Conceptualising antecedents of systems innovation on information security risks

By

Mogotsi Steven Botsime

Submitted in partial fulfilment of the requirement for the Degree

Magister Commercii

In

Business Management

College of Business and Economics

UNIVERSITY OF JOHANNESBURG

Supervisor: Prof. Kennedy Njenga

2019

ABSTRACT

This research represents a comprehensive conceptualisation of antecedents of systems innovation and how they affect systems innovation in an organisational context. It further examines the relationship between information security risks and systems innovation. Antecedents of systems innovation are identified based on the existing theories such as Diffusion of Innovation (DoI) and Organisational Innovation. This research makes use of new systems and technologies which include Big Data/Cloud Computing, Blockchain, Internet of Things (IoT), Virtual/Augmented reality and Artificial Intelligence (AI) to examine organisations strides towards systems innovation. This research is underpinned by the increase in systems innovation and the growing concerns of information security risks faced by organisations.

A quantitative method of analysis was used to analyse data using statistical methods with a view to identify relationships between variables. Data collected shows that systems and technology must have increased benefits in order to be adopted and the complexity of systems does not affect the adoption of such systems and technologies. Individual characteristics were found to have no effect in systems innovation whereas organisational and environmental elements highly influence innovation in the organisation. A relationship could not be established between systems innovation and information security risks. This research highlights the importance of ensuring that new systems and technologies adds value to the organisation and equally important is to ensure management of organisational and environmental elements that affect systems innovation. Information security risks should also not be a deterrence for systems innovation.

Keywords: Systems Innovation, Information Security Risks, Organisational Innovation, Diffusion of Innovation

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude and appreciation to the following people for having supported me throughout my research:

- My fiancé Ms. Phethile Manzini for your encouragement, patience and support during my research.
- My supervisor Prof. Kennedy Njenga for his guidance, motivation and patience. Thank you for always pushing me to do my best and I appreciate the faith you showed in me.
- My manager Ms. Joey Mabena, thank you for the continuous encouragement and allowing me time off work for my studies.

DEDICATION

I dedicate this dissertation to my son, Kgosietsile Itumeleng Botsime. Thank you for your understanding when I could not spend time with you while I was busy with this work. May this inspire you to relentlessly pursue excellence and to do your best in anything you do.

Table of Contents

List of Figures

List of Tables

CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1. Introduction

Organisations are increasingly pursuing systems innovation as a way to enhance their competitive advantage and to adopt emerging technologies with a view of transforming their business operations. Information security concerns that come with new technology often deters organisations from pursuing innovation. It is for this reason that a study of antecedents of systems innovation and its relationship with information security risks is imperative.

This research examines systems innovation in the context of adopting emerging technologies such as Blockchain, Internet of Things (IoT), Big Data/Cloud Computing, Virtual/Augmented Reality and Artificial Intelligence (AI). The concept of systems innovation refers to an interconnected set of innovations where each innovation influences the other (Mulgan & Leadbeater, 2013). The context of this research is relatively broad as it looks into all types and sizes of organisations in all sectors. This is because innovation is undertaken by various types of organisations and it is important to capture a broad sense of issues relating to this study.

Information security risks that come with these new systems and technologies are also at the core of this research as a relationship between systems innovation and information security risks will be examined. Antecedents of systems innovation, as identified from some prominent innovation theories, are used in this research to examine the way organisations pursue systems innovation. Information security is pertinent in the area of systems innovation, it is for this reason that this research seeks to examine the relationship between systems innovation and information security risks.

This chapter outlines the background of antecedents of systems innovation and information security and highlights related research that has been done on these topics. A research gap and problem statement are also outlined to provide a comprehensive overview of the significance of this research. The research questions and objectives are also highlighted in this chapter with a view to provide a clear understanding of what the research seeks to achieve.

1.2. Background

In understanding the concept of systems, the Aristotelian world view presents a profound statement that “the whole is more than the sum of its parts” (von Bertalanffy, 1972:407) which implies that a system is made up of various interconnected components. Systems theory has played an important role in many technological advancements (Antsaklis & Michel, 2007). As such, the concept of systems is closely related to innovation which is defined by Amabile (2011) as the successful implementation of creative ideas within an organisational context.

Pieters (2011) defines information security as the tools and instruments used to protect information assets against attacks. Organisations experience increasing costs as a result of information security risks which is why it has become a critical issue (Feng *et al.,* 2014). The issue of ensuring commitment and understanding of employees to the objectives of information security is increasingly becoming pertinent as organisations continue to capitalise, build and rollout information security systems (Chang & Lin, 2007). A large number of security breaches are as a result of employee non-compliance with information security policies (Nograšek & Vintar, 2014; Hu *et al.*, 2012; Thompson, 2016). According to Hallová *et al.* (2017), successful implementation of information security can be attained through the implementation of various interventions which include the development of policies, procedures, processes, organisational structures and software, and hardware functions.

According to Nechaev *et al.*, (2017) innovation activities often cannot be calculated in advance, therefore, there is always an element of risk involved. It is so because there is almost no complete guarantee of a successful outcome in any innovation initiative. Because of the uncertainty brought by innovation it is important to examine its risks, particularly from an information security context.

Most organisations face major challenges stemming from information security risks (Bulgurcu *et al.*, 2010) and various reports in the field of information security increasingly highlight that the main source of information security attacks are internal employees (Wall & Singh, 2018; Chmura, 2016). This emphasises the importance of having a comprehensive understanding of human behaviour in an organisational context and how it affects innovation.

When looking at similar studies conducted in a South African context it is worth noting that most studies relate to information security culture in organisations. Da Veiga (2008:02) defines information security culture as “the manner in which employees perceive and interact with the controls that are implemented to protect computer and information systems and assets in the organisation”. In his study, Nel (2017) investigates a measuring mechanism and acceptable standards for information security culture which aims at improving organisational culture. In their study van Niekerk and von Solms (2003) examined the establishment of information security culture within an organisation. Da Veiga and Martins (2015) have also studied how an information security culture within an organisation can be constantly improved to enhance employee compliance to policies and procedures relating to information security.

Some research has been done on information security to explain why employees engage in deviant security related acts, how to deter them as well as how to persuade them to act as protective agents of information assets (Wall & Singh, 2018). However, these studies are unable to comprehensively unpack the relationship or correlation between information security risks and antecedents of systems innovation in organisations.

1.3. Purpose of the Study

As organisations strive to innovate and invest heavily in information security systems and technologies, the concept of ensuring employees’ commitment and understanding of organisational information security interventions has become even more imperative (Chang & Lin, 2007). As such, the problem statement for this study is centred around understanding information security risks brought by the adoption of new and emerging technologies. This problem statement will assist in unpacking and gaining an understanding of the correlation between the two variables. Given this problem statement, the research therefore delimited to focus only on studying relationships between variables and shall only consider innovation in the context of the five technologies as highlighted in the introduction above. The study will also be limited to South African organisations only.

Millions are spent by organisations on technical security tools like firewalls, intrusion detection systems (IDSs) and encryption tools with a view to ensure protection against

common technological threats (Jouini & Rabai, 2016). Therefore, if information security risks and systems innovation correlate, it would mean that organisations would need to consider the use of multiplexity of solutions to tackle information security risks particularly in when adopting new systems. According to Alzamil *et al.* (2015) risk is considered proportional to the expected losses which can be caused by an event and to the probability of such event. This is an indication that organisations face a great loss if information security risks are not adequately managed and controlled.

1.4. Research Objectives

This study seeks to explore the relationship between systems innovation and its antecedents as well as with information security risks in an organisational context. In light of the above research objective, the main research shall also seek to meet the following secondary objectives;

- Examine the relationship between systems innovation and information security risks;
- Examine the relationship between systems innovation and its antecedents using attributes of Diffusion of Innovations; and
- Investigate the extent to which systems innovation is influenced by its antecedents through organisational innovation.

1.4.1. Research Questions

- How does systems innovation influence information security risks within an organisational context?
- What relationship exists between components of innovation theories and systems innovation?
- To what extent do antecedents of systems innovation influence the rate of systems innovation in organisations?

1.5. Justification of the Study

This study provides valuable insights as it investigates information security risks in relation to new technology and systems implemented in an organisational context. The findings of this research will be important as they will provide insights to organisations with regards to how information security relate to systems innovation. As stated in the background, a research gap exists in the literature as there has not been enough

research done on information security risks relating to systems innovation and the same is also true regarding the investigation into antecedents of systems innovation.

1.6. Chapter Layout

According to Academic Coach and Writing (ACW) (2017), there are many variations on how the chapters of a research report can be structured. For this research the chapters shall be structured as follows;

Chapter 1: Rationale and Background

This chapter provides a background of the research topic and also gives a brief overview of why the research is being conducted. The rationale and background chapter also identifies gaps in the literature which the research aims to address.

Chapter 2: Preliminary Literature Review

The preliminary literature review provides a broader theoretical understanding of the topic. This chapter also establishes a link with other similar studies that have been conducted. The literature review forms a theoretical basis for this study. The theoretical framework and research hypotheses are also outlined in this chapter.

Chapter 3: Research Methodology

This chapter examines the approach and methodological choice for the research. It also outlines the way the research will be conducted. The research methodology chapter explains the research paradigms, epistemological approach as well as the philosophical paradigms. Sampling techniques, research population, and data collection mechanisms are also outlined in Chapter 3.

Chapter 4: Research Findings and Analysis

In this chapter, the data gathered will be interpreted, analysed and evaluated. This chapter provides a statistical analysis of the data collected which shall assist in making conclusions thereby developing research findings. Therefore, the result of the research will be found in this chapter. The research hypothesis will also be tested in this chapter.

Chapter 5: Discussion and Conclusion

Chapter 5 links the research finding with the research objectives and also contextualises the data analysis to link with the objectives of the study. This chapter also discusses the research findings and their implications on the population and to the general business environment. While serving as the overall conclusion for the research, this chapter also discusses the limitations of the study as well as the contribution to knowledge.

1.7. Chapter Summary

The background, objectives and problem statement are outlined in this chapter, and these sections provide an outline of the study and its intentions. The concepts that are being studied are also outlined in this chapter providing a comprehensive view of how the study links to the organisational environment. This chapter, therefore, serves to introduce the study, it's intentions and its key components.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

Pieters (2011:327) defines information security as “the tools and mechanisms used for the protection of information in the face of attacks”. The main objective of information security is to ensure the confidentiality, integrity and information availability (Chmura, 2016). In order to achieve this objective organisations often implement technology tools, processes and procedures to protect against information security risks which are particularly aimed at undermining confidentiality, integrity and availability of information. Stewart & Jürjens (2017) considers human activity as the most critical factor in the management of information security and therefore this presents significant risks to information security.

2.2. Information Security Risks

Bhattacharjee *et al.* (2012) define information security risks as potential damage that is caused when a threat exploits a vulnerability to cause damage to an information asset. In order to deal with such vulnerabilities, organisations need to implement both physical and organisational measures (Fenz & Ekelhart, 2009). Also important is the measurement of the probability of information security risks, as Ekelhart *et al.* (2009) indicate that threat probability determination is the solution to determining realistic threat probability values and, thus the risk calculation. A quantitative and qualitative analysis is needed to determine the probabilities of the various possible threats (Ketel, 2008).

There are several security frameworks, which can be used to quantify the effectiveness of security controls in an organisation (Breier & Hudec, 2011). According to Ataya (2013), Control Objectives for Information and Related Technologies (COBIT) 5, is used by enterprises to build and sustain an efficient and effective core risk governance and management of activities as well as to describe processes of identifying, analysing, responding to and reporting on risk. The International Standards Organisation (ISO) 27001 is another framework used in the field of information security risk. Lomas (2011) states that ISO 27001 is a framework used mainly for risk assessment, risk treatment, risk controls, risk monitoring and reviews, risk improvements, documentation systems, audits, and reviews. Information security

standards provide an organised method of management to implement best practices in controls and in measuring the level of risk that is acceptable within organisations (Pinheiro & Júnior, 2016).

2.3. Information Security Policy Compliance

One of the most effective ways to manage information security in organisations is through the development and implementation of stringent policies that govern employee behaviour, particularly when dealing with information assets. Employees' adherence towards established Information Security Policies (ISP) is critical when seeking to reduce information security risks (Nasir *et al.*, 2017). Buthelezi *et al.* (2016) notes that organisational culture also plays an important role in this regard as compliance with the ISPs is heavily dependent on what is accepted as appropriate behaviour among fellow employees. The ISO 27001 assists organisations to have a policy and an approach or framework for implementing, sustaining, monitoring, and improving systems in line with organisational policies and culture (Lomas, 2011).

One of the major issues affecting ISP compliance is the awareness of such policies within an organisation. In their study, Bulgurcu *et al.* (2010) found that information security awareness of employees has a direct influence on their attitude toward compliance. As Hina and Dominic (2017) reiterates, the effectiveness of ISPs is still questionable as the content of these policies is not often delivered through reliable security education, training and awareness programs. Organisations therefore need to raise the information security awareness level of users in order to protect themselves against information security attacks (Alohali *et al.*, 2017).

2.4. IT Governance

Information Technology (IT) governance consists of policies and procedures with appropriate controls for monitoring IT risks, controlling IT assets, and ensuring compliance with laws and regulations (Nicho & Khan, 2017). The prevailing culture within organisations also has an impact on the manner in which they strive to manage the governance of IT. The interconnectedness of IT creates a gap in understanding how information security breaches occur which is why it is important that information security interventions are linked with IT governance as well as organisational corporate governance to ensure a holistic approach in managing information security.

There's often a common misconception in many organisations that information security governance falls under the jurisdiction of their information technology department and is separate from organisational corporate governance (Corriss, 2010).

2.5. Information Security Vulnerability

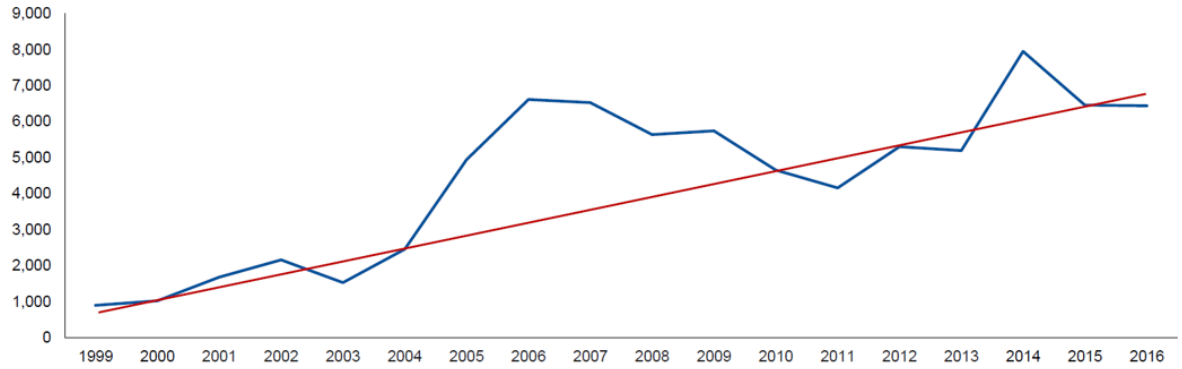
It is critically important for organisations to maintain the best condition of information security posture to lessen information security risks. According to Hlatshwayo and Adeyelure (2018) information security influences processes for successful deployment of systems in organisations. The following are some of the elements that affect information security vulnerability:

- Opazo *et al.* (2017) notes that social engineering related attacks take advantage of user apathy or lack of knowledge about good information security practices and deceive users into allowing access to malicious software programs to infiltrate information assets. These attacks are mainly based on gaining the user's trust and use various deception mechanisms to gain access to the information technology infrastructure or data. Conteh and Schmick (2016) identified various social engineering techniques which include pretexting (fabricating information in order to gain information from the target), baiting (which involves enticement strategies), *quid pro quo* where the target is offered service in exchange for information and tailgating which involves gaining access through impersonation or similar mechanisms;
- Technical flaws and ineffective information security systems to protect data also present vulnerabilities. Constant monitoring of access to information and access points, either remotely or by third-party vendors, is also essential to the continuing success of any cyber-risk plan (Thompson, 2016); and
- Social media also exposes organisations to a considerable amount of vulnerabilities and as Abubaker and Boluk (2016) indicates, activities such as sharing information, posting comments, uploading photos, and updating statuses may require users to install many types of applications and programs which may potentially pose threats to organisational information assets.

An increase in the number of vulnerabilities results in great threats to reliability and confidentiality of information systems (Zhao & Dai, 2012). Despite this reality, data

from the Gartner's (2018) database shows a steady increase of information security vulnerabilities over time as illustrated in Figure 2.1 below.

Figure 2.1: Information Security Vulnerabilities by year



Source: Gartner (2018)

Penetration testing and vulnerability assessments must be performed to identify and analyse information security vulnerabilities in order to defend networks and systems against threats and attacks (Savaglia & Wang, 2017). The use of Common Vulnerability Exposures (CVE) and Open Vulnerability Assessment Language (OVAL) lists is widely accepted as a form of best practice in dealing with information security vulnerabilities. According to Martin (2003), these lists allows for identification of mistakes in software code that may allow hackers to gain access to organisational information or capabilities.

2.6. Information Security and Organisational Culture

Studies have shown that non-technical issues are at least as important as technical issues in safeguarding an organisation's sensitive information (Alfawaz *et al.*, 2010; Bulgurcu *et al.*, 2010). Sung and Kang (2017) indicate that most security incidents start with people's mistakes and indifference, not technical inadequacies. Therefore, it is important that in combination with a technical approach, employee and organisational factors should also be addressed (Stewart and Jürjens, 2017). Corriss (2010) reiterates that in order to achieve positive results in information security management it is necessary to raise the levels of awareness of all members of the organisation so that information security becomes an integral part of the organisational culture.

Geert Hofstede developed a well-known multidimensional approach in quantitatively measuring culture in the 1980s. Hofstede's provides a theoretical framework clusters cultures based on four dimensions: power distance, individualism-collectivism, uncertainty avoidance, and masculinity-femininity (Ozdemir *et al.*, 2016). Although this model provides a rather comprehensive way in which dynamics of the organisational culture can be evaluated and measured, it is much more applicable at a national level than at a corporate or organisational level. Yoo (2011) adds that equating the stereotypical culture of a country directly to all citizens of the country would be misleading because when culture is defined at the national level it should still be tested if organisations are consistent with such cultural orientation. However, Khastar *et al.* (2011) argue that national culture has a significant impact on employees' attitudes and values. Therefore, it is important to view information security culture within an organisation as influenced by broader environmental and national cultural dynamics.

2.7. Innovation in an Organisational Context

Organisations pursue innovation for different reasons, however, all of them do it with an aim of gaining some sort of value. According to Pisano (2015) some of the reasons why organisations innovate is to make a product or service perform better, make it user friendly, more convenient to use, more reliable, more durable, and cheaper. This often requires a lot of commitment from organisations. Other organisations pursue more open-market and outbound innovation strategies where they open innovation borders to vendors, customers and even competitors (Rigby & Zook, 2002).

Organisational Factors

Innovation poses tremendous challenges, despite its promised potential, some of which may be detrimental to information security (Khazanchi *et al.,* 2007). Innovation is seen as part of a broader concept of organisational culture in many organisations. Shubin and Gladkyy (2013:240) define organisational culture as "an element of the internal environment of the organisation that has certain phenomenological components". Organisations often encounter challenges emanating from values and behaviours of employees which may include shortcuts, workarounds and informal ways of doing things, such informal ways of operating technology and systems are largely driven by organisational culture (Ashenden & Sasse, 2013). Organisational

culture is important when seeking to implement processes that support systems innovation (Khazanchi *et al.*, 2007; Tellis *et al.,* 2009).

Innovation in IT is heavily influenced by individuals and organisational culture (Seale, 2017). Joubert (2016) identifies technology innovation and a positive organisational culture as important synergies for positive technology influence in any organisation, particularly for new product development. There has been a developmental shift of privacy-enhancing technologies from risk governance and a move towards innovation governance (von Schomberg, 2011).

