response due to lack of the contingent funds put in place to supplement on the available funds (Von Solms & Von Solms 2010:3).

The extensive nature of the structures of certain widely growing and expanding e-retail enterprises can also cause the disintegration of the information security framework in which each division tends to manage its own information security system. The emergence of a more disintegrated information system limits effective monitoring and identification of information security breaches (Von Solms & Von Solms 2010:3). It also affects the standardisation of information security policies and procedures to minimise system and data vulnerability (Von Solms & Von Solms 2010:3).

7. DISCUSSION

Effective management of information security risks is one of the critical determinants for effective performance of the contemporary businesses. It edifies the identification and mitigation of the information security risks. This enables the executives to reduce and control financial costs and cost of inconveniences resulting from system failures.

Through the effective management of information security risks, e-retail executives are not only able to control costs, but also to significantly improve their operational efficiency to effectively respond to the needs and demands of the customers. This is often realised by the fact that as most of the information security risks are mitigated, reduction in the incidents of system failures can significantly impact on efficiency improvement.

However, to achieve such enormous business values, it is not only the allocation of the required financial resources that matter, but also the use of more logical steps ingrained in the six steps' framework (assets' analysis, assessment of sources and symptoms of risks, vulnerability's analysis, intervention & evaluation).

Although the use of such a framework influences the overall effectiveness of the process for managing e-retail information security risks (Almeida & Portela 2013:16; Forrester 2010:16; KPMG 2011:7), theories also indicated certain four elements for information security management (organisation, process, people & technology) to be moderated by certain six dynamic interconnections (culture, governance, architecture, emergence, enabling and support & human factors) to create a coherent three-dimensional and dynamic proactive framework for managing a firm's information security risks (Bediako 2014:119; Ekelhart *et al.* 2009:3; ISACA 2015:5). Such approach leaves the critical process for the identification and mitigation of e-retail information security risks strongly supported by transformed and changed organisational behaviours and practices.

However, the linkage with such moderating factors seems lacking in most of the frameworks used by most of the e-retail enterprises to diffuse the associated e-retail information security risks. Instead, most of the approaches used by the e-retail enterprises seem to take the tone of a more isolated and limited six steps' framework that authors such as Almeida and Portela (2013:16), Forrester (2010:16) and KPMG (2011:7) highlight to involve; the analysis of the existing assets, the assessment of the sources and symptoms of information security risks, the analysis of the vulnerability of a firm's assets, the design of the intervention measures, and monitoring and evaluation (Hansen 2013:16).

Even for e-retail enterprises that strive to adopt the appropriate frameworks for mitigating e-retail information security risks, the initiatives to do so are often still inhibited by unsupportive organisational culture and poor integration of e-retail information security risks as part of the enterprise-wide risks that must be effectively identified and mitigated (Jordan 2014:116; Nyoni & Mthulisi 2015:6).

In some of the e-retail enterprises, all these are often further exacerbated by the poor management recognition of e-retail information security risks as a vice that threatens the effective performance of the contemporary South Africa e-retail enterprises (Hansen 2013:12).

The implications are latent in the fact that as the e-retail executives engage in such practices, most of the e-retail information systems are left largely vulnerable to the

increasingly complex internal and external sources of information security risks (Hansen 2013:12).

8. MANAGERIAL IMPLICATIONS

For e-retail executives to identify and diffuse all the potential sources of e-retail information security risks, it is reiterated in Figure 4 that they must be able to adopt a framework that not only enhances a logical step by step approach for identification and mitigation of e-retail information security risks, but also the integration of ISACA's (2015:5) four elements and six dynamic interconnections.

The adoption of a logical step by step framework will provide a systematic process for e-retail executives to conduct constant monitoring and evaluation and mitigate all sources of information security risks. The integration of ISACA's (2015:5) four elements and six dynamic interconnections will aid and induce the evolution of the organisational culture, behaviours and practices that support the daily initiatives to avoid exposure of the e-retail enterprises to information security risks.

To accomplish this, it is illustrated in Figure 4 that the *first* initiative will require the e-retail executives to integrate information security risks as part of the enterprise risk management framework and in the strategic planning process. Such approach will enhance allocation of sufficient resources and the entire organisational commitment.

Secondly, the e-retail executives must create an interface between the four (4) BMIS' elements and six (6) dynamic interconnections to provide effective foundation for the implementation of information security measures.

The four (4) BMIS' elements for information security management that the e-retail executives must consider include organisation, process, people and technology.