According to Hwang and Choi (2017), an innovative culture may strengthen cooperation between employees, and also improve compliance to ISPs and procedures. According to Stewart and Jürjens (2017) employees trained in security awareness improve innovation and increase work productivity. In order to reduce information security risks, leaders at all levels of an organisation can assist in building and sustaining a culture with strong support for innovation, experimentation, flexibility, and continuous improvement (Hagen *et al.*, 2011).

However, in their study Chang and Lin (2007) found that innovation orientated organisational culture traits are not associated with information security management principles of the CIA (Confidentiality, Integrity, and Availability) triad. Chang and Lin (2007) found that organisation characterized by innovation-oriented culture traits would find a low level of information security management implementation of confidentiality, integrity, availability, and accountability. György *et al.* (2012) also concur that user-driven innovations that are non-compliant with ISPs pose a security risk in many organisations.

Environmental Factors

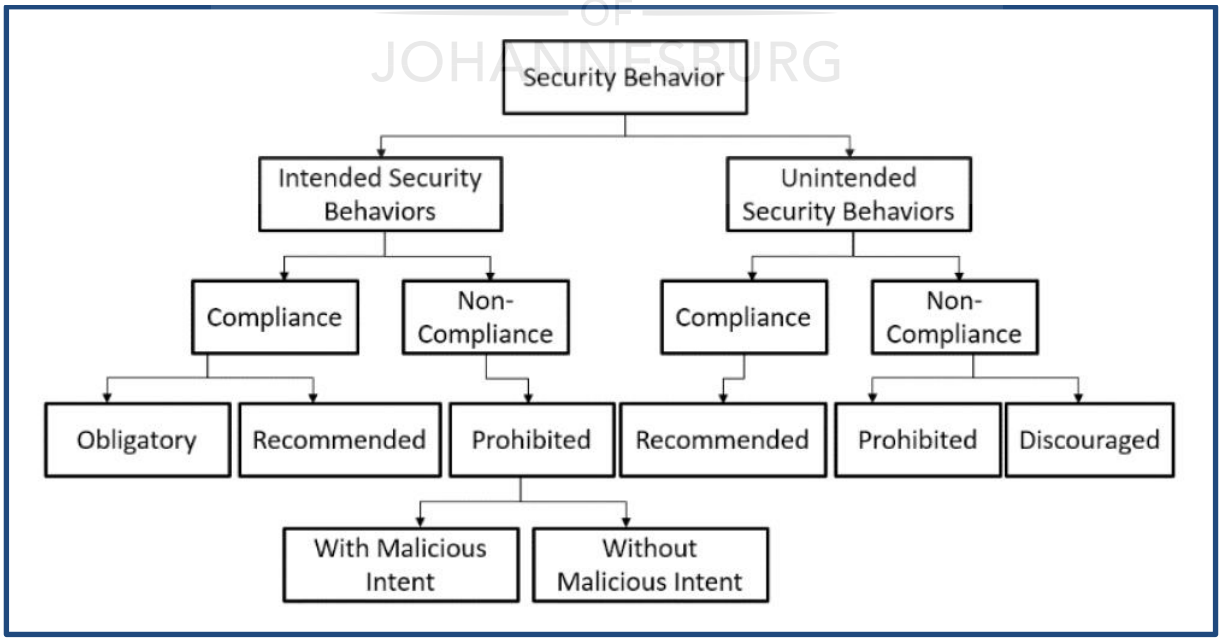
Current innovations in IT are practically applicable in almost all sectors of business and they have lower levels of risks in their local environment, however, the usage of information systems has expanded significantly with some extended to the global environment, therefore exposing these systems vastly to more security risks (Kumar & Singh, 2013; Mubarak, 2016).

Innovation is increasingly regarded as a critical source of sustainable competitive advantage that organisations can use to deal with the rapidly changing environment (Yeh-Yun Lin & Liu, 2012; Crossan & Apaydin, 2010; Hogan & Coote, 2014; Khazanchi *et al.,* 2007; Lynch *et al.,* 2010). Hogan and Coote (2014) state that innovation is a prerequisite for any organisation to succeed in increasingly dynamic and competitive markets and research also indicates that there is a positive correlation between organisational success and innovative culture.

Individual Factors

Information security research has become a well-established area within the information systems discipline over the past decade. A number of underlying theories are used by researchers from reference disciplines which includes psychology and sociology to critically analyse information security risk management (Appari & Johnson, 2010). Omidosu and Ophoff (2016) state that the ultimate success of implemented information security measures is highly dependent on the information security behaviour of computer users and actual adoption and use of security measures. Figure 2.2 below is a model of information security behaviour amongst employees.

Figure 2.2: Model of Information Security Behaviour amongst Employees



Source: Barzak *et al.* (2016)

The model by Barzak *et al.* (2016) indicates that employee behaviour towards information security can be intended or unintended and it also follows levels of compliance as well as checks on whether the behaviour is obligatory or recommended. Using this model, one can determine whether the behaviour is intended to cause harm or not. Non-compliance of employees to ISPs has been noted to lead to breaches that have cost organisations (Njenga, 2017).

2.8. Antecedents of Systems Innovation

A number of organisations are embracing and welcoming the notion of information system innovation and the effective adoption and the diffusion of information systems and technologies in organisations has become a key managerial objective (Matsebula & Mnkandla, 2016). For this reason, systems innovation is unpacked examining the adoption of systems and technologies such as the Internet of Things (IoT), Artificial iIntelligence (AI), blockchain, cloud computing/big data, and augmented reality/virtual reality.

2.8.1. Artificial Intelligence (AI)

XIao-yang (2011) defines artificial intelligence as the study of how machines are used to imitate the human brain to conduct thinking and cognitive activities. Over the past 20 years, significant progress has been made towards the advancement of AI technologies and some of the examples include Google's AI system, AlphaGo, which successfully challenged Lee Se-Dol (one of the world's Go players) in a Go match (Gan *et al.*, 2017). Recent studies also show that AI applications may be better at identifying and diagnosing eye diseases than human doctors (Ward, 2018). Developments of AI applications in the past years enable the use automation of customer service tasks with significant efficiency gains in various sectors (Riikkinen *et al.,* 2018).

A study conducted by Gartner in 2018 shows that 4% of Chief Information Officers (CIOs) have already implemented AI within their organisations, while a further 46% have developed plans to do so (McCall & van der Meulen, 2018). Forni and van der Meulen (2018) predicts that by 2022, AI applications will replace highly trained professionals in the fields of medicine, law and IT. In the next decade, AI applications

and techniques will increasingly be adopted in our daily lives to decrease the human burden of some tasks (Lyu, 2018).

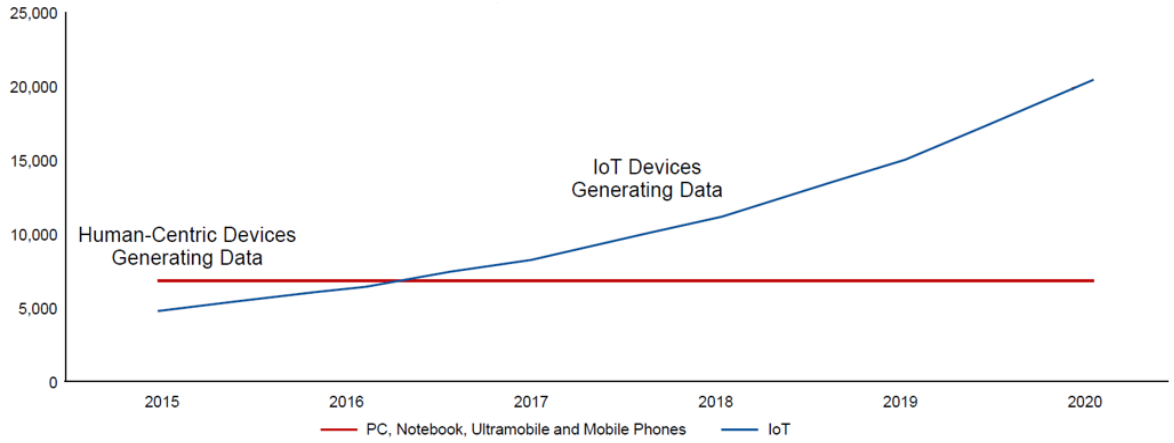
XIao-yang (2011) argues that with the increasing development of AI and maturation of its application methods, AI will become increasingly powerful in its serviceability of information security assurance. However, Gan *et al.* (2017) believe that an increase in the AI adoption may present many unintended consequences if related threats are not identified and prevented timeously. With all the benefits of AI, there comes new threats of diminishing privacy (Srivastava *et al.*, 2017).

2.8.2. Internet of Things (IoT)

IoT involves the use of different technologies and applications with capabilities involving blockchains, virtual reality, connectivity to the cloud, artificial intelligence and big data analytics (Vermesan *et al.,* 2017). The use of computers has moved from mobile devices to connected IoT devices, in an era where IoT security has changed from time to time in response to technological changes and market needs (Vorakulpipat *et al.*, 2018). Li *et al.* (2018) state that while IoT has the potential to offer users smart capabilities, it is also affected by raising security and privacy challenges.

IoT technologies have experienced tremendous growth over the past years, by 2015, 4.9 million devices were already connected and 25 billion devices will be connected by 2020 (Lyu, 2018). There has been a number of estimates of the impact of the IoT on the global economy, with projections that the number of deployed devices will reach 50 billion by the year 2020 and that the total global economic impact may be up to USD10 trillion by 2025 (Gartner, 2018). Figure 2.3 below shows the growth of IoT devices versus traditional human-centric devices.

Figure 2.3: Human Computer Versus IoT Devices (Millions of Units)



Source: Gartner (2018)

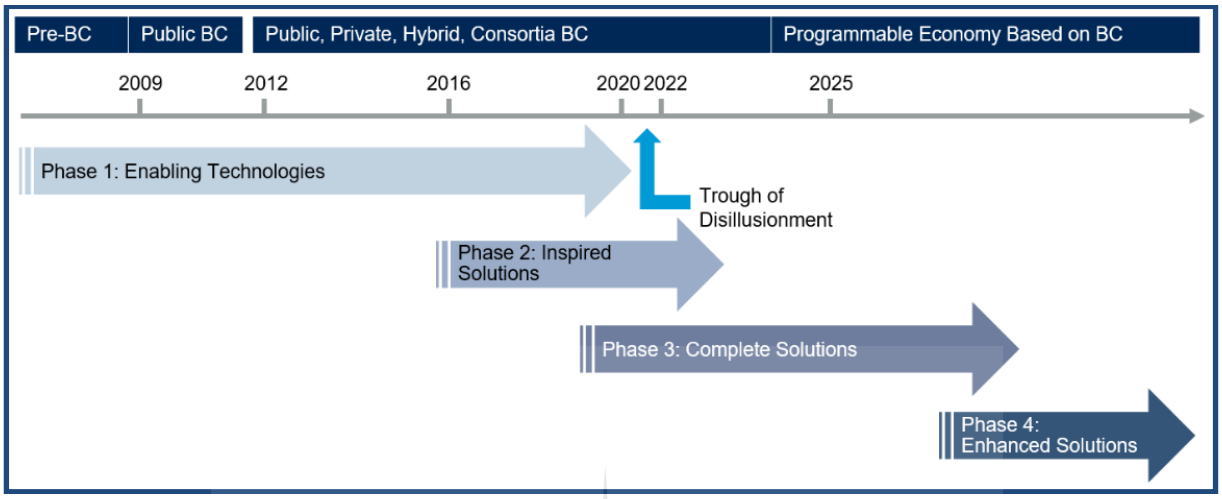
The number of diverse interconnected IoT devices keeps increasing exponentially, introducing new security and privacy challenges (Anthi *& Burnap*, 2018; Chawla & Thamilarasu, 2018). IoT is increasingly becoming a successful technology, corporations which adopted it have experienced a positive outcome on their annual revenue (Nzabahimana, 2018). Although many organisations have cultivated benefits from IoT implementation, it is equally important to consider its challenges with cybersecurity. According to Lyu (2018) it is important to consider that IoT cybersecurity challenges and attacks may outweigh any of its benefits. In their study, Pan and Yang (2018) conclude that creating synergy between the IoT and the emerging blockchain, AR/VR and AI technologies could potentially generate many useful impacts and present a multifaceted information security posture.

2.8.3. Blockchain

According to Liu & Xu, 2018 and Rawat & Alshaikhi, 2018 blockchain is a distributed public ledger technology. This technology is also commonly used as a platform for cryptocurrencies with the most prominent one being Bitcoin. Blockchain technology has redefined how information is stored and disseminated on the information network where neither participant needs to know each other, and nor does it require third-party certification bodies to participate (Liu & Xu, 2018). The growth of blockchain has led to a number of solutions that provides a decentralized personal data management system that enables users to own and control their information (Zyskind & Nathan, 2015). Figure 2.4 below provides a forecast of the growth pattern for blockchain

showing its different phases. The growth envisaged is one that involves a widespread programmable economy with comprehensive solutions for different industries.

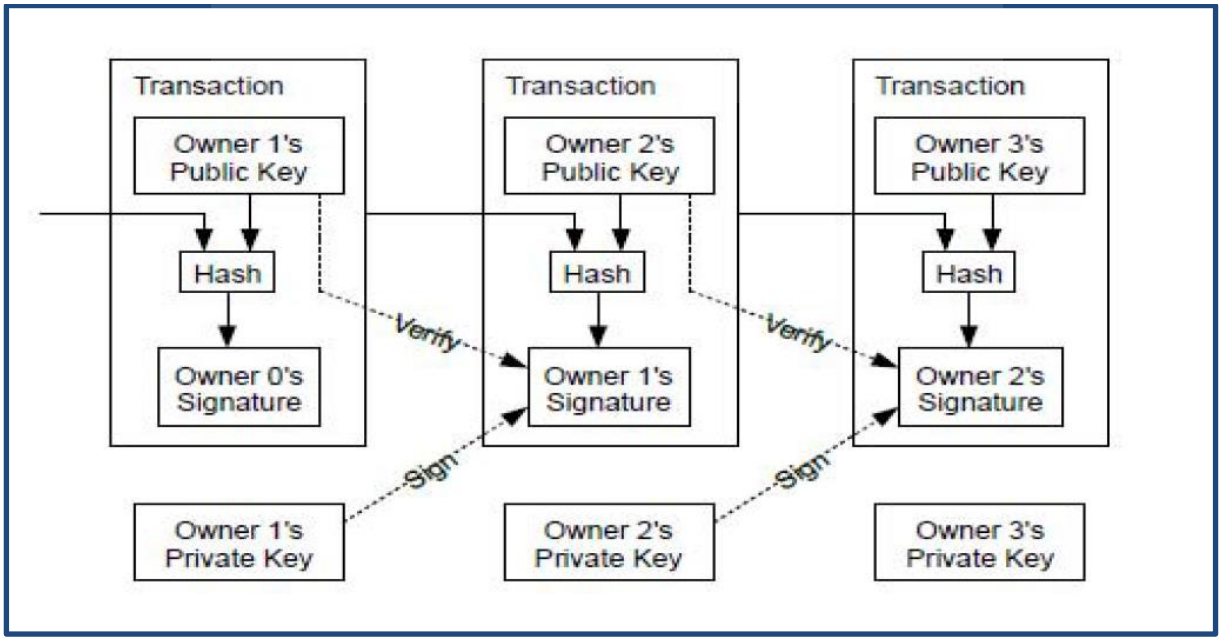
Figure 2.4: Blockchain Spectrum



Source: Gartner (2018)

Blockchain technology is highly secure and its structure makes it almost impossible to maliciously tamper with the recorded transactions (Pan & Yang, 2018). The security posture presented by this technology makes it more desirable to organisations who would like to adopt it. The technical framework for blockchain is outlined in the diagram below.

Figure 2.5: Blockchain Technical Framework



Source: Dai *et al.* (2017) Big Data/ Cloud Computing

Cloud computing and big data continue to be disruptive forces in the technology environment (Eickholt & Shrestha, 2017). Cloud computing has experienced an extremely successful paradigm of service-oriented computing and this has led to a tremendous increase in the scale of the data generated and consumed by applications (Agrawal, 2011). The management of big data has also led to several cloud-based applications and this is indicative of how the two technologies are complementary to one another.

2.8.4. Virtual/Augmented Reality

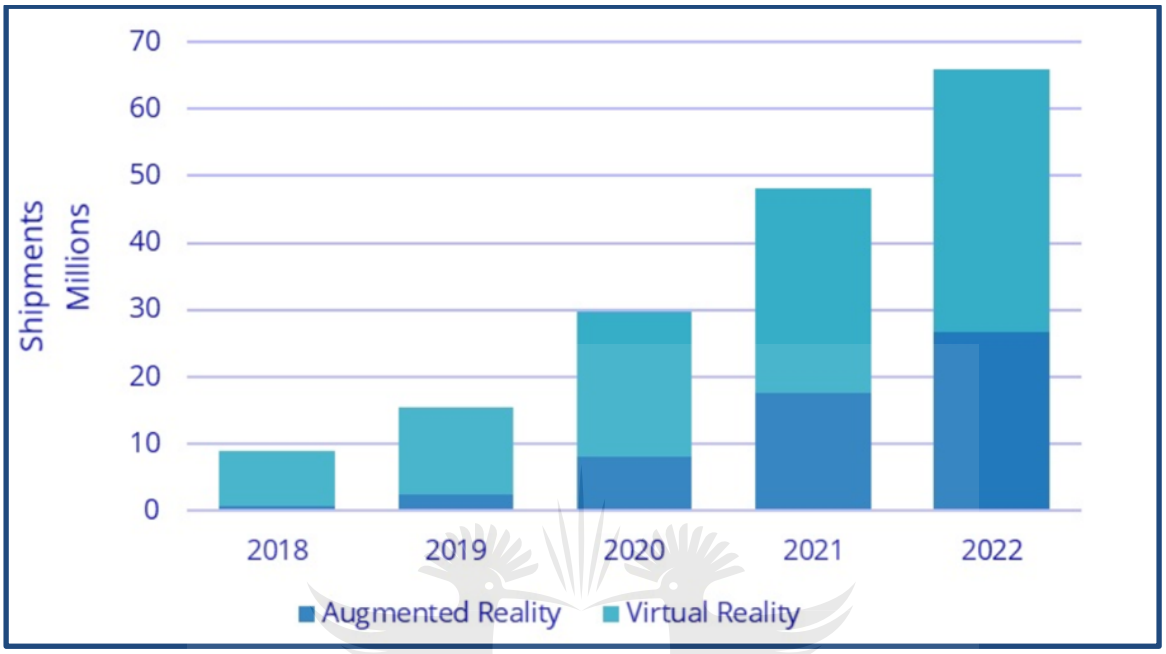
The concept of visual reality was developed in 1999 to supplement the existing broader views on virtual reality and the first research experiments measuring the effectiveness of virtual reality started as early as 1995 (Toumpalidis *at al.*, 2018). According to Wang (2011), virtual reality has four essential factors which are simulation, immersion, feedback and interactive. Security remains a primary concern in the adoption of virtual reality and augmented reality technology as there's often a large amount of data that is cultivated on these technologies. Augmented reality and virtual reality technologies also place a lot of emphasis on reliability, therefore, it is essential for these technologies to present a solid information security posture.

Gulec *et al.* (2018) identify virtual reality as a technology that immerses the users in a virtual environment that is designed to be similar to real life whereas with augmented reality users are presented with a realistic view which is augmented with elements of virtuality. Virtual reality technology provides suitable services for many sectors, according to Hill and Lee (2010) this technology is extensively explored by librarians, gamers, museum curators and educators to develop a simulated immersive exploratory and learning environment.

Virtual reality and augmented reality technologies has experienced significant growth over the years with devices such as Head Mounted Displays (HMD) having attracted interest and investment from major corporations such as Facebook, Sony and Samsung (McGill *et al.*, 2015). It is without a doubt that these technologies will continue to grow. The International Data Corporation (IDC) (2018) forecasts that virtual reality and augmented reality HMDs will grow from 8.1 million units in 2018 to

39.2 million units by the end of 2022. Figure 2.6 below represents the growth forecasts for HMD devices between 2018 and 2022.

Figure 2.6: Worldwide AR/VR Headsets Forecast



Source: IDC (2018)

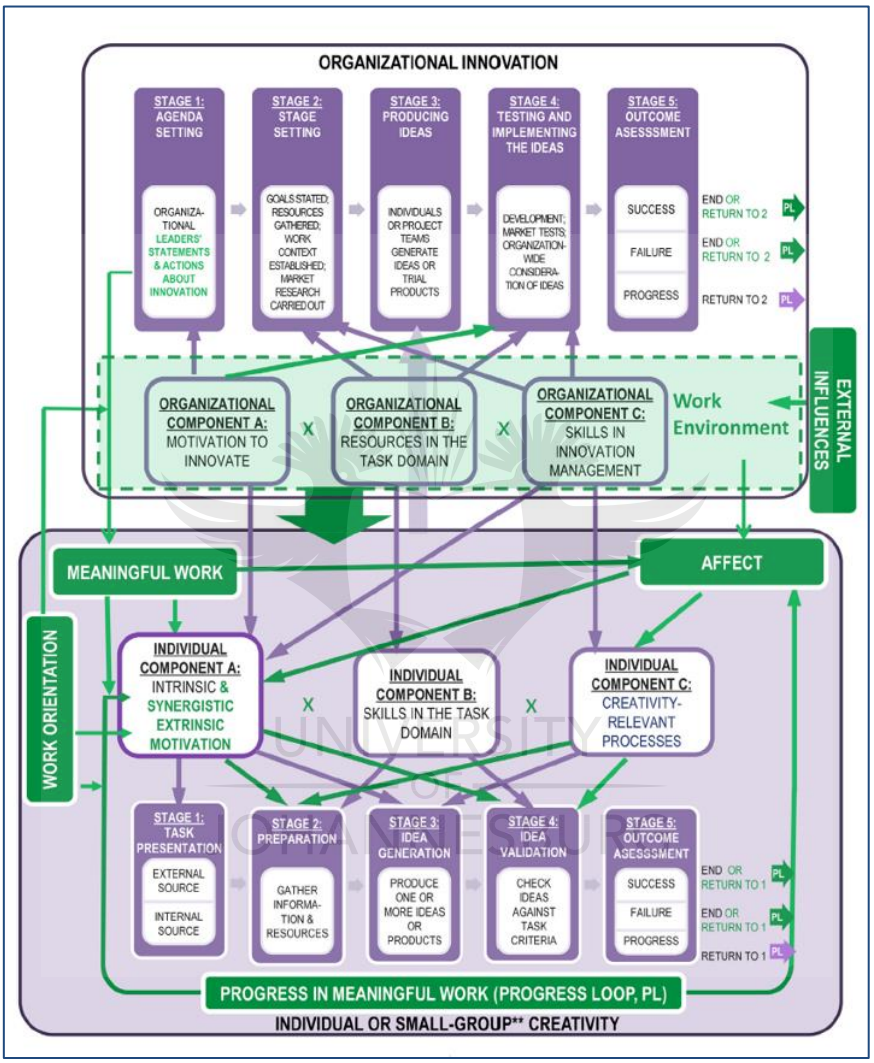
Despite the growth rate of cloud computing adoption and the benefits it brings to businesses, there is also a growing information security concern especially relating to risk areas such as external storage of data, dependency on the public internet connections, lack of control, multi-tenancy and integration with internal security controls (Hashizume *et al.*, 2013). Zissis and Lekkas (2012) identified other information security concerns associated with cloud computing as trust, identification of threats, confidentiality and privacy, integrity as well as availability. As cloud computing is rapidly evolving, the risks and controls addressing it are also subject to continuous change (Bendovschi & Ionescu, 2015).

2.9. Amabile's Theory of Innovation

The concept of innovation has become an important element in organisational research (Chuang, 2007). This has led to the development of various theories that are further used in this research to unpack and understand the concept of innovation from an organisational context. One such theory is the organisational innovation model that derived from Amabile (1988) who developed a model for creativity and innovation in organisations. In this theory, there are four components that are necessary for any

creative response which include domain relevant skills, creativity-relevant processes, intrinsic task motivation, and the social environment in which the individual is working (Amabile, 2011). Figure 2.7 below depicts Amabile's model for organisational creativity and innovation.

Figure 2.7: Model for Organisational Innovation and Creativity



Source: Amabile and Pratt (2016)

This model shows major elements in which innovation and creativity are measured, emphasis is made on the three major elements of innovation which are individual, organisational and environmental elements. According to Chuang (2007), these components mutually complement and interact with one another, and affect organisational innovation. Organisational innovative behaviours include actions such as seeking out new ideas, championing ideas within an organisation as well as

securing funds and planning for the implementation of creative ideas (Carmeli & Spreitzer, 2009).

2.9.1. Individual Components

One of the greatest characteristics of the organisational innovation model is that it places emphasis on individual creativity as it is believed to be the main element that influence organisational and environmental factors of innovation (Chuang, 2007). Individual components of the organisational innovation model include intrinsic motivation to perform the task, skills in the task domain and skills in creative thinking. Apart from being influenced by knowledge, skills, and abilities, innovative behaviour has been found to be largely a motivational issue (Pieterse *et al.,* 2010). This highlights the important role that intrinsic motivation plays in individual innovation and creativity.

The desire to perform better than others can motivate individuals to tap into the full potential of their skills and abilities and this can drive them to participate in innovating and developing ideas (Witt & Robra-Bissantz, 2012). Skills are important as they provide individuals with the fundamental knowledge of how things work. Lynch *et al.* (2010) indicate that the personality trait of openness or open-mindedness is used to refer to an innovative individual and this refers to the cognitive ability of an individual to think creatively and innovate.

2.9.2. Organisational Components

According to Noruzy *et al.* (2013) innovation is more of a collective achievement than an individual act. An organisation is formed by a collective of individuals who share the same goal and interest. Different organisational variables such as policies, resources, and culture can influence organisations (either positively or negatively) in their information security interventions. Organisational components are discussed below in relation to information security risks.

Policies

According to Beris (2016), organisations have recognised that successful information security management involves managing undesirable security behaviour from employees. Such undesirable security behaviour can be managed through the application and enforcement of security policies, guidelines and procedures and ensuring compliance (Bhattacharjee, 2012). Whilst employees are the ones violating

information security policies and are considered as a threat, Njenga (2017) argues that they should be equally and uniquely seen as the solutions to information security risks while also being co-creators of policies. Bulgurcu *et al.* (2010) reiterate that information security is shifting towards individual and organisational perspectives and this has emerged as a key socio-organisational aspect because employees are often the weakest link when it comes to information security.

Resources

The desire for accomplishment, accountability, and contingent awards does not necessarily lead to perceived self-efficacy towards compliance, other factors such as resources must be in place to achieve intended results in information security management (Hu *et al.*, 2012). Information security is also about the protection of the information using resources (van Niekerk & von Solms, 2003). Therefore, the resources at the disposal of the organisation can play a role in the manner in which information security interventions are implemented.

Culture

According to Chang and Lin (2007) organisation culture is the media between management and organisational behaviour, and different companies usually have different organisational cultures. In their study, Stewart and Jürjens (2017) recommended that information security interventions should be delivered in line with organisational culture and best practices. The information security culture within an organisation is also a very significant variable as it shows the extent to which information security behaviour is embedded with organisational values as well as best practices.

2.9.3. Environmental Components

Legislation

Information security has been identified as a critical component contributing towards national security in South Africa (Grobler *et al.*, 2012) and it is for this reason that national legislation is developed to protect the interests of the country and particularly individuals and organisation from becoming victims of incidents relating to information security. According to Kshetri (2013) under-regulation and lack of enforcement have

led to a growth in the informal economy and organised crime, culminating in the growth of cybercrimes. Therefore, changes in legislation may also affect information security interventions in organisations. These developments have led to the enacting of the Protection of Personal Information (PoPI) Act 4 of 2013 and the development of the Cybercrimes and Cybersecurity Bill by the South African Government.

Technology

Changes in information technology are often rapid and compel organisations to make changes to their internal environment in order to adapt. New technologies require new policies, and both require employee training and education (Whitman & Mattord, 2012). Novel technologies may have an effect on information security, for example, with each exposure the user learns more about the technology and so the probability of infection would increase (Myers *et al.*, 2012). It is critical for organisations to keep track of changes not only of technology but also on patterns of data, consumer trends and other infrastructure related to technology.

Competitors

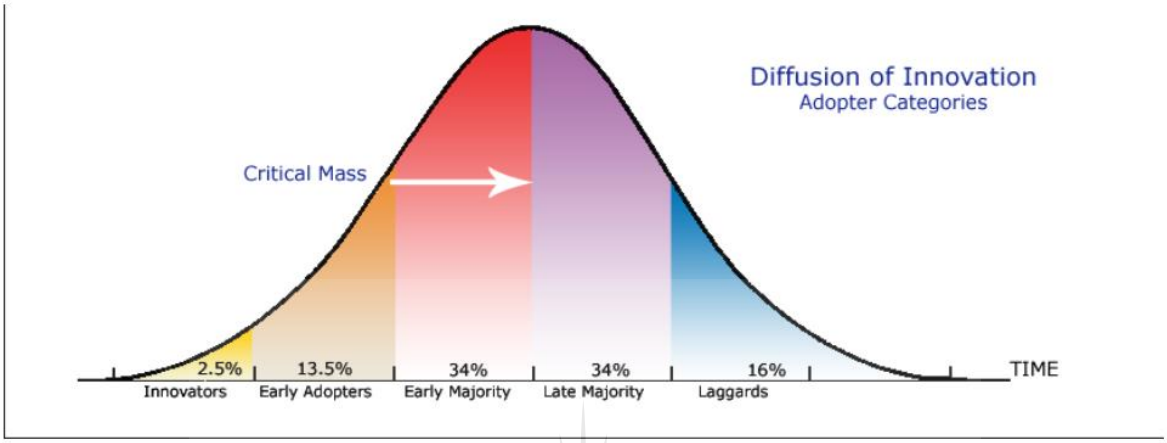
Competitors have a number of ways in which they can influence an organisation's information security interventions. One is by engaging in direct malicious acts to try and gain information about an organisation through various mechanisms such as hacking and espionage. Competitors can also use their competitive advantage to advance their business thereby forcing other organisations to also explore new technologies, processes or business strategies to keep up. Such advances may come with new information security risks and would compel an organisation to act accordingly.

2.10. Diffusion of Innovation

The Diffusion of Innovation (DoI) theory was developed by Everett M. Rogers in the late 1960s and more research is still being developed using this theory (Gouws & van Oudtshoorn, 2011). Rogers's theory is one of the most popular ones for studying the adoption of technology and understanding how innovation is spread amongst the users (Zhang *et al.,* 2015; Al-Jabri & Sohail, 2012). Innovation in information communication technology (ICT) has continuously provided new opportunities, it has transformed people's lives and their adoption to technology (Waheed *et al.*, 2015). The

DoI has different categories for innovation adoption, Gouws and van Oudtshoorn (2011) indicates that these categories move along a continuum of innovation adoption. Figure 2.8 below shows the different categories identified in the DoI.

Figure 2.8: Categories of Diffusion of Innovation



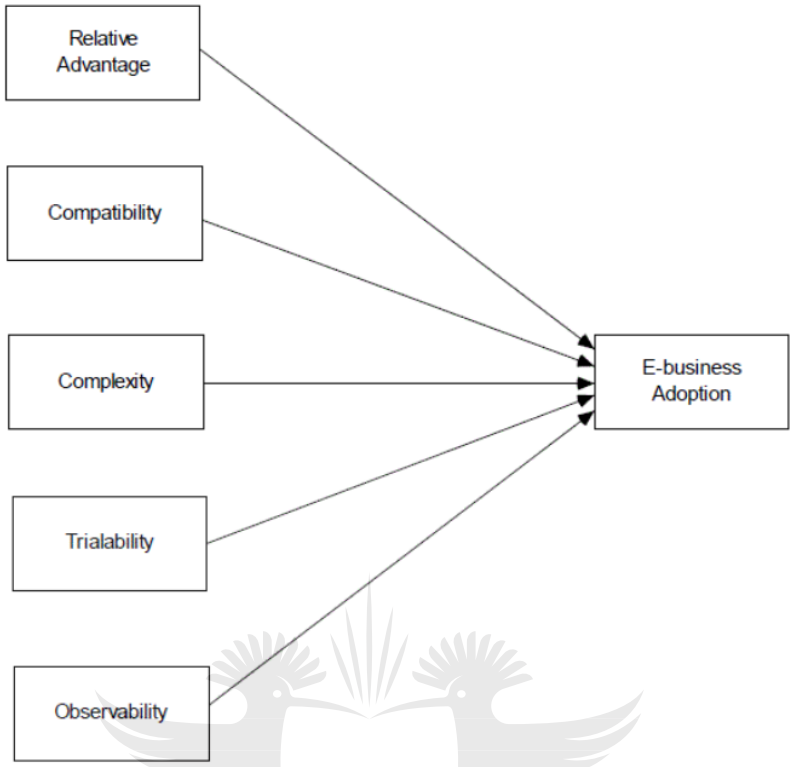
Source: Kaminski (2011)

These categories are mainly used in research that seeks to understand the innovation adoption patterns as they serve as a consequence of the diffusion processes (Al-Jabri & Sohail, 2012). However, in research that seeks to evaluate the relationship between information security risks and systems innovation, the components of DoI provide much more relevant options as variables.

Attributes of DoI

Over and above the categories of DoI, Rogers identified several attributes of innovation that are key in influencing innovation adoption (Al-Jabri & Sohail, 2012). Technological innovation research has provided several variables for studying organisational adoption (Al-khafaji *et al.*, 2014). According to Rogers (1995), these attributes are relative advantage, complexity, compatibility, trialability, and observability. For the purposes of this research, only relative advantage and complexity will be used as variables because the two attributes are widely used in information systems adoption. An example of the DoI attributes on the adoption of e-business is shown in Figure 2.9 below.

Figure 2.9*:* Schematic Diagram of the DoI Attributes



Source: Luqman and Abdullah (2011)

2.10.1. Relative Advantage

According to Zhai (2011), relative advantage is considered as the degree to which an innovation is perceived to be better than other competing innovations. Research has shown that when businesses perceive a relative advantage regarding an innovation, the likelihood of the adoption can increase (Gide & Sandu, 2015). Therefore, the innovation potential of the organisations increases with relative advantage.

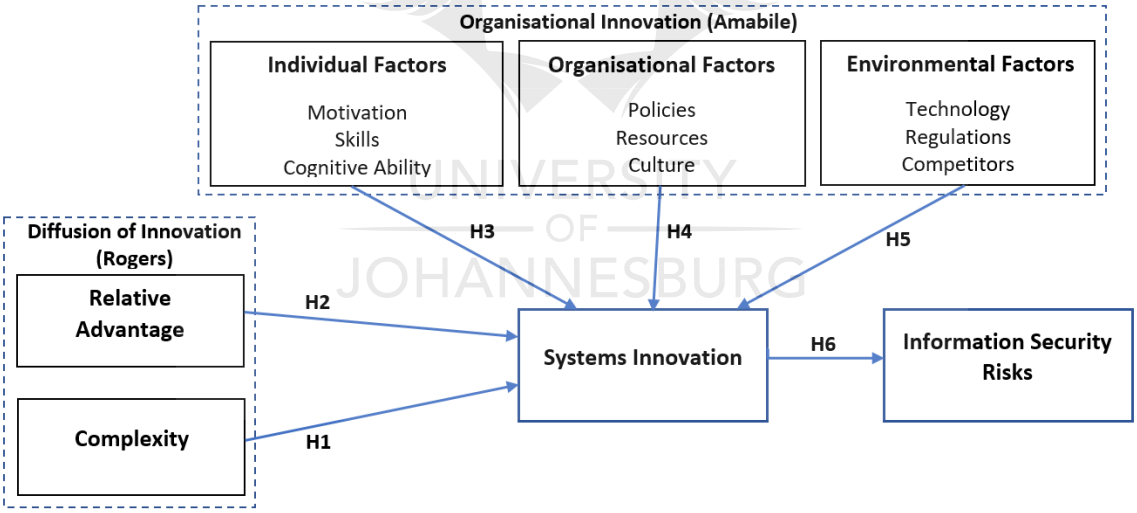
2.10.2. Complexity

Complexity has been defined as the degree of difficulty users experience in understanding or using an innovation (Zhai, 2011). Some researchers have concluded that new technologies must be easy-to-use and accessible for amplifying the proportion of adoption (Ali *et al.*, 2015). Therefore, when a new product, service, process, or system is introduced within an organisation, it is important to ensure that such innovation is not complex especially for the users as this can affect the rate of adoption.

2.11. Research Hypotheses

The model in Figure 10 below provides an illustration of the conceptual framework for this research. The hypotheses described below are outlined in the diagram below with a view to depict the relationship between the variables. This model comprehensively show what variables are being studies and how such variables will be tested against one another. The two innovation theories illustrated in the literature review above are integrated with this framework with a view to ensure that technological and organisational aspects of innovation are represented in the research. These theories also provide important sub-components or attributes which are further used in the research to measure antecedents of innovation. Diffusion of Innovation and Organisational Innovation theories were preferred because of their relevance to the study and also because these are prominent theories in the area of innovation which have been tested by various scholars.

Figure 2.10: Conceptual Research Framework



H1: Complexity of systems influences the rate at which organisations implement system innovation.

H2: There is a relationship between relative advantage and systems innovation.

H3: Individual factors are affected by the rate of systems innovation.

H4: Organisational factors such as policies, resources, and culture influence systems innovation.

H5: The external environment which includes technology, competitors and regulations is affected by systems innovation.

H6: Information security risks are affected by an increase in the organisation's systems innovation.

2.12. Chapter Summary

This chapter provides a theoretical background of the study whilst also unpacking theoretical underpinnings related to the variables being studied in this research. The technologies being studied in this research are further outlined in this chapter together with theories surrounding information security and systems innovation. The literature review looks at these technologies from an adoption point of view and highlights research that has been done in such areas. The two theories used in this research are also outlined in detail to substantiate why the theories are relevant for this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

This chapter outlines the research strategy and methodology which is an important section indicating how the research will be carried out. The research paradigm discussed below provides a philosophical stance for the research while the research methods indicate which research methods will be used for the research. Other key concepts discussed in this chapter include population and sampling, data collection, data analysis as well as ethical considerations for this research.

3.2. Research Paradigm

The selection of a methodology is largely dependent on the research paradigm which informs the research approach, particularly, ideas about the nature of reality and humanity (ontology), the theory of knowledge that informs the research (epistemology) and the method used to gain knowledge (methodology) (Tuli, 2010). This research follows an ontological assumption of objectivism as it is based on principles of objective reality and independence with an epistemological assumption of objectivism. Interpretivism would not be suitable for this study because a quantitative methodology is used. According to Goldkuhl (2012) interpretivism is a dominant research paradigm for qualitative studies. The positivist ontological assumption is therefore ideal for this study because it is objective as opposed to interpretivism which is considered to be highly subjective.

As the literature review above suggests, there is significant knowledge that has been tested through various methods and vetted to be valid in the field of information security risk as well as innovation. Therefore, the epistemological approach to this research is that existing innovation theories will be used to better understand how systems innovation affect information security risks. This study involves the use of two theories to develop the conceptual framework which are the Diffusion of Innovation by Rogers (1995) and Organisational Innovation by Amabile (1988). A deductive approach to theory development is therefore taken as it deemed relevant when using existing theories to explain relationships between various phenomena.