The six dynamic interconnections (DIs) for information security management encompass culture, governance, architecture, emergence, enabling and support, and human factors. The creation of such interface will provide the foundation for the design and application of a five step framework for e-retail information security risks management.

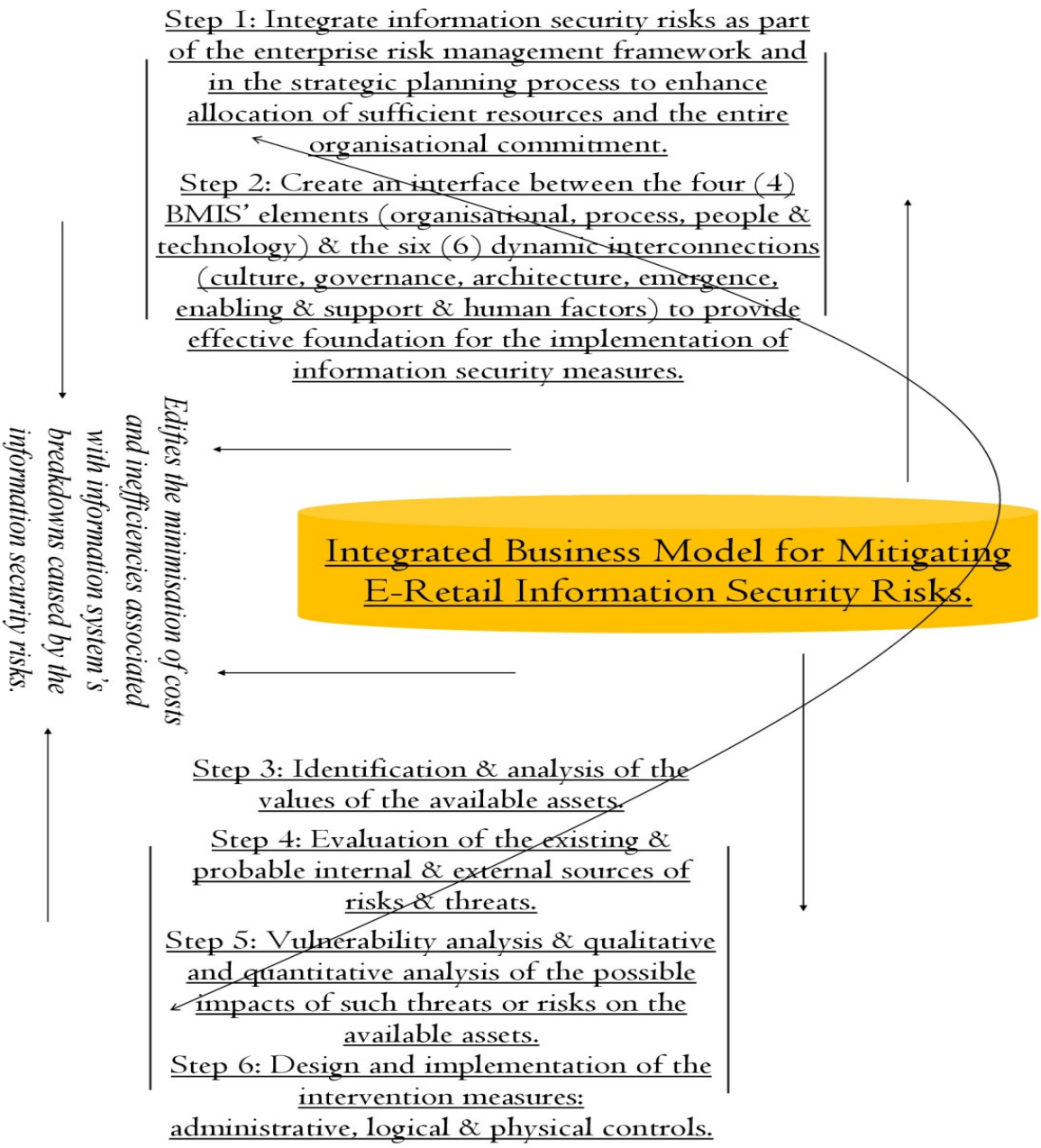

FIGURE 4: Integrated business model for mitigating e-retail information security risks

Source: Researcher's own construct as derived from the linking of the six steps' framework articulated by authors such as Almeida and Portela 2013:16, Forrester 2010:16 and KPMG 2011:7 with ISACA's 2015:5 four elements and six dynamic interconnections.