The research philosophy behind this study is positivism which according to Saunders *et al*. (2012), relates to a philosophical stance of the natural scientist and entails working with an observable social reality to produce generalisations.

3.3. Research Strategy

The study follows a methodological choice of mono-method quantitative. According to Rusli and Ali (2003), quantitative research is commonly understood as research that extensively uses descriptions, concepts and theories to examine the nature of and relationship between variables. A survey questionnaire was used to collect data which sought to measure constructs relating to antecedents of system innovation, systems innovation, and information security risks. In quantitative research, several hypotheses are developed and statistical analysis is used to explain several complex and causal relationships between variables (Desai, 2016). As the objective of this research is to measure correlation, the measurement and analysis of causal relationships between variables becomes very crucial as it assists in understanding how the constructs relate with one another. Therefore, this research places a lot of emphasis on measuring and analysing causal relationships between different constructs.

It is important to note that this research strategy has limitations in that it has limited outcomes due to the closed type of questions used and the researcher is also unable to control the environment where respondents provide answers to questions (Matveev, 2002). The advantages of using the selected research strategy are that the objectives of the research are clearly stated, the research is based on existing theories and the subjectivity of the research is somewhat eliminated as the research assumes the ontological assumption of objectivism and independence.

According to Stewart and Subramaniam (2010), objectivism ensures that unbiased assessments, judgments, and decisions are made and as this research assumes an ontological position of objectivism it therefore assures independence as the researcher assumes an objective and independent stance in the study. A deductive research approach draws from existing theory, in following this approach the researcher develops hypotheses, tests, observes and validates them (Saunders *et al*., 2012).

3.4. Population and Sampling

The research sample was made up of employees and students from various organisations/institutions who interact and use information systems on a regular basis. Students who were sampled to participate on this research are all part-time students who are also employed. This was done to ensure that students are also able to effectively respond to questions relating to their employment status and work experience. To gain a representative sample of the typical business demographic of South Africa, the respondents were selected proportionally from different areas of business including both public and private sector, small businesses, medium to large businesses, multinational companies as well as IT students from various institutions of higher learning. Therefore, the target population for this research includes IT practitioners working in various organisational sectors as well as IT students. People based in the informal sector were excluded from the sample.

Questionnaires usually have a disadvantage of having a poor response rate and the responses can be biased based on the respondent's level of understanding (Leedy & Ormrod, 2005). It is for these reasons that stringent sampling is applied in this research. The sampling criteria used in this research was judgemental sampling, which according to Sharma (2017), relies on considerations of the researcher whereby a selection is made based on the researcher's knowledge of the population being studied. Therefore, this research targeted respondents who use information systems on a regular basis and are aware of information security considerations. The targeted respondents would typically include people who work in IT departments particularly those that have extensive knowledge of the variables being studied.

A snowballing sampling method was used to develop a sample of 185 respondents. Snowballing, which is also referred to as chain-referral, is a selection method where the "seed" individuals are identified to start the survey and then asking them for additional contacts in the population of interest (Yarwood, 2011). In this study, 93 seed respondents were selected through a purposeful sampling method and they provided the initial responses and subsequently shared the survey questionnaire with other individuals that fall under the target group. For the purposes of this study, the population is defined as IT Practitioners and students in South Africa.

As Kalof *et al.* (2007) indicate, a pilot test must be performed prior to the questionnaire being distributed to the sample. A pilot test was performed on a smaller sample to test the appropriateness of questions to the target respondents, the validity of the questions and to identify mistakes in the questionnaire. As a result, a few errors were identified and corrected prior to sending out a final survey to the respondents. A pilot survey proved to be an important tool to minimise errors on a survey and also to determine the amount of time respondents would take to complete the survey. This process also assists the researcher to gain insights on the type of data that will be provided during data collection.

3.5. Data Collection

Data collection was done by way of self-administered survey questionnaires which comprised of questions relating to the hypotheses examined in this study. Online and manual survey questionnaires were developed and distributed to the relevant respondents as identified in 3.3. above. Data was collected over a period of one month and 185 responses were received. 144 of those responses were completed using the online questionnaire and 41 were completed manually. The online survey questionnaires were distributed to the target respondents through e-mail, WhatsApp messenger and Facebook messenger. A “drop and collect” method was used to distribute the manual survey questionnaires.

Although manual surveys ensured data collection within the Gauteng Province, the online questionnaire assisted significantly in reaching a wide spectrum of respondents from different geographical locations within South Africa. A cross-sectional data collection method was followed because the research intended to compare the respondents’ perception and experience of systems innovation and information security risks at a point in time. Data collection was conducted from 05 September 2018 to 05 October 2018, therefore, the data collected represents the respondents’ perception and experience during that particular period.

3.6. Survey Questionnaire

A survey questionnaire, which was developed by the researcher, was used to collect data from respondents regarding their experience and perception of systems innovation antecedents and information security risks. A cover letter was distributed

together with the survey questionnaire which provided a brief overview of the research, explained ethical considerations i.e. informed consent and provided contact details of the researcher. The survey questionnaire comprised of eight sections. Section A comprised of five questions that sought to obtain demographic details of the respondent and that included details relating to job title, level of employment, work experience, level of education and the sector in which the respondent's organisation operates. Section B to H comprised of 35 questions that sought to obtain information from respondents that is specific to the constructs being studied i.e. relative advantage, complexity, individual factors, organisational factors, environmental factors, information security risks and systems innovation.

Section B to H of the survey questionnaire mainly contained statements that are aimed at measuring the perception and experience of respondents regarding the various constructs. The survey questionnaire was used in this research to obtain ordinal data from respondents. Therefore, respondents were given a scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, to indicate the extent to which they agree or disagree with the statements. Only one out of 35 questions had a different scale where 1 = Not at All, 2 = Small Extent, 3 = Some Extent, 4 = Large Extent and 5 = Very Great Extent. This question aimed to measure the extent to which various technologies were adopted by the respondent's organisation.

Each section of the survey questionnaire, except for Section A, has a construct which is linked to each of the hypotheses of this study. Each section had a total of five questions which were all aimed to obtain information regarding that particular construct.

The manual survey questionnaires that were not fully completed were disregarded and online surveys were set such that it does not record or save incomplete responses. Online surveys were configured to exclude any incomplete surveys. This means that in all 185 survey questionnaires completed all questions were responded to. A sample of the survey questionnaire is attached as Annexure A.

3.7. Data Analysis

The manually collected data was captured and incorporated with the data collected through the online survey questionnaire to develop a single data sample which

included all responses. The data was automatically extracted into an excel spreadsheet then loaded onto the IBM SPSS software for further analysis. Google Forms was used for descriptive data analysis and IBM SPSS software provided a more comprehensive analysis which includes factor analysis, regression analysis, correlation analysis, reliability testing and cross-tabulation.

Demographic data collected through Section A of the survey questionnaire was analysed through descriptive statistics and cross-tabulation was also performed to compare various groups of data. Data collected through Section B of the survey questionnaire was collected and analysed through various statistical methods which includes factor analysis, correlation analysis and regression analysis. Reliability tests were also performed on all data sets in order to test the reliability and sampling adequacy of the data. The key findings of this research are based on the analysis from the regression testing.

3.8. Ethical Considerations

Diener and Crandall (1978) identified four main areas of ethics that are of great importance when conducting research which include harm to a participant, informed consent, privacy and confidentiality as well as deception. These areas will be used to unpack research ethics for this study. Ethical issues arise at different stages in business research (Bryman & Bell, 2011) and it is for this reason that ethical considerations were clearly outlined and explored before conducting this research.

The respondents were not incentivised, deceived, nor coerced to take part in this research and issues of consent, confidentiality and anonymity were also given consideration throughout this study. According to Chang *et al.* (2010), respondents must be given assurance that their anonymity and confidentiality will be protected and be given an opportunity to withdraw their consent at any stage of the research. The cover letter attached to the survey questionnaire served to provide assurance to respondents that their information will be kept with the highest degree of confidentiality and anonymity. To this end, Section A of the questionnaire allows respondents to give consent prior to participating in the study.

Demographic data collected on the respondents did not seek any personally identifiable information thus ensuring the protection of the respondents' confidentiality. Privacy of information is also protected as the manually collected data is stored in a locked cabinet in a locked office and the data contained in the online surveys is securely stored in a password protected device.

The research sample was limited to IT practitioners in different organisations and IT students at institutions of higher learning. The selection of this sample ensured that the research does not use minors or mentally disabled persons at any stage of the study. At no stage of this research was there a participant harmed or any who suffered adverse consequences as a result of participating in this research. Information received from respondents is kept private and confidential and shall not be shared with any third parties. The research has also been endorsed by the University of Johannesburg's Ethics Committee.

3.9. Chapter Summary

Chapter 3 outlines the research strategy as well as the philosophical stance that the research will be taking. The chapter further outlines the sampling and data collection techniques used and also explains how the data was analysed. The data collection instrument used and the method of collection are highlighted. This chapter also explains ethical considerations relating to this study.

CHAPTER 4: DATA ANALYSIS

4.1. Introduction

Data analysis is an important part of this research as it ensures that the data collected is interpreted and given meaning. It is through data analysis that one is able to make assumptions and findings. In this research, the relationship between systems innovation, its antecedents as well as information security risk will be tested through various statistical methods.

Descriptive statistics are used to provide an analysis of demographic data and this provides valuable insight as it helps to better understand the calibre of people who provided the data. Descriptive statistics is also used to analyse the various constructs of this study and this provides a general understanding of how respondents responded. Cross-tabulation is also used to compare data between various constructs, this further allows for better interpretation of the demographic data.

Validity and sampling adequacy are tested to evaluate the credibility of the sample and the data collected. Factor analysis is also performed and the results are presented to reflect variance and rotated component matrix. Lastly, regression and correlation tests are performed to examine the relationship between constructs. Both linear and multiple regression tests were performed to test the hypothesis of this study.

4.2. Descriptive Statistics

Data collected through the survey questionnaires was compared and analysed through descriptive statistics. The sections below present an analysis of the demographic information of the respondents. Cross-tabulation is also used to compare the various datasets with a view of identifying patterns and relationships. This section also presents descriptive statistics for DoI attributes as well as factors of organisational innovation.

4.2.1. Demographic Details

Section A of the questionnaire sought demographic details of the respondents, most of the data collected pertains to the respondent's occupational details as well as data relating to their work experience and academic qualification. Demographic data allows for better comprehension of the respondents and their credibility, especially pertaining to the data provided. As the study seeks to understand the relationship between

system innovation and information security risk, it is important that one ensures that data is provided by respondents who are sufficiently qualified and experienced on the subject. The demographic details of the respondents are outlined below.

Level of Employment

The level of employment pertains to the rank at which the respondent is in his or her career or the level at which he or she is employed. Data collected shows that 34.1% of the respondents were employed at a technical/functional level and this is the category of employees who have a daily engagement with technology and information systems. It is also important to note that functional and technical employees in most cases are expected to have some level of understanding of information security. The second largest group of respondents came from Middle Management with 27% which is typically the group that plays a managerial role in making sure that new systems are implemented and information security arrangements are put in place.

There were also somewhat equal responses received from Interns and Top Management which recorded 10.8% and 11.9% responses respectively. The least number of responses were recorded from Admin (8.6%) and Other (7.6%). The "other" category mainly comprised of people belonging between the Middle Management and Top Management as most of them included Specialists and Senior Managers. Table 4.3 below provides a summary of all the respondent's level of employment.

Table 4.1: Level of Employment Responses

Level of Employment	Percentage
Intern	10.8
Admin	8.6
Technical/Functional Level	34.1
Middle Management	27
Top Management	11.9
Other	7.6

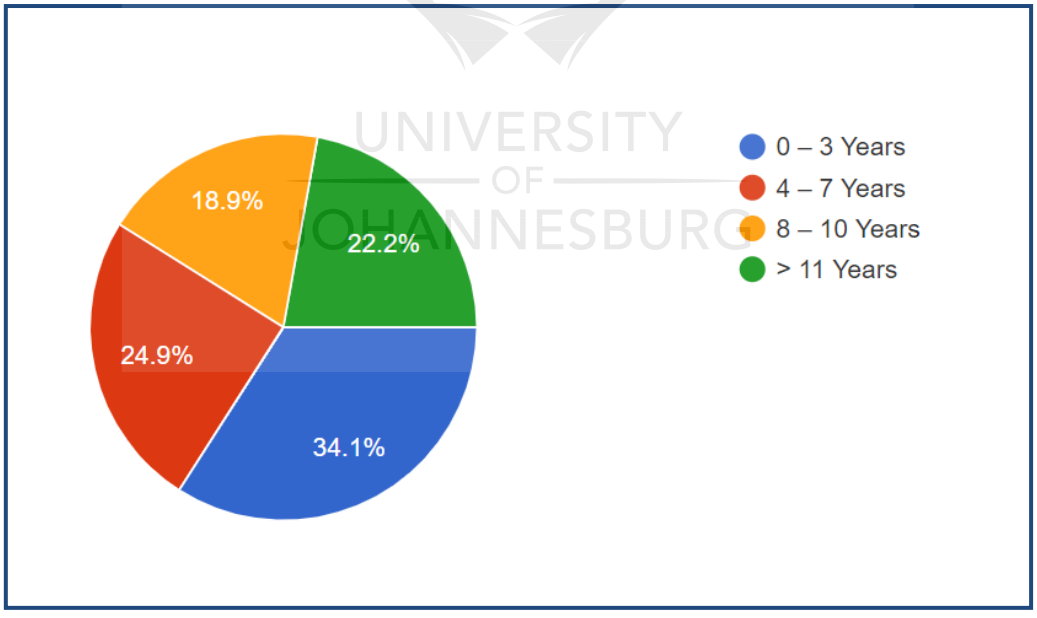
Due to the nature of this study, it is important to understand the occupational and operational level of the respondents providing the data. The study relies heavily on the perception and personal experiences of the respondents, therefore, it is important to

have the data coming from various levels of organisations. Having Technical/Functional and Middle Management respondents being the biggest group also shows that the data provided comes from people who have daily and personal interactions with the variables being studied.

Work Experience

One of the most important elements in determining a person's competency and capability on a certain subject is through their work experience. The questionnaire assessed the respondents' work experience, particularly in working with information systems. The majority of the respondents (34.1%) had 0-3 years' experience which was the least experienced group whereas the most experienced group of respondents, who had more than 11 years' experience, was 22.2%. The 4 – 8 years and 8 – 10 years' groups recorded 24.9% and 18.9% respectively. This again shows that each of the categories was sufficiently represented. Figure 4.1 below represents a summary of all the responses received.

Figure 4.1: Work Experience Responses



In his study, Parsons (2015) found that age is positively related to an employee's ability to innovate, meaning that young people who often have less experience are less likely to innovate. This brings in an element of experience and shows its significance in the study of innovation. Therefore, one can consider the 0 – 3 years category less experienced employees who make up 34.1% of the respondents followed by 4 -7 years

who are slightly more experienced. The highly-experienced respondents made up 22.2% and 18.9% of the responses showing a marginal representation. It is also important to have each of the categories represented to eliminate biases that would come as a result of the level of the respondents' experience.

Level of Education

The level of education also provides details of how knowledgeable the respondents are based on their formal education. Respondents with Bachelors or B-Tech degrees form the majority of the respondents at 29.2% followed by those with a National Diploma at 27% and those with Honours degrees (23.2%). A small number of respondents had Matric and Doctoral Degrees. Respondents who selected other are those who have various certificates in IT, some of which might not have a matric qualification. The responses are summarised in Table 4.4 below.

Table 4.2: Level of Employment Responses

Level of Employment	Percentage
Matric/Grade 12	6.5
National Diploma	27
Bachelors or B-Tech	29.2
Honours	23.2
Masters	12.4
Doctoral	0.5
Other	1.2

Organisational Sector

There has been a substantial growth in the interest of innovation over the past years (Borins, 2001) this has led to a number of technological solutions that seek to modernise and transform both the public and private sector. The private sector has for many years been perceived as a leader in innovation, however according to Borins (2001), government and business are working together in many countries to encourage innovation activity. In this study, information was collected to reflect the sector in which the respondents are working. The two sectors have significant representation with the public sector leading with 54.6% followed by the private sector

38.9%. Respondents from Parastatals and Non-Profit Organisations (NPOs) received a marginal representation at 4.3% and 2.2% respectively.

Figure 4.2: Organisational Sector Responses

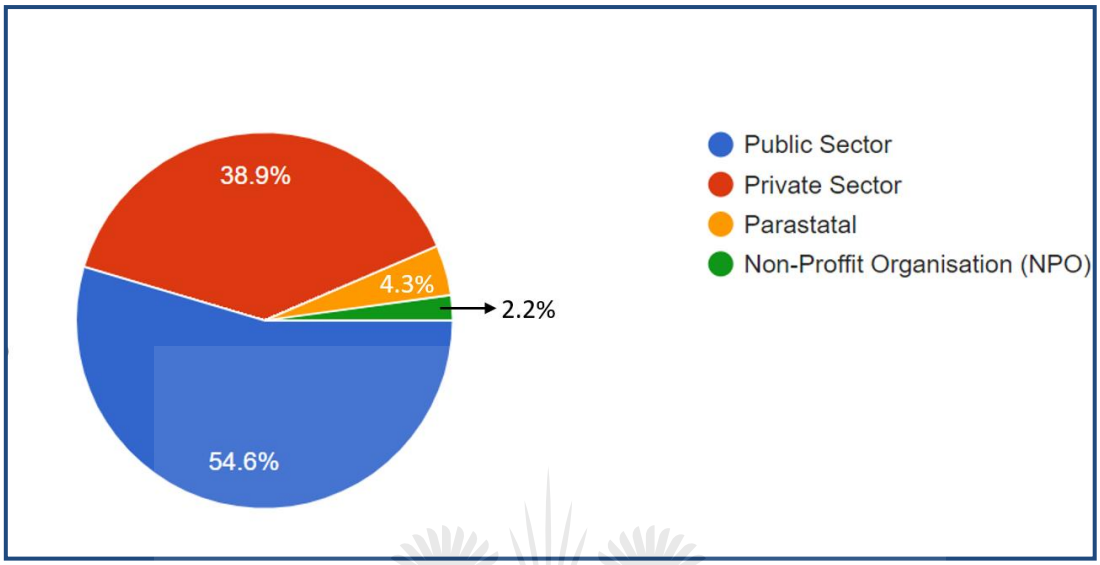


Figure 4.2 gives an indication that with all the sectors represented it is possible to generalise the findings to organisations belonging in all sectors of business. This information is also important as it indicates that systems innovation and information security risks exists in all sectors of business, therefore, this research provides an opportunity for organisations in all sectors to examine how the two variables influence and relates to one another.

Cross-Tabulation

The level of education of the respondents, when compared with their experience, indicate that respondents with 0 to 3 years of experience predominantly hold National Diplomas. Respondents with 4 to 7 years' experience predominantly hold a Bachelors or B-Tech degrees. The totals also show that respondents who hold Bachelors or B-Tech and those who have National Diplomas makes up the majority of the responses in these categories. Therefore, based on the information presented in the cross tabulation in Table 4.5, the majority of respondents at least had a National Diploma or Bachelors' Degree with an average of 0 to 3 years' experience.

Table 4.3: Level of Education and Experience

		What is your Level of Education?							
		Matric/ Grade 12	National Diploma	Bachelors or B-Tech	Honours	Masters	Doctoral	Other	Total
How long have you been working in IT?	0 to 3 Years	6	25	17	12	3	0	0	63
	4 to 7 Years	1	9	13	16	5	0	2	46
	8 to 10 Years	1	9	9	9	7	0	0	35
	More than 11 Years	4	7	14	6	9	1	0	41
Total		12	50	53	43	24	1	2	185

When comparing the respondents' level of experience with the sector in which they work, the data shows that most of the respondents are from the public sector with an average of 0 to 3 years' experience. The private sector produced most of the respondents with 4 to 7 years' experience, it also produced the second largest number of respondents in the survey. The Parastatals and NPOs produced the least of respondents with most of them belonging to the 0 to 3 years and 2 to 7 years' categories respectively. The cross-tabulation on experience and sector, not only provides information about the level of education the respondents have but it also indicates which sectors the respondents are predominantly come from. This is important as it ascertains that data is collected from respondents who are knowledgeable and represent different business sectors.

Table 4.4: Work Experience and Sector

		In which sector is your organisation?				
		Public Sector	Private Sector	Parastatal	Non-Profit Organisation (NPO)	Total
How long have you been working in IT?	0 to 3 Years	43	16	1	3	63
	4 to 7 Years	16	26	3	1	46
	8 to 10 Years	22	11	2	0	35
	More than 11 Years	20	18	2	1	41
Total		101	71	8	5	185

The level of education and occupational level are typically used to determine the knowledge that one possess. This provides an indication that the respondents are specialists and subject matter experts based on their education and level of responsibility within an organisation. The two measures were cross tabulated and the results show that the respondents with Bachelors or B-Tech degrees who are at a Technical/Functional level make up the majority of the respondents. People at a Technical/Functional level in the organisation are the ones who work with information systems on a day-to-day basis, which means that they have a practical knowledge of technology, information systems and information security. These groups of respondents also seem to have a solid academic knowledge of technology and information systems as they also possess Bachelors or B-Tech degrees.

Table 4.5: Level of Education and Level of Employment

		What is your Level of Education?							
		Matric/ Grade 12	National Diploma	Bachelors or B-Tech	Honours	Masters	Doctoral	Other	Total
What is your Level of Employment?	Intern	0	16	3	1	0	0	0	20
	Admin	3	4	5	5	0	0	0	17
	Technical/ Functional Level	4	15	24	15	3	0	1	62
	Middle Management	1	13	11	14	9	0	1	49
	Top Management	2	1	5	3	11	1	0	23
	Other	2	1	5	5	1	0	0	14
Total		12	50	53	43	24	1	2	185

4.2.2. Descriptive Statistics for DoI

This section sought to measure the respondent's perception and experience regarding the two attributes of DoI and their relationship with systems innovation. The results for complexity and relative advantage are discussed below.

Complexity

Complexity in the context of systems innovation involves the level of difficulty users experience when using the system or their inability to understand how the system works. The three items used to measure complexity include user-friendliness,

simplicity, and the error-free nature of the systems. On user-friendliness, most respondents agree that the user-friendliness of a system makes it easier for it to be adopted. 34.6% of the respondents agreed while 56.8% of them strongly agreed with this statement. 30.8% of the respondents agreed that they are likely to adopt a system that simplifies their work while 64.3% of them strongly agreed. Most respondents also seem to agree (51.9%) that it is easier to adopt a system that does not give frequent errors, 39.5% of them strongly agree with this notion.

This data shows that most respondents seem to be in agreement. It is therefore valid to deduce that most of the respondents indicate that the less complex the system, the easier the adoption and subsequently used as an element of innovation. Table 4.8 below provides a summary of the responses in relation to complexity.

Table 4.6: Complexity Responses

	Strongly Disagree	**Disagree**	**Neither Agree nor Disagree**	**Agree**	**Strongly Agree**	**Mean**	**Standard Deviation**
C1	3.2%	1.6%	3.8%	34.6%	56.8%	4.40	.898
C2	3.2%	1.6%	0%	30.8%	64.3%	4.51	.860
C4	2.7%	1.1%	4.9%	51.9%	39.5%	4.24	.821

Relative Advantage

Relative advantage measures the degree of how much a new system is better than an existing or old one. The items used to measure this construct include functionality, productivity, speed, the look and feel, and relevance to one's work. Less than 10% of the respondents either strongly disagreed or simply disagreed that their decision to adopt a new system is to some extent influenced by whether the new system is better than old ones. Table 4.9 below provides a summary of the responses on relative advantage.

Table 4.7: Relative Advantage Responses

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
RA1	3.2%	1.1%	5.4%	34.1%	56.2%	4.38	.895
RA2	1.6%	6.5%	14.6%	40.5%	36.8%	4.03	.969
RA3	2.2%	3.8%	25.4%	43.8%	24.9%	3.83	.932
RA4	3.2%	9.7%	31.4%	36.8%	18.9%	3.57	1.015
RA5	2.7%	6.5%	8.6%	35.1%	47%	4.15	1.042

4.2.3. Description Statistics for Organisational Innovation

Organisational innovation has three constructs that seek to examine the extent to which organisational factors relate to system innovation. These constructs examine system innovation from an individual, organisational and environmental point of view. The data collected on the three contracts is outlined and discussed below.

Individual Factors

Four items including motivation, technical skills, creativity, and cognitive ability were used to measure this construct. 32.4% of respondents strongly disagree that they lack the motivation to use new systems followed by 47.6% of respondents who disagree. Similarly, when coming to lacking technical skills for using new systems 35.7% of respondents strongly disagree and 45.9% disagree. The items that were using creativity and cognitive ability to measure the individual factor construct and its relationship with systems innovation received responses on strongly disagree and disagree options. For creativity, 37.3% responded with strongly disagree and 42.2% responded with disagree. The results for the cognitive ability item were 32.4% and 44.3% for strongly disagree and disagree respectively. On average, 10.4% of the respondents neither agreed nor disagreed with statements. A summary of the responses for the individual factors is provided for below in Table 4.10.

Table 4.8: Individual Factors Responses

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
IF1	32.4%	47.6%	8.6%	9.2%	2.2%	2.02	.986
IF2	35.7%	45.9%	9.2%	5.4%	3.8%	1.96	1.004
IF3	32.4%	44.3%	14.1%	7%	2.2%	2.03	.969
IF5	37.3%	42.2%	9.7%	7.6%	3.2%	1.97	1.034

The results for the agree and strongly agree options seem to be significantly lower in all the options, 2.85% on average. This indicates that most respondents believe their individual characteristics such as motivation, technical skills, cognitive ability and creativity allows them to adopt new systems and play an active role in the organisation's efforts towards systems innovation.

Organisational Factors

Organisational factors play an important role in determining the success or failure of any innovative venture. This is why it is an important construct in assisting with the examination of organisational factors that play a role or influence systems innovation. This construct was measured by three items namely the organisation's financial investments towards new systems, organisational culture, and organisational politics.

The majority of respondents (37.8%) disagree with the statement that their organisation does not invest enough in new systems. 43.2% of the respondents also disagree that their current organisational culture does not support systems innovation while 27% of respondents strongly disagreed. On organisational dynamics and politics, most respondents agree that systems innovation is negatively affected by politics and organisational dynamics. The first two items, OF2 and OF3, point towards the notion that organisational factors such as culture and financial investments are not barriers to systems innovation. However, respondents seem to think organisational dynamics and politics have a negative effect on systems innovation. Organisational factors results are summarised in Table 4.11 below.

Table 4.9: Organisational Factors Responses

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
OF2	18.9%	37.8%	18.9%	15.7%	8.6%	2.58	1.213
OF3	27%	43.2%	12.4%	9.2%	8.1%	2.30	1.195
OF4	7.6%	17.8%	27.6%	34.6%	12.4%	3.28	1.112

Environmental Factors

Part of the objectives of this research was to determine how systems innovation is influenced by factors external to the organisation. These factors often force organisations to adopt new systems and innovate. The items used to measure this construct include changes in government regulations, pressure from competitors and customers, enhancing operational competitiveness, and compliance with government compliance.

Most respondents agree with most of the items showing that indeed external factors have played a role in ensuring that the organisation adopts new systems and innovates. Although some respondents disagree on one or more items, the overwhelming majority agree with most options. It is also worth noting that this construct received a high number of respondents who neither agree nor disagree, 23.52% on average, this could be because respondents are afraid to divulge details about their organisation or they are not informed about the items being measured in relation to their organisation. Table 4.12 below summarises the responses for environmental factors and its specific items.

Table 4.10: Environmental Factors Table

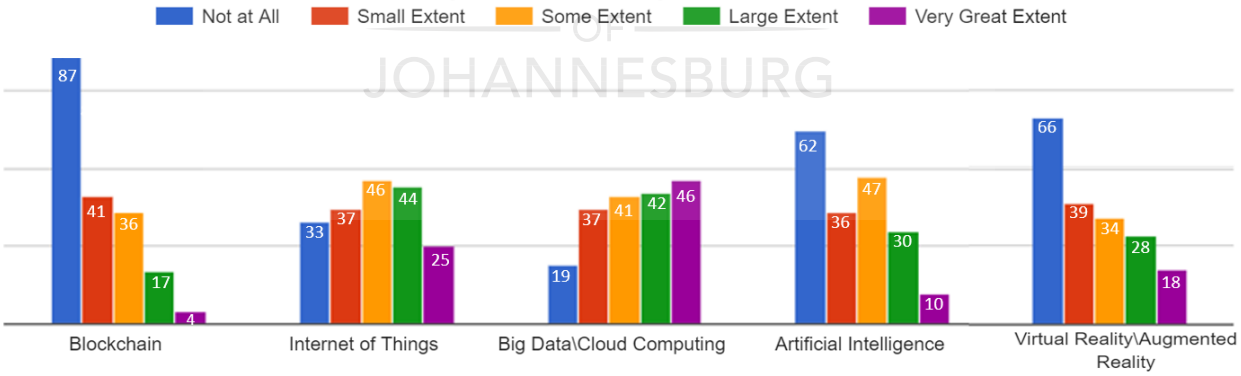
	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
EF2	2.2%	17.3%	25.9%	44.9%	9.7%	3.42	.953
EF3	4.3%	20%	29.2%	32.4%	14.1%	3.30	1.091
EF4	2.7%	7.6%	16.8%	48.6%	24.3%	3.84	.964
EF5	2.7%	8.1%	22.2%	50.3%	16.8%	3.69	.931

4.2.4. Systems Innovation

Systems innovation is one of the key independent variables being used to examine information security risks in this study. The five constructs discussed above in 4.2.2 and 4.2.3 respectively represents antecedents of systems innovation. Systems Innovation is examined in the context of the adoption of new systems in the form or blockchain, IoT, big data/cloud computing, artificial intelligence and virtual/augmented reality.

Respondents were asked *"To what extent have your organisation adopted the following technologies"* and options provided were Not at All, Small Extent, Some Extent, Large Extent and Very Great Extent. These options provided for the five systems/technologies that are covered under the spectrum of system innovation. The objective of this item was to determine the level of innovation organisations have done in terms of the five identified technologies/systems. This would ensure that a determination is made on whether these technologies/systems introduce or increase information security risks.

Figure 4.3: Systems Innovation Responses



Data collected shows that respondents noted that most organisations have not adopted blockchain, artificial intelligence and virtual/augmented reality. Most of the respondents selected "Not at All" for these technologies. However, a substantial number of respondents shows a somewhat high adoption of IoT and big data/cloud computing with the leading technology being cloud computing. 46 respondents chose "Very Great Extent" for big data/cloud computing which shows that it is a leading technology as far as systems innovation is concerned. It is also important to note that

even on items where most respondents indicate a low adoption there is some level of adoption by other respondents or organisations.

Other items that were used to measure systems innovation are problem-solving, increased efficiency, digital transformation, and meeting business objectives. Most respondents agreed, showing that there is a consensus that their organisation has adopted system innovation as measured through the different items. Although the majority of respondents seem to agree on all of these items, it is important to note that there is a high number of respondents who neither agreed nor disagreed. This is an indication that respondents may not have understood the questions or they were reluctant to share information about their organisation.

Table 4.11: Systems Innovation Responses

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
SI2	5.9%	14.6%	18.9%	47%	13.5%	3.46	1.089
SI3	4.3%	10.3%	22.7%	49.7%	13%	3.55	.983
SI4	3.2%	11.4%	30.3%	43.8%	11.4%	3.48	.944
SI5	4.3%	6.5%	24.3%	47%	17.8%	3.67	.980

4.2.5. Information Security Risks

Information security risks are central to this research, this construct serves as a dependent variable. As this research seeks to study the relationship between systems innovation and it's antecedents as well as information security risks, special focus is placed on these two constructs particularly looking at the relationship between the two. The data collected on this construct is specifically linked to systems innovation and it takes into consideration the CIA triad. The data collected on this construct is meant to reflect organisational practices rather than individual ones as this would link seamlessly with systems innovation as it is also measured at the organisational level.

This construct is measured using new information security threats, system vulnerabilities, non-compliance, data integrity, and access rights. The selection of these items was based on the view to measure information security risks holistically.

On the first two items that relates to the increase in threats and vulnerabilities brought by new systems the data seems to point towards a narrative that systems innovation does increase threats and vulnerabilities. 30.3% of respondents agree that new system bring threats while 38.9% agree that rapid adoption increases vulnerabilities. The other three items suggest the opposite as the data seems to point towards the narrative that new systems do not lead to policy non-compliance, data leaks and incorrectly assigned access rights. 38.4% of respondents disagreed regarding policy non-compliance, 41.6% disagreed for data leaks and 38.9% disagreed regarding incorrectly assigned access rights.

Table 4.12: Responses for Information Security Risks

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Standard Deviation
SR1	4.3%	24.3%	28.1%	30.3%	13%	3.20	1.097
SR2	4.9%	25.9%	24.9%	38.9%	5.4%	3.11	1.034
SR3	7%	38.4%	32.4%	17.8%	4.3%	2.73	.985
SR4	7%	41.6%	33%	13%	5.4%	2.67	.980
SR5	9.2%	38.9%	28.6%	17.3%	5.9%	2.71	1.054

4.3. Reliability Test

Santos (1999) indicates that reliability tests are very important in studies where derivative variables are used for predictive analysis. In a study where one seeks to identify the relationship between antecedents of systems innovation and information security risks, it is important to perform a test on reliability in all constructs. Cronbach's Alpha provides a measure for internal consistency of a construct and internal consistency describes the interrelatedness and the extent to which all the items in a test measure the same construct (Tavakol & Dennick, 2011). Each construct initially had a total of five items and some of the items could not meet a sufficient level of consistency and were therefore removed.

Table 4.13: Reliability Analysis

Construct Name	Cronbach's Alpha	Mean	Number of Items retained
Complexity	0.793	0.556	3
Relative Advantage	0.804	0.449	5
Individual Factors	0.763	0.446	4
Organisational Factors	0.734	0.477	3
Environmental Factors	0.773	0.410	5
Systems Innovation	0.904	0.707	4
Information Security Risks	0.776	0.413	5

Acceptable values of Cronbach's Alpha range from 0.70 to 0.95 (Tavakol & Dennick, 2011). The above table shows that all seven constructs have achieved a Cronbach Alpha value greater than 0.7 with Relative Advantage and Systems Innovation having the highest values at .804 and .904 respectively. One can then deduce using Cronbach's Alpha that all seven contracts are reliable.

In relation to the number of items per construct, it is important to note that most items on each construct were found to be consistent and interrelated. Relative Advantage, Environmental Factors and Information Security Risks maintained consistency in all five items whereas only one item was found inconsistent on Individual Factors and System Innovation. Complexity and Organisational Factors maintained consistency in three items.

There are various techniques that can be used to analyse and interpret data and some of the most reliable data analysis tests include Analysis of Variance (ANOVA), test for difference in means (T-tests), and the Spearman ranked correlation coefficient. According to Norman (2010), ANOVA is more suitable for larger samples and one should use a t-test for a smaller sample. Therefore, ANOVA tests were not performed on the data as these tests and the t-test were performed as part of the regression testing where an analysis to determine the difference between two constructs is conducted.

4.4. Factor Analysis

Factor analysis was performed with the data collected from the questionnaires, extraction with varimax rotation and principle components was run on all seven constructs. Factor analysis is a multivariate statistical method (Williams *et al.,*2010) which makes use of mathematical measures to simplify interrelated measures to discover patterns in a set of variables (Yong & Pearce, 2013).

4.4.1. KMO and Bartlett's Test

Prior to performing factor extraction, it is important to perform a Kaizer-Meyer-Olkin (KMO) test of sampling adequacy and Bartlett's test of sphericity. According to Williams *et al.* (2010), the KMO measure of sampling adequacy has a range of 0 to 1 and in order to proceed with factor analysis, a KMO value of 0.5 or more is considered suitable. The data collected for this research obtained a KMO value of 0.764 which indicates that the factor analysis was statistically appropriate. Bartlett's test of sphericity was also performed, this test provides an indication of whether variables are unrelated (Varol, 2011). For factor analysis to be considered statistically suitable, Bartlett's test of sphericity should be significant at $p<0.5$. As shown in Table 4.15 below, the test of sphericity seems to be significant at $p<0.001$.

Table 4.14: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.764
Bartlett's Test of Sphericity	Approx. Chi-Square	2168.133
	Df	325
	Sig.	.000

The results obtained from a KMO and Bartlett's test shows that the sample size was adequate for the variables being measured and that there is a strong relationship between items measuring the same variable. Section 4.3.3 below provides a comprehensive overview of the correlation of items measuring the same construct. There are different opinions in the literature regarding what a suitable sample size should be. Williams *et al.* (2010) and many works of literatures cite the work of Comrey Lee which regards 100 – poor, 200 – fair, 300 – good, 500 – very good and >1000 – excellent, however, other authors found that studies with a correlation coefficient

greater than 0.8 require smaller sample sizes. For the purposes of this study, a sample size of 185 respondents was used.

Zamanzadeh *et al*. (2015) refer to validity as the data collection instruments' capability to measure the properties of the construct or concept being studied. The validity tests that were performed on the data showed that most items did measure what they are supposed to measure. Items that were found to not measure what they supposed to measure were removed. Each construct had five items and Table 4.2. below shows the number of items that were retained. Two items were removed from complexity and organisational factors, one was removed from individual factors and systems innovation. All items were retained for relative advantage, environmental factors as well as information security risks.

Another way to ensure validity and sampling adequacy is to perform a Kaizer-Meyer-Olkin (KMO) test on each of the variables being measured. Table 4.1 below shows the results for the KMO test which shows that the values for each of the variables range between 0.568 to 0.825. According Kaiser (1974) values greater than 0.5 are recommended as barely acceptable. Values between 0.5 and 0.7 are ordinary, values between 0.7 and 0.9 are good, values between 0.8 and 0.9 are very good and values above 0.9 are superb (Hutcheson & Sofroniou, 1999).

Table: 4.15: KMO and Bartlett's Test Values

			RA	C	IF	OF	EF	SR	SI
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.764	.805	.623	.745	.568	.764	.755	.825
Bartlett's Test of Sphericity	Approx. Chi-Square	2168.133	284.637	231.234	203.042	156.763	242.507	257.028	327.748
	Df	325	10	10	10	10	10	10	10
	Sig.	.000	.000	.000	.000	.000	.000	.000	.000

4.4.2. Total Variance

The most common method used in exploratory factor analysis is Eigenvalue-greater-than-one rule (Patil *et al.*, 2008). The analysed data shows that seven factors were retained as they all have eigenvalues of greater than one with the highest eigenvalue being 5.418 and 1.115 being the lowest. The communalities value for extraction range

from 0.427 to 0.867 as shown in the communalities table in Annexure B. Table 4.16 below summarises the exploratory factor analysis showing the Eigenvalues for the seven factors retained.