Such a foundation will edify the effective accomplishment of the activities in the *third step* that require the identification and analysis of the values of the available assets.

The assets that can be examined encompass computer hardware, software, data and supplies, building, communication equipment, valuable information and people.

With thorough understanding of the available assets, the assessment of the degree of their vulnerability can be undertaken using the *fourth step* that involves the evaluation of the existing and probable internal and external sources of risks and threats.

In such analysis, the common sources of information security risks are often linked to employees, customers and supplier related sources, and external sources related to cybercrimes. This analysis must be accompanied by the identification of the symptoms of information security risks such as evidence of intrusion, data interference, computer interference, information modification, false use of data, unauthorised transactions, frequent computer failures, unsolicited e-mails from suspicious sites and attachments and evidence of negligence.

All these lead to vulnerability analysis that requires the assessment of whether the enterprise information system can be affected if the risk or threat occurs. In this regard, it is indicated in the *fifth step* of the business model in Figure 4 that vulnerability analysis must be accompanied by qualitative and quantitative analysis of the possible impacts of such threats or risks on the available asset, productivity, cost effectiveness and value of the asset.

This leads to the *sixth step* that entails the design and implementation of the intervention measures that may include the establishment of administrative controls, logical controls-such as data encryption the use of passwords and codes, and physical controls.

As these measures are being implemented, it is critical to undertake constant monitoring and evaluation of the efficiency of the intervention measures as well as how such measures are aiding the e-retail enterprise minimise costs and inefficiencies resulting from frequent cyber attacks that cause system failures.

Such evaluation must also involve the assessment of the change and transformation in the organisational behaviours and practices to support the initiatives for ensuring effectiveness of the information security risk management.

9. CONCLUSION

Effective management of information security is a critical determinant of e-retail operational efficiency. However, a major paradox seems still linked to the fact that the approach adopted for the identification and mitigation of e-retail information security risks is still largely underdeveloped due to poor management recognition of e-retail information security risks as a vice that threatens the effective performance of the contemporary e-retail enterprises.

Even for e-retail enterprises that strive to adopt the appropriate frameworks for mitigating e-retail information security risks, the initiatives to do so are often still inhibited by unsupportive organisational culture and poor integration of e-retail information security risks as part of the enterprise-wide risks that must be effectively identified and mitigated. In effect, it is quite evident that this research has achieved its fundamental motive which was to evaluate the overall effectiveness of the strategies used for mitigating information security risks by the e-retail enterprises in South Africa, so as to develop a business model that edifies the e-retail enterprises' capabilities to identify and mitigate all e-retail information security risks.

To solve the identified conceptual deficiency of lack of an effective business model, it is suggested in Figure 4 that the executives must consider adopting a business model that links the four elements and six dynamic interconnections with the six steps' framework to create a coherent proactive approach for enhancing effective identification and mitigation of e-retail information security risks.

However, considering that the nature of the contemporary e-retail information security risks is constantly changing, future studies can explore how the critical constructs outlined in Figure 5 remain relevant and effective for identification and mitigation of such risks.

REFERENCES

ALMEIDA F & PORTELA I. 2013. Organizational, legal, and technological dimensions of information system administrator. London, UK: IGI Global Publishing.

ALQATAWNA J. 2014. The challenge of implementing information security standards in small and medium e-business enterprises. *Journal of Software Engineering and Applications* 7(1):883-890.

AL-SOMALI SA, CLEGG B & GHOLAMI R. 2010. E-business adoption and its impact on performance. *Encyclopaedia of E-Business Development and Management in the Global Economy* 2(1):3-11.

BEDIAKO T. 2014. Enterprise risk management. integrated framework. ISACA'S IT Audit, information security & risk insights Africa 2014, Alisa Hotel May 20.

BEDI DS & WARDEN SC. 2010. Information security in hospitality SMMEs in Cape Metropolitan Area: the management and culture perspective. Proceedings of the South African Information Security Multi-Conference (SAISMC).

BELAYNEH B. 2014. Time is here to fight back cybercrooks: 10 questions to answer. Centurion: South African Centre for Information Security.

BLANCHETTE P. 2012. Frege's concept of logic. New York, NY: Oxford University Press.

BOGHOSSIAN P. 2011. Williamson and the a priori and the analytic. *Philosophy & Phenomenological Research* 82(1):488–497.

BOJANC R & BLAZIC BJ. 2013. A quantitative model for information-security risk management. *Engineering Management Journal* 25(2):25-35.