Table 4.16: Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	5.418	20.840	20.840	5.418	20.840	20.840	3.253
2	3.549	13.649	34.488	3.549	13.649	34.488	2.725
3	2.805	10.787	45.275	2.805	10.787	45.275	2.484
4	1.717	6.604	51.880	1.717	6.604	51.880	2.407
5	1.584	6.092	57.972	1.584	6.092	57.972	2.245
6	1.233	4.743	62.715	1.233	4.743	62.715	2.172
7	1.115	4.290	67.004	1.115	4.290	67.004	2.135
8	.911	3.502	70.506				
9	.809	3.110	73.617				
10	.741	2.849	76.466				
11	.694	2.670	79.136				
12	.584	2.248	81.383				
13	.574	2.207	83.591				
14	.528	2.029	85.620				
15	.503	1.935	87.555				
16	.475	1.826	89.380				
17	.461	1.774	91.155				
18	.386	1.486	92.640				
19	.349	1.342	93.982				
20	.331	1.274	95.256				
21	.275	1.057	96.313				
22	.257	.988	97.301				
23	.220	.848	98.149				
24	.204	.786	98.935				
25	.151	.581	99.516				
26	.126	.484	100.000				

The table above further shows that the seven factors retained cumulatively explain 67% of the variance in the factors which is quite significant. The measuring instrument initially comprised of 35 questions and after factor analysis, nine questions were removed hence, there are 26 factors. This reiterates the validity of the measuring instrument and further validates the questions used in the measuring instrument.

4.4.3. Rotated Component Matrix

An extraction method of principal component analysis was performed on the data using a varimax rotation with Kaiser normalisation. The rotation covered seven iterations on the seven extracted components. Table 4.17. below show component loadings of the seven components as extracted. The matrix shows that each component loads with at least one variable where systems innovation loads with Component 1 and information security risks loads with component 2. Individual, organisational and environmental factors load with component 3, 6 and 5 respectively. Lastly, complexity and relative advantage load with component 7 and 4 respectively. It important to note that all constructs measured in this study are loading and this provides assurance on the validity of the measuring instrument and the items used to measure these constructs.

Table 4.17: Rotated Component Matrix

	Component						
	1	2	3	4	5	6	7
SI3	.904	-.014	-.027	.071	.171	-.044	.111
SI5	.827	.033	-.043	.153	.100	-.146	.001
SI2	.824	.086	-.048	.002	.181	-.073	.105
SI4	.820	.059	-.084	.099	.187	-.273	-.028
SR2	-.014	.827	.008	-.087	.046	-.096	.097
SR3	.179	.735	.081	.024	.064	.091	-.070
SR4	.081	.735	.155	.123	-.044	.095	-.156
SR1	-.061	.714	-.060	-.052	.072	-.016	.103
SR5	-.016	.571	.246	.069	-.051	.117	-.142
IF2	-.079	.167	.806	-.059	-.109	-.064	-.053
IF5	-.030	.021	.768	-.052	.088	.025	-.135
IF3	-.193	.113	.765	-.087	-.044	.007	-.245
IF1	.195	.086	.563	-.407	-.109	-.013	.050
RA2	.147	.019	-.191	.828	.004	.096	.060
RA3	.052	.027	-.071	.780	.073	.071	.258
RA4	.135	.017	-.071	.720	.188	-.011	.246
EF3	.156	.171	.009	-.004	.784	.019	-.019
EF4	.172	-.049	-.143	.083	.766	-.241	.169
EF5	.092	-.019	-.089	.162	.665	-.419	-.043
EF2	.262	-.015	.057	.111	.552	-.095	.175
OF3	-.201	.025	-.015	.019	-.108	.848	.026
OF4	-.072	.090	-.138	-.004	-.136	.710	.117
OF2	-.194	.048	.144	.183	-.199	.709	-.206
C2	.018	-.086	-.287	.145	.141	.087	.835
C1	.120	-.084	-.187	.245	.092	.049	.812
C4	.064	.059	.035	.432	.019	-.170	.594

4.5. Correlation Analysis

The sections below present a correlation analysis for both DoI and organisational innovation constructs. The section also shows the correlation between systems innovation and information security risks. Correlations are used to identify relationships between constructs.

4.5.1. DoI attributes Correlation

Complexity and relative advantage seeks to measure the innovation potential of organisations based on the DoI theory. The two constructs are important as they provide a comprehensive understanding of whether an organisation is able to adopt new systems easier and at a faster pace when systems are easy to use and perceived to be better than old or existing systems.

The correlation table below. 4.18, shows that there is a significant positive correlation between the two constructs. A positive correlation with complexity shows that the increased ease of use on the system, the easier it is for a such system to be adopted. Therefore, one can deduce that there is a positive relationship between a reduction in systems complexity and systems innovation. The data also shows a significant positive relationship between relative advantage and systems innovation. The correlation coefficient for these two variables is 0.191 with a significant value of 0.009. The positive correlation suggests that an increase in the notion that new systems offer more advantages compared to existing or old ones. This finding is also consistent with the DoI model as it also shows a significant positive correlation between the two variables.

Table 4.18: Correlation Analysis for DoI Attributes

		Systems Innovation
Complexity	Correlation coefficient	.226
	Sig. (2 tailed)	.002
	N	185
Relative Advantage	Correlation coefficient	.191
	Sig. (2 tailed)	.009
	N	185

The hypotheses for complexity and relative advantage suggests that a relationship exists between systems innovation and the two constructs and the findings are consistent with both hypotheses as a positive relationship can be detected in each case. The data also shows that the relationships are both significant and therefore consistent with the hypotheses.

4.5.2. Organisational Innovation Correlation

The organisation is at the heart of this study and it is for this reason that three organisational elements are used to examine systems innovation in an organisational context. Table 4.19 below shows that systems innovation has a significant negative relationship with individual factors as well as with organisational factors. A significant positive relationship exists between systems innovation and environmental factors.

Items used to measure individual factors construct include motivation, technical skills, cognitive ability and creativity. A negative relationship exists between the two constructs which is significant at $p<0.05$. Organisational factors also have a negative relationship with systems innovation, the items used to measure the correlation between these constructs were financial investment, organisational culture, dynamics and politics. The correlation data shows that the relationship between organisational factors and systems innovation is significant. This finding is consistent with the hypotheses which state that there is a relationship between the two constructs.

Table 4.19: Correlation Analysis for Organisational Innovation Attributes

		Systems Innovation
Individual Factors	Correlation coefficient	-.165
	Sig. (2 tailed)	.025
	N	185
Organisational Factors	Correlation coefficient	-.357
	Sig. (2 tailed)	.000
	N	185
Environmental Factors	Correlation coefficient	.439
	Sig. (2 tailed)	.000
	N	185

The data collected shows a positive correlation between environmental factors and systems innovation which is also significant at $p<0.05$. Items used to measure environmental factors include changes in government regulations, pressure from customers and competitors and compliance with regulations. The significance in the

relationship means that these items do influence the rate at which organisations innovate.

Organisational innovation hypotheses suggest that systems innovation has a negative relationship with individual and organisational factors whereas a positive relationship exists with environmental factors. Correlation data shows all relationships measuring these constructs are significant as they are all below the significance level of 0.05. These findings reiterate that antecedents of systems innovation do have an influence in the level of systems innovation organisations take on.

4.5.3. Systems Innovation and Information Security Risks

Measuring the correlation between information security risks and systems innovation is one of the key objectives of this study and the data analysed shows that there is no significant correlation between the two constructs. The significance level of this correlation is very low as indicated in Table 4.20.

Table 4.20: Information Security Risks and Systems Innovation Correlation Coefficient

		Systems Innovation
Information Security Risks	Correlation coefficient	.066
	Sig. (2 tailed)	.373
	N	185

The findings dispel the hypothesis which suggests that a relationship exists between systems innovation and information security risks. The correlation coefficient between the two variables is 0.66 and $p>0.05$, therefore, one can deduce that changes in Systems Innovation will not affect Information Security Risks.

4.6. Regression Analysis

A linear and multiple regression test were performed with the aim of testing the research hypotheses. A multiple regression test is conducted between systems innovation and all its antecedents. A linear regression test was performed between systems innovation and information security risks.

4.6.1. Multiple Regression for Systems Innovation

A multiple regression analysis was conducted to test the extent to which variance systems innovation can be predicted using complexity, relative advantage, individual factors, organisational factors, and environmental factors. Due to the large number of predictors, this model may be affected by issues of multicollinearity which according to Kraha *et al.* (2012) refers to the extent to which the predictor variable has non-zero correlations with each other. This happens in models with multiple predictors such as this one. However, collinearity diagnostics were performed on the data and the results are attached in Annexure B.

Table 4.21: Systems Innovation's Overall Significance on the Model

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	35.231	5	7.046	11.696	.000
	Residual	107.840	179	.602		
	Total	143.071	184			

Table 4.21 shows that the model is significant at F=11.696 and p<0.05 which means that independent variables influence the dependent variable. This shows that changes in attributes of DoI and organisational innovation have an influence in the rate at which organisations use systems to innovate. This is also confirmed in the correlation analysis which detected correlations with all the variables of DoI and organisational innovation. One can also deduce that the variance in systems innovation can therefore be predicted using DoI Attributes and those of organisational innovation.

Table 4.22: Systems Innovation Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.502	.252	.229	.75496

The R square in Table 4.22 above indicates that independent variables explain 25.2% of the variance in systems innovation in an organisational context. This is important as it is consistent with the hypotheses which all suggest that independent variables do predict the variance on systems innovation.

Table 4.23: Systems Innovation Regression Analysis

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	2.102	.598	-	3.517	.001	.923	3.282	-	-
	Relative Advantage	.170	.083	.159	2.057	.041	.007	.333	.707	1.413
	Complexity	.036	.095	.030	.384	.702	-.151	.224	.695	1.440
	Individual Factors	-.012	.082	-.010	-.144	.886	-.174	.150	.835	1.197
	Organisational Factors	-.212	.068	-.228	-3.137	.002	-.345	-.079	.797	1.255
	Environmental Factors	.346	.089	.291	3.865	.000	.169	.522	.744	1.344

It is also important to examine each construct to see its level of influence on systems innovation. The above table of coefficients breaks down each independent variable to identify the ones with a significant influence on systems innovation. Only complexity and individual factors do not show a significant relation. All the other variable shows a significant influence.

4.6.2. Simple Linear Regression for Information Security Risks

Simple linear regression was performed analyse the extent to which the independent variable accounts for the variance in the dependent variable. Multiple linear regression was not used in this case as it only involves two variables. This is important for the accuracy of the model as it guards against multicollinearity which according to Tu *et al.* (2005) can significantly distort the manner in which the model is interpreted.

Table 4.24: Information Security Risks' overall significance on the model

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.600	1	.600	1.071	.302
	Residual	102.564	183	.560		
	Total	103.165	184			

Table 4.24 shows the significance of information security risks and systems innovation in the model where F=1.071 and p=0.302. This shows that variances in the dependent variable cannot be used to predict variance in the independent variable. This means that based on the results from the regression test, there is no significant relationship between information security risks and systems innovation.

Table 4.25: Information Security Risks Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.076	.006	.000	.74864

As indicated in Table 4.25, R Square is 0.006 which indicates that the model only explains 0.6% of the changes in information security risks. The R Square value is significantly low with the adjusted R square being 0.000, one can therefore deduce that the variance in information security risks cannot be predicted by systems innovation. Table 4.26 below which shows correlation coefficients also confirms this as p>0.05.

Table 4.26: Information Security Risks' Correlation Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	2.655	.228		11.628	.000	2.204	3.105		
	Systems Innovation	.065	.063	.076	1.035	.302	-.059	.188	1.000	1.000

4.7. Hypothesis Test Results

Hypothesis testing allows for testing the theoretical model as illustrated in Figure 2.10 above. Since the model is generally testing correlations between variables, correlation and regression analysis are used to test these hypotheses. Table 4.27 below shows that out of six hypotheses, three were rejected and three were supported. The three-rejected hypotheses include those which were measuring the complexity, individual

factors and information security risk constructs. As the main objective of this study was to examine the relationship between antecedents of systems innovation and information security risks, the data analysed failed to prove that there is a significant relationship between systems innovation and information security risks however some significant relationships could be established between systems innovation and some antecedents.

Table 4.27: Hypothesis Test Results

Hypotheses	Cronbach's Alpha	Sig. (p)	Beta (β)	t-value
Complexity (H1)	0.793	.041	.159	2.057
Relative Advantage (H2)	0.804	.702	.030	.384
Individual Factors (H3)	0.763	.886	-.010	-.144
Organisational Factors (H4)	0.734	.002	-.228	-3.137
Environmental Factors (H5)	0.773	.000	.291	3.865
Systems Innovation (H6)	0.904	.302	0.076	1.035

H1: *Complexity of systems influences the rate at which organisations implement system innovation.* The relationship between complexity and systems innovation is not significant. Multiple regression tests found that β=0.030 and p>0.702. H1 is rejected.

H2: *There is a relationship between relative advantage and systems innovation.* A positive and significant relationship does exist between relative advantage and systems innovation. Multiple regression test results show that β=0.159 and p<0.05. H2 is supported.

H3: *Individual factors are affected by the rate of systems innovation.* Multiple regression analysis data shows that the relationship between individual factors and systems innovation is not significant as β=-0.010 and p>0.05. H3 is rejected.

H4: *Organisational factors such as policies, resources, and culture influence systems innovation.* A negative relationship exists between organisational factors and systems innovation, the data also shows that such a relationship is significant. Multiple regression results show that β=-0.228 and p<0.05. H4 is supported.

H5: *The external environment which includes technology, competitors and regulations is affected systems innovation.* A positive relationship exists between environmental factors and systems innovation, the data shows a high significance. Multiple regression tests show that β=0.291 and p<0.05. H5 is supported.

H6: *Information security risks are affected by an increase in the organisation's systems innovation*. A linear regression test shows that there is no significant and positive relationship between systems innovation and information security risks where β=0.076 and p>0.05. H6 is rejected.

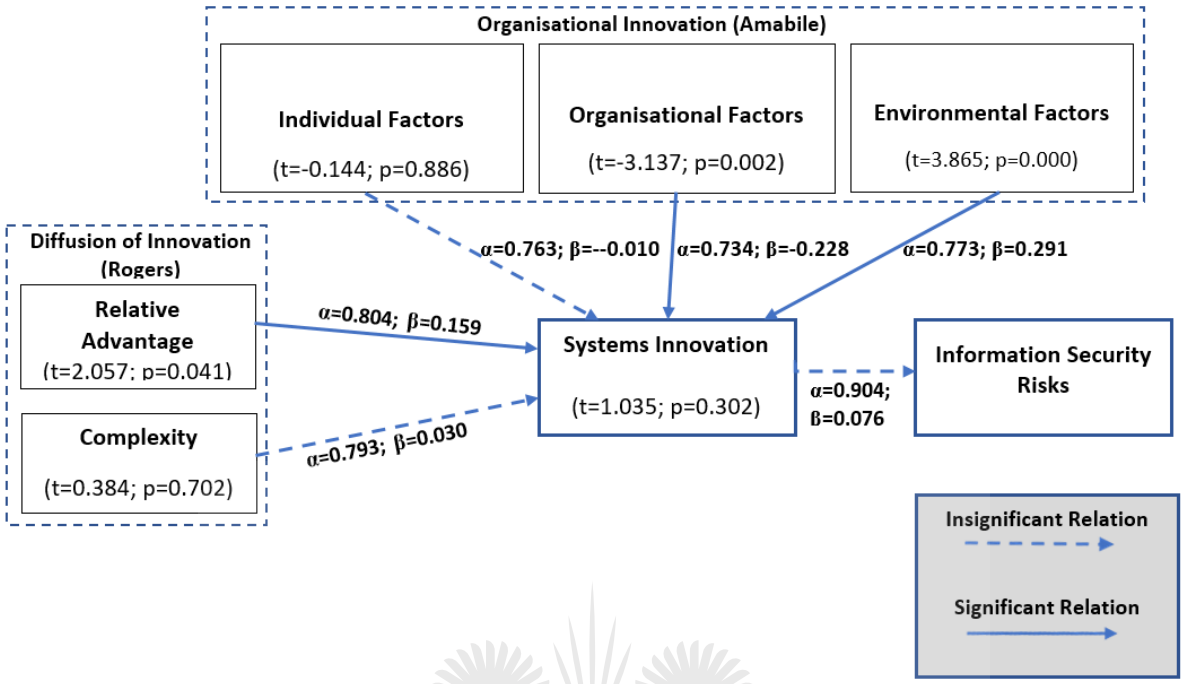
Table 4.28: Key Findings Summary

Variables	Regression Test Results Sig. (p)	Hypotheses Results
Complexity (H1)	.041	Rejected
Relative Advantage (H2)	.702	Failed to Reject
Individual Factors (H3)	.886	Rejected
Organisational Factors (H4)	.002	Failed to Reject
Environmental Factors (H5)	.000	Failed to Reject
Systems Innovation (H6)	.302	Rejected

4.8. Revised Theoretical Model

A conceptual model is developed based on the results of regression tests and factor analysis. The revised theoretical model illustrates the results as well as the relationship between the constructs as presented in Figure 4.4. below. When looking at the two theories that were used to develop the theoretical model, it is important to note that there are certain discrepancies in the correlations identified between constructs. It is for this reason that the revised model differs slightly with the initial theoretical model.

Figure 4.4: Revised Theoretical Model



In the literature review, it was established that in the DoI theory, complexity will have a positive and significant relationship with systems adoption which leads ultimately affects systems innovation. A vast body of research suggests that decreased complexity has a strong impact on the adoption of new technology (Al-Jabri & Sohail, 2012). Inconsistencies were also found in the organisational innovation model where an insignificant relationship was found between individual factors and systems innovation. The initial theoretical model proposed a strong relationship between the two variables. The same is true for systems innovation and information security risks where the model was revised from a significant to an insignificant relationship. All other variables were found to be consistent with the initial theorised model.

The revised model is relevant for organisations that seek to pursue systems innovation and effectively manage their information security exposure. The significant relationships identified by the model should be viewed as key focus areas as a causal relationship has already been developed. Where insignificant relationships exist, organisations may need to do more investigations of their own on how such factors can be used to drive innovation and information security management. Organisations may also choose to manage the two factors separately where an insignificant relationship exists.

4.9. Chapter Summary

It is evident that data analysis is vital in providing an interpretation of the data in order to deduce the research findings. Descriptive statistics provided a comprehensive overview of how the respondents responded and analysis of demographic information. Validity and reliability test were performed in this chapter providing the assurance on the measuring instrument and the sample. Regression and correlation test results were also highlighted in this chapter. Regression test were used to test hypotheses, and a revised theoretical model was also presented in this chapter.

CHAPTER 5: DISCUSSION AND CONCLUSION

5.1. Introduction

This research sought to examine the relationship between systems innovation and information security risks and to examine the relationship between systems innovation and its antecedents. To meet these objectives, an extensive literature review was conducted in order to conceptualise the study of innovation together with the theory of information security risks. The literature review was used to develop a conceptualised model which identified constructs that can assist in measuring systems innovation and information security risks. Research hypotheses were developed based on the research objectives and the conceptual model that was constructed. A quantitative method was used to analyse the data collected from 185 respondents using an SPSS software. The conceptual model was tested through regression and factor analysis.

According to Hart (2018), a review of the literature is important as it provides a broader understanding of the concepts, highlights research that has already been done on them and the key issues regarding the concepts. Because this research brings together the concepts of systems innovation and information security, it is vital to understand the theoretical background of these two concepts. A literature review provided a thorough investigation of these concepts as well as the key issues surrounding them.

5.2. Components of Innovation Theories

In seeking to answer the research question of “what relationship exists between components of innovation theories and systems innovation?” this section examines the two theories used to study antecedents of systems innovation and information security risks. The analysis of these two theories draws on the findings of the research as well key insights derived from the literature.

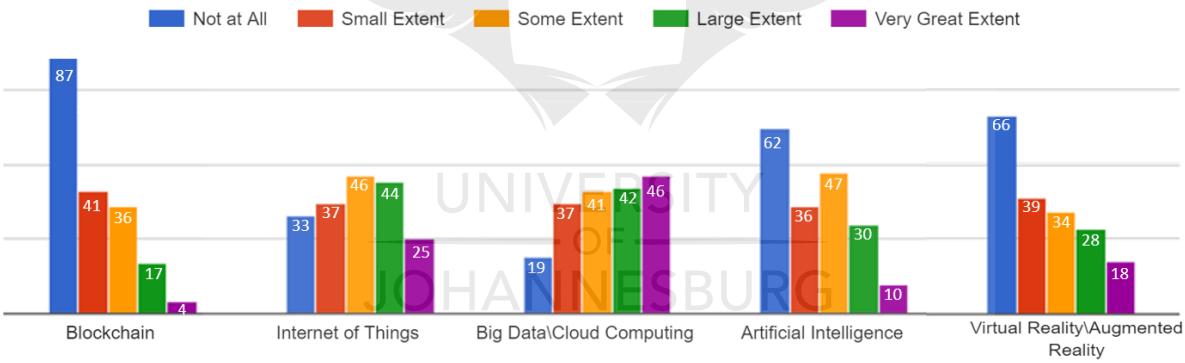
5.2.1. Attributes of DoI

The two attributes of DoI used in this research provide valuable insights into the manner in which systems innovation is understood. However, one of the key indicators of systems innovation in organisations is through evaluating the adoption of emerging technologies. The data collected shows the level of adoption by an organisation on technologies such as blockchain, the internet of things, big data/cloud computing,

artificial intelligence, and virtual/augmented reality. The results from the data show that technologies/systems that provide more benefits are likely to be adopted. This may also explain why some innovations are generally accepted by most organisations while others are not.

Data extracted from the descriptive analysis shows that blockchain is not readily adopted by organisations compared to cloud computing/big data, one may then deduce that blockchain is a complex technology and because of its uniqueness, it is difficult to measure its relative advantage. The ability to provide a secure transactional platform is a great value proposition for organisations however this is not enough to compel organisations to adopt it. One can also deduce that some organisations have not realised the potential benefits of blockchain thus explaining the slow adoption. Figure 5.1 below provides a summary of systems adoption for each technology/system.

Figure 5.1: System Adoption



Big data/cloud computing presents numerous opportunities for organisations as it provides increased accessibility of information and allows for aggressive analysis. It is easy to measure relative advantage on big data/cloud computing as a comparison can be made with technologies such as data warehousing and locally hosted solutions. Judging from the analysis derived from descriptive statistics, one can deduce that benefits from big data/cloud computing far outweigh those of previous technological solutions. System complexity did not have an influence in the adoption of big data/cloud computing as regression analysis shows it has an insignificant relationship with systems innovation. Hashem *et al.* (2015) agree that big data/cloud computing has significantly shifted ICT and services in organisations towards a more complex and large scale computing.

As the research findings suggest, systems innovation has an insignificant relationship with information security risks. It is important to note that information security risks should not be an impediment used to prevent organisations from innovating. Although this finding is not conclusive, it helps to provide valuable insights to ensure that innovation behaviour is not perceived as risky and reckless. Some of the key information security concerns with big data/cloud computing involves data integrity, accessibility and third-party reliance. This means that there are serious information security considerations prior to the adoption of this technology however the data shows that big data/cloud computing was widely adopted by a number of organisations. The benefits of using this technology outweighed the disadvantages that come with information security risks. According to Thierer (2015), innovation must be allowed to continue uninterrupted and if problems arise, they can be addressed later.

The adoption of IoT is moderate and although it is a growing technology, organisations seem to derive value using interconnected devices. Such benefits include increased communication, efficiency in delivering business results, interoperability between systems, and better management of organisational assets. Because of the increased internet exposure, IoT is highly vulnerable to cyber-attacks and other internet-based threats. However, there have been many research achievements in dealing with security concerns for IoT and that has led to the successful implementation of privacy and security infrastructure in IoT technologies (Farooq *et al.*, 2015). Despite information security risks IoT received a relatively high level of adoption by many organisations.

The findings of this research also suggest that information security risks that come with artificial intelligence and virtual/augmented reality are not the reason for the low levels of adoption. The low adoption of these two technologies may come as a result of organisations' inability to realise their potential benefits. Other factors such as pricing, operational requirements and alignment with organisational strategic objectives could be the reason for the low adoption. Concerns have already been raised that artificial intelligence and virtual/augmented reality may lead to job losses and these controversies may be the real reason behind the low adoption.

Research finding indicates that relative advantage is the main contributing factor leading to an increase in systems innovation. Complexity does not have much of an

influence as it is found to have an insignificant relationship with systems innovation. The systems adopted have proven to have several benefits which further emphasises the importance of relative advantage as an antecedent of systems innovation. Another key finding is that there is no significant relationship between information security risks and systems innovation. The lack of a significant relationship between these two variables brings an important narrative that seeks to disqualify information security as the reason for the low adoption of systems in organisations.

5.2.2. Attributes of Organisational Innovation

Individual factors such as motivation, cognitive ability, and skills, proved not to influence the level at which organisations adopt technology and systems. This is based on the insignificant relationship that was identified between individual factors and systems innovation. One can therefore deduce that employees' individual attributes such as motivation, skills, and cognitive ability will not lead to increased systems innovation. Based on the literature review in Chapter 2, individual factors are significant elements with a high influence on information security, however, they have an insignificant link with systems innovation. This further explains the lack of a significant relationship between information security risks and systems innovation.

Organisational factors such as policies, culture, and resources also lead to an increase in systems innovation. This means that organisations with better resources, effective policies and an organisational culture that supports innovation can rapidly adopt information systems. As the research findings suggest, rapid systems innovation does not lead to increased information security risks. However organisations must continue to strive towards strengthening compliance with information security policies, create an organisational culture that supports information security and increase investments in information security systems and tools. Amabile (2011) indicates that innovation requires a combination of various components and most importantly, it works in an organisational environment where it is highly supported.

The multiple regression test shows a significance level of 0.000 between systems innovation and environmental factors, this is a significantly high relationship between the two variables which suggests that environmental factors such as competitors, technology advancement, and changes in government regulations have a high influence in systems innovation. These external factors are often determinants of the

organisation's competitive edge. This finding shows that organisations do not operate in a vacuum and that innovation is often triggered by events external to the organisation. Innovation models revolve around the recognition of the importance of the competitive advantage that often come from leveraging these external environment (Lakovleva, 2013).

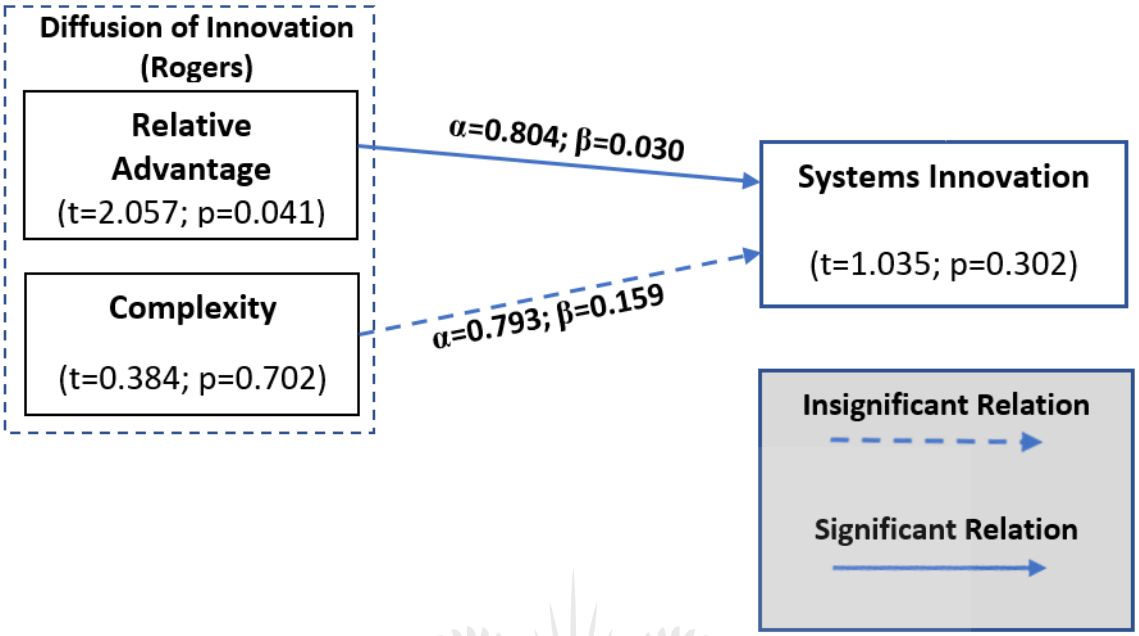
5.3. Achieving Research Objectives

One of the key objectives of this research was to examine the relationship between systems innovation and information security risks. Secondary to this objective, the research also seeks to investigate the relationship between systems innovation and its antecedents. These research objectives are further discussed below.

5.3.1. Relative Advantage and Complexity

The significant relationship between relative advantage and systems innovation is consistent with the DoI theory. The relationship between systems innovation and complexity is insignificant meaning systems complexity is not the main course for lack of system adoption. This means it is highly critical for organisations to focus more on developing systems with more benefits than to focus on user-friendly ones. Results from the descriptive statistics also indicate that a significantly high number of respondents responded positively to questions that suggest that it is easier to adopt a system that has more benefits compared to older or existing systems. Figure 5.2. below provides a summary of the relationship between attributes of DoI and Systems Innovation with results from the regression analysis.

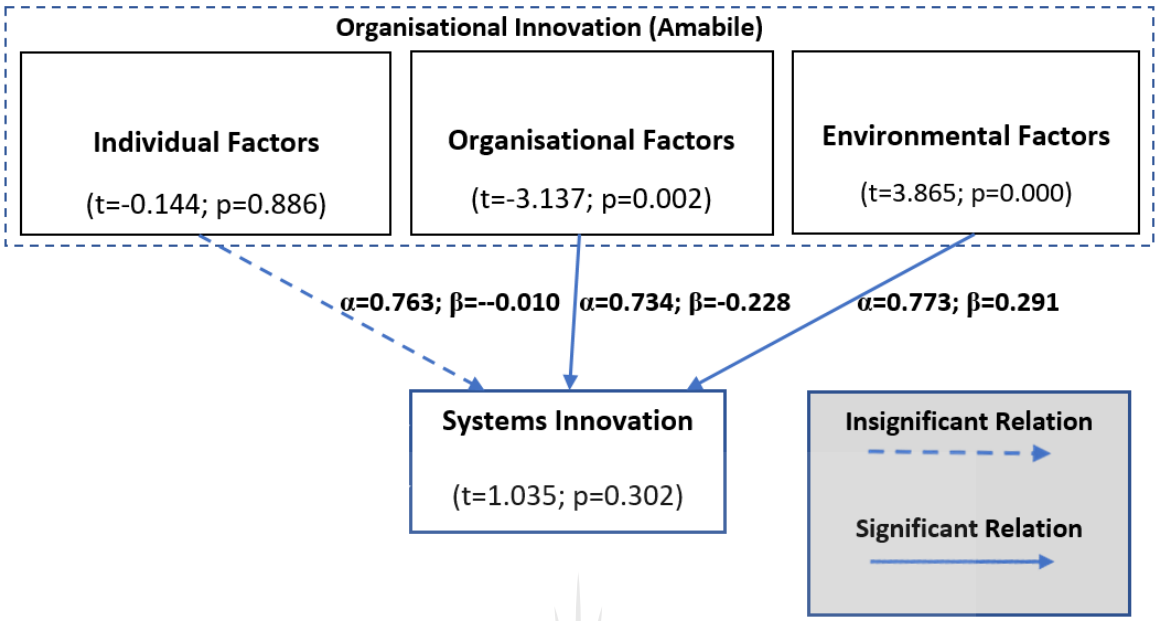
Figure 5.2: Summary of DoI Attributes Relationship



5.3.2. Individual, Organisational and Environmental Factors

The three elements of organisational innovation have a somewhat complex relationship as organisational factors and environmental factors show a strong positive relationship with systems innovation. Individual factors on the other hand seem to have an insignificant relationship with Systems Innovation. This means it is difficult for the personal attributes of employees to influence systems innovation in an organisation. Organisational and environmental factors are the major drivers of organisational innovation. This means that organisations would have to focus more on cultivating and creating an innovation-friendly culture and to use innovation as a competitive advantage to respond to events triggered by external factors such as customers and competitors. These key findings are derived from regression test results and are somewhat confirmed by the correlation analysis which identified positive correlations with all the three variables. A summary of the relationship between organisational innovation elements and systems innovation can be found in Figure 5.3. below.

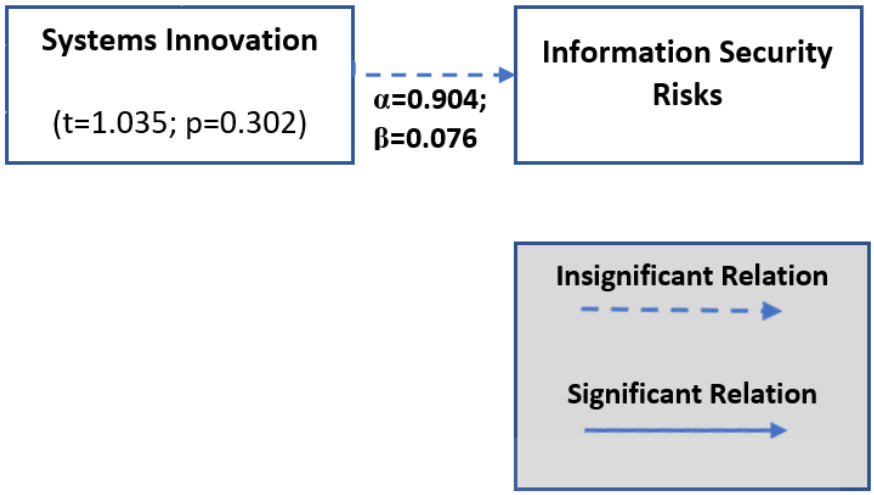
Figure 5.3: Summary of Organisational Innovation Elements



5.3.3. Systems Innovation and Information Security Risks

As the main research objective of this study is to examine the relationship between systems innovation and information security risks, the data from both correlation and regression tests confirm that there is an insignificant relationship between these two variables. This means that in an organisation, an increase in information security risks cannot be attributed to an increase in systems innovation. This finding is not conclusive however it is important as it dispels the notion that innovation is a catalyst for growing information security risks. Organisations seeking to pursue systems innovation should still worry about information security however, they must also be able to strike a balance by putting in place mitigation strategies for such risks. Figure 5.4. below shows a summary of the relationship between systems innovation and information security risks.

Figure 5.4: Summary of Systems Innovation and Information Security Risks



5.4. Implications to Research Population

This research identifies IT practitioners within various organisations and It students in South Africa as the population. This population often has a key task of delivering new information systems and finding innovative ways in which the organisation can adopt to create business value. Organisations are also faced with pressures from the external environment which leave them with no choice but to innovate as a way of enhancing their competitive advantage. It is important for this population to have a holistic understanding of information security and how it relates to innovation. The population must also be aware of ascendants of innovation which can be used as catalysts to accelerate innovation initiatives by the organisations.

5.5. Contribution to Knowledge

The contribution of this research to knowledge is quite a significant one as it uses various pre-existing theories to answer questions relating to innovation and information security risks. The fact that this research found its basis on well-established theories is important as it seeks to expand on the knowledge that already exists. The research also examined five technologies which are relatively new therefore, the findings are important in assisting with better decision making with regards to the technologies/systems examined. The building of this theory also assists those who have the responsibility of developing new technologies as the findings of this research provides valuable lessons to learn regarding to the adoption of new

technology. This research contributes to the body of knowledge in areas of DoI and organisational innovation with a specific focus on the South African context.

5.6. Limitations

There are several limitations associated with this study, although several interventions were put in place to minimise the effect of these limitations, it is equally important to outline them. The following are the limitations associated with the study:

- The sample size for this study is 185 respondents, given the nature of this study and methodological choice, it would have been ideal to have a sample size of 200 to allow for better statistical analysis:
- The snowballing sampling method allows respondents to nominate and refer other respondents to participate in the study. This presents its own challenges as the researcher is not able to verify if the referred respondents fit the sampling criteria which in this case is IT Professionals and students; and
- Limiting the sample to IT Professionals and students ensured that the respondents have enough knowledge about the variables being measured however this sample introduces problems with the generalisation of the findings. The findings of this research cannot be generalised onto the broader South African population.

5.7. Recommendations for Future Research

Further research that can be developed on this topic may examine the relationship between information security risks and systems innovation perhaps using a different methodology and theoretical lens. This would assist in providing a comprehensive understanding of these two variables and how they relate to one another. Developing an information security framework for systems innovation would also be a key research area linked to this research as it would provide a blueprint of how IT practitioners need to approach issues of information security when pursuing systems innovation.

This research does not examine how antecedents of systems innovation relate to one another and this presents an opportunity to explore how these antecedents are related. A Technology Acceptance Model (TAM) may also be developed using the five

systems that were examined in this research as this will further explain how and why other technologies are adopted compared to others.

5.8. Conclusion

It is evident that the research was able to meet its objectives and it produced valuable findings that assists to better understand the relationship between systems innovation and its antecedents as well as with information security risks. One of the findings in this research is that relative advantage was identified as a catalyst for systems innovation and that complexity did not influence systems innovation. From this finding, it is important to note that it is very important for organisations to focus more on ensuring that new systems and technologies provide more benefits and value for the organisation rather than focusing on making them less complex.

The second key finding shows that individual characteristics of employees do not have any effect on systems innovation. Therefore it is more important to focus on organisational and environmental factors when seeking to accelerate innovation. One can therefore deduce that efforts seeking to strengthen organisational factors such as investment in information systems, creating an innovation-friendly culture and policies will have a positive effect on systems innovation.

Lastly, the research findings also show that information security risks are not impacted by systems innovation. Although this finding is not conclusive, it is important to note that organisations need not use information security risks as a barrier to innovation. It is evident that the lack of a significant relationship indicates that organisations would need to strike a balance between managing the information security risks associated with new systems and making sure that such systems provide more value for the organisations.

5.9. Chapter Summary

This chapter provides a comprehensive discussion of the findings and a holistic summary for the research. The findings made in Chapter 4 are linked to the research objectives and the chapter also provides a contextualisation of the findings to the research population. The contribution of the study to the body of knowledge is discussed in this chapter together with the limitations of the study.

References

Abubaker, F. R. & Boluk, P.S. (2016). August. An Intelligent Model for Vulnerability Analysis of Social Media User. In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on* (pp. 258-263). IEEE.

Academic Coaching & Writing. (2017). Dissertation proposal online. Available at: https://www.academiccoachingandwriting.org/dissertation-doctor/resources/dissertation-proposal-outline (Accessed 30 May 2018)

Agrawal, D., Das, S. & El Abbadi, A. (2011). Big data and cloud computing: current state and future opportunities. In *Proceedings of the 14th International Conference on Extending Database Technology* (pp. 530-533). ACM.

Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security-Volume 105*(pp. 47-55). Australian Computer Society, Inc.

Ali, O., Soar, J., Yong, J., McClymont, H. & Angus, D. (2015). Collaborative cloud computing adoption in Australian regional municipal government: An exploratory study. In *Computer Supported Cooperative Work in Design (CSCWD), 2015 IEEE 19th International Conference on* (pp. 540-548). IEEE.

Al-Jabri, I. & Sohail, M.S. (2012). Mobile banking adoption: Application of diffusion of innovation theory.

Al-khafaji, N.J., Shittu, A.J.K. & Osman, W.R.Z.S. (2014). May. G2G interaction among local agencies in developing countries based on diffusion of innovations theory. In *Digital Information and Communication Technology and it's Applications (DICTAP), 2014 Fourth International Conference on* (pp. 125-131). IEEE.

Alohali, M., Clarke, N., Furnell, S. & Albakri, S. (2017). Information security behavior: Recognizing the influencers. In *Computing Conference, 2017* (pp. 844-853). IEEE.

Alzamil, I., Djemame, K., Armstrong, D. & Kavanagh, R. (2015). Energy-aware profiling for cloud computing environments. *Electronic Notes in Theoretical Computer Science*, *318*, pp.91-108.