CEB. 2015. Information risk: audit and compliance teams turn to root cause analysis. London, UK: CEB.

CHERDANTSEVA Y & HILTON J. 2013. A reference model of information assurance & security, availability, reliability and security (ARES). New York, NY: Pearson Press.

CITRIX. 2014. Top 10 reasons to strengthen information security with desktop virtualization: regain control and reduce risk without sacrificing business productivity and growth. Santa Barbara, CA: Information Security White Paper. [Internet: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/top-10-reasons-to-strengthen-information-security-with-desktop-virtualization.pdf; downloaded 2016-11-24.]

DAGADA R, ELOFF MM, VENTER LM & MERAKA SAP. 2013. Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant? Johannesburg: University of the Witwatersrand.

DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS. 2014. Information security breaches survey. London, UK: Information Security Europe.

DLODLO N & DHURUP M. 2003. Barriers to e-marketing adoption among small and medium enterprises (SMEs) in the Vaal Triangle. *Acta Commercii* 1:164-180.

EASTTOM C. 2011. Computer security fundamentals. New York, NY: Pearson Press.

EKELHART A, FENZ S & NEUBAUR T. 2009. AURUM: a framework for information security risk management. *Proceedings of the 42nd Hawaii International Conference on System Sciences.*

FARIBORZ F, NAVATHE B, GUNTER P & ENSLOW SPH. 2014. Evaluating damages caused by information systems security incidents. Atlanta, GA: Georgia Institute of Technology.

FERNIE S, FERNIE J & MOORE C. 2013. Principles of retailing. Edinburg, SCO: Herriot-Watt University.

FICHARDT C. 2015. Just how big a threat is cybercrime to SA? Johannesburg: Business Day.

FORRESTER M. 2010. The value of corporate secrets. Johannesburg: EMC (Security Division.)

HANSEN S. 2013. Cybercrime: security risks and challenges facing business. Johannesburg: Symantec.

HARNISH P. 2015. What are the most common causes of security breaches? London, UK: Net Security.

HARTONO E, HOLSAPPLE C, KIM K & SIMPSON J. 2014. Measuring perceived security in B2C electronic commerce website usage: a respecification and validation. *Decision Support Systems* 62(2):11-21.

HOWARTH F. 2014. The role of human error in successful security attacks. *Security Intelligence* 14(2):1-16.

IGLESIAS PS, PASCUAL MF, HERNANDEZ GA & CHAPARRO PG. 2013. Barriers and drivers for non-shoppers in B2C e-commerce. *Computers in Human Behaviour* 29(2):314-322.

ISACA see INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. 2015. The business model for information security. Meadows, NC: ISACA.

JORDAN P. 2014. Information security awareness in small information technology-dependent business organisations. Johannesburg: University of Johannesburg.

KAMARAJU A. 2012. The 4 leading causes of data security breakdowns. London, UK: VP Product Development and Partner Management.

KGOPA AT. 2013. Information security issues facing internet café users. *International Journal of Computer Science and Electronics Engineering (IJCSEE)* 1(5):580-587.

KPMG. 2011. Cutting through complexity; information security risk assessment; what hasn't been assessed, can't be managed. Cape Town: IT Advisory Services.

MICHALSON L. 2014. Current trends of information security in South Africa. Centurion: Centre for Information Security Law.

MOBIUS. 2014. Corporate information security in South Africa. Johannesburg: Mobius Consulting.

NOTENBOOM L. 2008. Keeping your computer save on the internet. *The Electronic Journal of Internet Safety* 1(2):1-40.

NYONI P & MTHULISI V. 2015. Data protection laws and privacy on Facebook. *South African Journal of Information Management* 17(1):1-10.

PICK N PAY. 2013. Integrated annual report. Cape Town: Pick n Pay.

PM&A. 2014. Cyber security in South Africa. Cape Town: PM&A.

PRICEWATERHOUSE COOPERS. 2015. Managing cyber risks in an interconnected world. Johannesburg: PWC.

SALEH MS & ALFANTOOKH A. 2011. A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics* 9(2):107-118.

SOTO AP & MERONO CAL. 2008. Analyzing e-business value creation from a resource-based perspective. *International Journal of Information Management* 28(1):49-60.

VON SOLMS B & VON SOLMS R. 2010. The 10 deadly sins of information security management. Johannesburg: RAU-Standard Bank Academy for Information Technology.

WOOLWORTHS. 2014. Integrated report. Cape Town: Woolworths.