Amabile, T. (2011). Componential theory of creativity. Harvard Business School.

Amabile, T.M. & Pratt, M.G. (2016). The dynamic componential model of creativity and innovation in organizations: Making progress, making meaning. *Research in Organizational Behavior*, *36*, pp.157-183.

Amabile, T.M. (1998). *How to kill creativity* (Vol. 87). Boston, MA: Harvard Business School Publishing.

Anthi, E., Williams, L. & Burnap, P. (2018). Pulse: An adaptive intrusion detection for the Internet of Things.

Antsaklis, P.J. & Michel, A.N. (2007). *A linear systems primer* (Vol. 1). Boston: Birkhäuser.

Appari, A. & Johnson, M.E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), pp.279-314.

Ashenden, D, & Sasse, A (2013). 'CISOs and organisational culture: Their own worst enemy?', Computers & Security, 39, pp. 396-405, Inspec, EBSCOhost, viewed 11 October 2017.

Ataya, G. (2013). Information security, risk governance and management frameworks: An overview of cobit 5. In *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 3-5). ACM.

Barzak, O., Molok, N.N.A., Talib, S. & Mahmud, M. (2016), November. Information Security Behavior among Employees from the Islamic Perspective. In *Information and Communication Technology for The Muslim World (ICT4M), 2016 6th International Conference on* (pp. 211-215). IEEE.

Bendovschi, A.C. & Ionescu, B.Ş. (2015). The Gap between Cloud Computing Technology and the Audit and Information Security. *Audit Financiar*, *13*(125).

Beris, O., Beautement, A. & Sasse, M.A. (2015). Employee rule breakers, excuse makers and security champions:: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 73-84). ACM.

Bhattacharjee, J., Sengupta, A., Mazumdar, C. & Barik, M.S., (2012). A two-phase quantitative methodology for enterprise information security risk analysis. In *Proceedings of the CUBE International Information Technology Conference* (pp. 809-815). ACM.

Borins, S. (2001). Encouraging innovation in the public sector. *Journal of intellectual capital*, *2*(3), pp.310-319.

Breier, J. & Hudec, L. (2011). Risk analysis supported by information security metrics. In *Proceedings of the 12th International Conference on Computer Systems and Technologies* (pp. 393-398). ACM.

Bryman, A & Bell, E. (2011). Ethics in business research. Oxford University Press. London Available at: https://www.utwente.nl/en/bms/research/forms-and-downloads/bryman-bell-2007-ethics-in-business-research.pdf (Accessed 28 September 2018)

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), pp.523-548.

Buthelezi, M.P., Van Der Poll, J.A. & Ochola, E.O. (2016). Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis. In *Computational Science and Computational Intelligence (CSCI), 2016 International Conference on* (pp. 1360-1367). IEEE.

Carmeli, A. & Spreitzer, G.M. (2009). Trust, connectivity, and thriving: Implications for innovative behaviors at work. *The Journal of Creative Behavior*, *43*(3), pp.169-191.

Chang, S. E. & Lin, C. (2007). "Exploring organizational culture for information security management", Industrial Management & Data Systems, Vol. 107 Issue: 3, pp.438-458, https://doi.org/10.1108/02635570710734316

Chang, S.J., Van Witteloostuijn, A. & Eden, L. (2010). From the editors: Common method variance in international business research.

Chawla, S. & Thamilarasu, G. (2018) April. Security as a service: real-time intrusion detection in internet of things. In *Proceedings of the Fifth Cybersecurity Symposium* (p. 12). ACM.

Chmura, J. (2016). "*The impact of positive organisational culture values on information security management in the company"*. Journal of Positive Management, [S.l.], v. 7, n. 1, p. 87-98, sep. 2016. ISSN 2392-1412. Available at: <http://apcz.umk.pl/czasopisma/index.php/JPM/article/view/JPM.2016.006>. Date accessed: 11 Oct. 2017.

Chuang, L.M. (2007). The social psychology of creativity and innovation: Process theory (PT) perspective. *Social Behavior and Personality: an international journal*, *35*(7), pp.875-888.

Conteh, N.Y. & Schmick, P.J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), p.31.

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. In *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35-41). ACM.

Crossan, M.M. & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of management studies*, *47*(6), pp.1154-1191.

Da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49():162–176. http://dx.doi.org/10.1016/j.cose.2014.12.006. [April 10, 2015].

Da Veiga, A. (2008). Cultivating and Assessing Information Security Culture. University of Pretoria

Dai, F., Shi, Y., Meng, N., Wei, L. & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In *Systems and Informatics (ICSAI), 2017 4th International Conference on* (pp. 975-979). IEEE.

Desai, M.R. (2016). *An integrated approach for information security compliance in a financial services organisation*(Doctoral dissertation, Cape Peninsula University of Technology).

Diener, E. & Crandall, R. (1978). *Ethics in social and behavioral research*. U Chicago Press.

Eickholt, J. & Shrestha, S. (2017). Teaching big data and cloud computing with a physical cluster. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (pp. 177-181). ACM.

Ekelhart, A., Fenz, S. & Neubauer, T. (2009). Aurum: A framework for information security risk management. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1-10). IEEE.

Farooq, M.U., Waseem, M., Khairi, A. & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

Feng, N., Wang, H.J. & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, *256*, pp.57-73.

Fenz, S. & Ekelhart, A. (2009). Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security* (pp. 183-194). ACM.

Forni, A. A., & van der Meulen, R. (2017). Gartner Says Artificial Intelligence Could Turn Some Skilled Practices Into Utilities. Available at https://www.gartner.com/en/newsroom/press-releases/2017-05-09-gartner-says-artificia-intelligence-could-turn-some-skilled-practices-into-utilities [Accessed 13 December 2018]

Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Richardson, D. & Zorn, B. (2017). *Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things*. Technical Report. Computing Community Consortium.

Gan, W., Lin, J.C.W., Fournier-Viger, P., Chao, H.C. & Zhan, J. (2017). Mining of frequent patterns with multiple minimum supports. *Engineering Applications of Artificial Intelligence*, *60*, pp.83-96.

Gartner, Inc. (2018). Blockchain Technology Spectrum: A Gartner Theme Insight Report. Available from: https://www.gartner.com/doc/3891399?plc=ddp [Accessed 26 October 2018]

Gartner, Inc. (2018). Top Strategic Predictions for 2018 and Beyond: Pace Yourself, for Sanity's Sake. Available from: https://www.gartner.com/document/3803530?ref=SiteSearch&sthkw=cybersecurity&fnl=search&srcId=1-3478922254 [Accessed 26 October 2018]

Gide, E. & Sandu, R. (2015). A study of the current situation of adoption of Cloud based services in Indian SMEs.".

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, *21*(2), pp.135-146.

Gouws, T. & Rheede van Oudtshoorn, G.P. (2011). Correlation between brand longevity and the diffusion of innovations theory. *Journal of Public affairs*, *11*(4), pp.236-242.

Grobler, M., van Vuuren, J.J. & Leenen, L. (2012) September. Implementation of a cyber security policy in south africa: Reflection on progress and the way forward. In *IFIP International Conference on Human Choice and Computers*(pp. 215-225). Springer, Berlin, Heidelberg.

Gulec, U., Yilmaz, M., Isler, V., O'Connor, R.V. & Clarke, P. (2018). Adopting virtual reality as a medium for software development process education. In *Proceedings of the 2018 International Conference on Software and System Process*(pp. 71-75). ACM.

György, A.A.B., Cleven, A., Uebernickel, F. & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation.

Hagen, J., Albrechtsen, E. & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information management & computer security*, *19*(3), pp.140-154.

Hallová, M, Polakovič, P, Virágh, R, & Slováková, I. (2017). Information Security and Risk Analysis in Companies of Agriresort, Agris On-Line Papers In Economics & Informatics, 9, 1, pp. 49-55, Academic Search Complete, EBSCOhost

Hart, C. (2018). *Doing a Literature Review: Releasing the Research Imagination*. Sage.

Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A. & Khan, S.U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, *47*, pp.98-115.

Hashizume, K., Rosado, D. G., Fernandez-Medina, E. & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*. 4(5), pp.1-13. Available from http://www.jisajournal.com/content/4/1/5 [Accessed:27 September 2017]

Hill, V. & Lee, H.J. (2010). Libraries and museums in virtual worlds: Adoption of immersive learning environments. In *Virtual Systems and Multimedia (VSMM), 2010 16th International Conference on* (pp. 386-389). IEEE.

Hina, S. & Dominic, D.D. (2017). Need for information security policies compliance: A perspective in Higher Education Institutions. In *Research and Innovation in Information Systems (ICRIIS), 2017 International Conference on* (pp. 1-6). IEEE.

Hlatshwayo, M. & Adeyelure, T.S. (2018). Deployment of Environmental Management Systems in South African Small and Medium Enterprises. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1-4). IEEE.

Hogan, S.J. & Coote, L.V. (2014). Organizational culture, innovation, and performance: A test of Schein's model. *Journal of Business Research*, *67*(8), pp.1609-1621.

Hu, Q., Dinev, T., Hart, P. & Cooke, D., (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

Hutcheson, G. and Sofroniou, N. (1999), The multivariate social scientist. London: Sage.

Hwang, K, & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism, Government Information Quarterly, 34, 2, pp. 183-198, *Library, Information Science & Technology Abstracts, EBSCOhost*

International Data Corporation, (2018). Augmented Reality and Virtual Reality are on the verge of growth. Available from: https://www.idc.com/getdoc.jsp?containerId=prUS44001618 [Accessed 23 November 2018]

Joubert, J. (2016). *Embedding risk management within new product and service development of an innovation and risk management framework and supporting risk processes, for effective risk mitigation: an action research study within the Information and Communication Technology (ICT) Sector* (Doctoral dissertation, University of Cape Town).

Jouini, M. & Rabai, L.B.A. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science*, *83*, pp.1084-1089.

Kaiser, H.F. (1974). An index of factorial simplicity. Psychometrika, 39, 31-36

Kalof, L., Dan, A. & Dietz, T. (2007). Essentials of social research, Open university press

Kaminski, J. (2011). Diffusion of innovation theory. Canadian Journal of Nursing Informatics, 6(2), pp.1-6.

Ketel, M. (2008). IT security risk management. In *Proceedings of the 46th Annual Southeast Regional Conference on XX* (pp. 373-376). ACM.

Khastar, H., Kalhorian, R., Khalouei, G.A. & Maleki, M. (2011). Levels of Analysis and Hofstede's Theory of Cultural Differences: The Place of Ethnic Culture in Organizations. In *International conference on financial management and economics* (Vol. 11, pp. 320-323).

Khazanchi, S, Lewis, M, & Boyer, K. (2007). Innovation-supportive culture: The impact of organizational values on process innovation, Journal Of Operations Management, 25, 4, pp. 871-884, Inspec, EBSCOhost

Kraha, A., Turner, H., Nimon, K., Zientek, L. & Henson, R. (2012). Tools to support interpreting multiple regression in the face of multicollinearity. *Frontiers in psychology*, *3*, p.44.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Springer.

Lakovleva, T.A. (2013). Open innovation at the root of entrepreneurial strategy: A case from the Norwegian oil industry.

Leedy, P. & Ormrod, J. (2005). Practical research: Planning and design, Prentice Hall, New Jersey

Li, S., Da Xu, L. & Zhao, S. (2018). 5G internet of things: A survey. *Journal of Industrial Information Integration*.

Liu, L. & Xu, B. (2018). Research on information security technology based on blockchain. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 380-384). IEEE.

Lomas, L. (2011). Information Security Risk Management: Handbook for ISO/IEC 27001, *Records Management Journal*, Vol. 21 Issue: 3, pp.239-240

Luqman, A. & Abdullah, N.K. (2011). E-business adoption amongst SMEs: a structural equation modeling approach. *Journal of Internet Banking and Commerce*, 16(2), p.1.

Lynch, P., Walsh, M.M. & Harrington, D. (2010). Defining and dimensionalizing organizational innovativeness.

Lyu, M.R. (2018). AI Techniques in Software Engineering Paradigm. In *ICPE* (p. 2).

Martin, R.A. (2003). Integrating your information security vulnerability management capabilities through industry standards (CVE&OVAL). In *Systems, Man and Cybernetics, 2003. IEEE International Conference on* (Vol. 2, pp. 1528-1533). IEEE.

Matsebula, F. & Mnkandla, E. (2016). Information systems innovation adoption in higher education: Big data and analytics. In *Advances in Computing and Communication Engineering (ICACCE), 2016 International Conference on* (pp. 326-329). IEEE.

Matveev, A.V. (2002). The advantages of employing quantitative and qualitative methods in intercultural research: Practical implications from the study of the perceptions of intercultural communication competence by American and Russian managers. *Theory of communication and applied communication*, *1*(1), pp.59-67.

McCall, T., & Van der Meulen, R. (2018). Gartner Says Nearly Half of CIOs Are Planning to Deploy Artificial Intelligence. Available at https://www.gartner.com/en/newsroom/press-releases/2018-02-13-gartner-says-nearly-half-of-cios-are-planning-to-deploy-artificial-intelligence [Accessed 13 December 2018]

McGill, M., Boland, D., Murray-Smith, R. & Brewster, S. (2015). A dose of reality: Overcoming usability challenges in vr head-mounted displays. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2143-2152). ACM.

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication and Ethics in Society*, *14*(3), pp.254-271.

Mulgan, G. & Leadbeater, C. (2013). Systems innovation. *London: Nesta*.

Myers, S.A., Zhu, C. & Leskovec, J. (2012). Information diffusion and external influence in networks. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 33-41). ACM.

Nechaev, A.S., Ognev, D.V. & Antipina, O.V. (2017). Analysis of risk management in innovation activity process. In *" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS), 2017 International Conference* (pp. 548-551). IEEE.

Nel, F. (2017). Determining a standard for information security culture. University of Pretoria

Nicho, M., Khan, S. & Rahman, M.S.M.K. (2017). Managing Information Security Risk Using Integrated Governance Risk and Compliance. In *Computer and Applications (ICCA), 2017 International Conference on* (pp. 56-66). IEEE.

Njenga, K. (2017). Understanding internal information systems security policy violations as paradoxes. *Interdisciplinary Journal of Information, Knowledge, and Management,* 12, 1-15.

Nograšek, J., & Vintar, M. (2014). E-government and organisational transformation of government: Black box revisited? Government Information Quarterly, 31(1), 108–118.

Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in health sciences education*, *15*(5), pp.625-632.

Noruzy, A., Dalfard, V.M., Azhdari, B., Nazari-Shirkouhi, S. & Rezazadeh, A. (2013). Relations between transformational leadership, organizational learning, knowledge management, organizational innovation, and organizational performance: an empirical investigation of manufacturing firms. *The International Journal of Advanced Manufacturing Technology*, *64*(5-8), pp.1073-1085.

Nzabahimana, J.P. (2018). Analysis of security and privacy challenges in Internet of Things. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 175-178). IEEE.

Omidosu, J. & Ophoff, J., (2016). A theory-based review of information security behavior in the organization and home context. In *Advances in Computing and Communication Engineering (ICACCE), 2016 International Conference on* (pp. 225-231). IEEE.

Opazo, B., Whitteker, D. & Shing, C. (2017). Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help. 13th International conference on natural computation.

Ozdemir, Z.D., Benamati, J.H. & Smith, H.J. (2016). A cross-cultural comparison of information privacy concerns in Singapore, sweden and the united states. In *Proceedings of the 18th Annual International Conference on Electronic Commerce: e-Commerce in Smart connected World* (p. 4). ACM.

Pan, J. & Yang, Z. (2018) Cybersecurity Challenges and Opportunities in the New Edge Computing + IoT World. In *Proceedings of the 2018 ACM International*

Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 29-32). ACM.

Parsons, R.A., (2015). The impact of age on innovation. *Management Research Review*, *38*(4), pp.404-420.

Patil, V.H., Singh, S.N., Mishra, S. & Donavan, D.T. (2008). Efficient theory development and factor retention criteria: Abandon the 'eigenvalue greater than one'criterion. *Journal of Business Research*, *61*(2), pp.162-170.

Pieters, W. (2011). 'The (Social) Construction of Information Security', Information Society, 27, 5, pp. 326-335, Academic Search Complete, EBSCOhost,

Pieterse, A.N., Van Knippenberg, D., Schippers, M. & Stam, D. (2010). Transformational and transactional leadership and innovative behavior: The moderating role of psychological empowerment. *Journal of organizational behavior*, *31*(4), pp.609-623.

Pinheiro, F.S. & Júnior, W.R. (2016). INFORMATION SECURITY AND ISO 27001. *Revista de Gestão & Tecnologia*, *3*(3).

Pisano, G.P. (2015). You need an innovation strategy. *Harvard Business Review*, *93*(6), pp.44-54.

Rawat, D.B. & Alshaikhi, A. (2018). Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints. In *2018 International Conference on Computing, Networking and Communications (ICNC)* (pp. 332-336). IEEE.

Rigby, D. & Zook, (2002). Open-market innovation. *Harvard business review*, *80*(10), pp.80-93.

Riikkinen, M., Saarijärvi, H., Sarlin, P. & Lähteenmäki, I. (2018). Using artificial intelligence to create value in insurance. *International Journal of Bank Marketing*.

Rogers, E. (1995). Diffusion of Innovation: modifications of a model for telecommunications. Die Diffusion von Innovationen in der Telekommunikation, pp.25-38.

Rusli, A., & Ali, N. A. (2003). The use of cognitive mapping technique in management research: theory and practice. Journal: Management Research News, Volume 26, Issue 7, pp.1-16

Santos, J.R.A. (1999). Cronbach's alpha: A tool for assessing the reliability of scales. *Journal of extension*, *37*(2), pp.1-5.

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students* (6th ed). London: Prentice Hall.

Savaglia, J., & Ping Wang. (2017). 'Cybersecurity vulnerability analysis via virtualization', Issues in Information Systems, vol. 18, no. 4, pp. 91-98.

Seale, T. (2017). *Factors influencing the decision to adopt an Information Technology Risk Management framework at universities in South Africa*. University of Cape Town.

Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research*, *3*(7), pp.749-752.

Shubin, O., & Gladkyy, M. (2013). 'Organisational culture as a socio-economic phenomenon in the context of the modern management paradigm', Problems Of Economy, 3, pp. 239-246.

Singh, A.K., Shafique, M., Kumar, A. & Henkel, J. (2013). Mapping on multi/many-core systems: survey of current and emerging trends. In *Design automation conference (dac), 2013 50th acm/edac/ieee* (pp. 1-10). IEEE.

Srivastava, S., Bisht, A. & Narayan, N. (2017). Safety and security in smart cities using artificial intelligence—A review. In *Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on* (pp. 130-133). IEEE.

Stewart, H. & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), pp.494-534.

Stewart, J. & Subramaniam, N. (2010). Internal audit independence and objectivity: emerging research opportunities. *Managerial auditing journal*, *25*(4), pp.328-360.

Sung, W. & Kang, S. (2017). An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness. In *Proceedings of*

the 18th Annual International Conference on Digital Government Research (pp. 84-93). ACM.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education. 2011; 2:53-55. DOI: 10.5116/ijme.4dfb.8dfd

Tellis, G.J., Prabhu, J.C. & Chandy, R.K. (2009). Radical innovation across nations: The preeminence of corporate culture. *Journal of marketing*, *73*(1), pp.3-23.

Thierer, A.D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Rich. JL & Tech., vol. 21, pp. 6–15, 2015.

Thompson, R. E., (2016). Cybersecurity: Getting Proactive about Data Vulnerability. *Fla. BJ*, *90*, p.36.

Toumpalidis, I., Cheliotis, K., Roumpani, F., & Hudson-Smith, A. (2018). VR Binoculars: an immersive visualization framework for IoT data streams. IET Digital Library, pp.39 (7 pp.). DOI:10.1049/cp.2018.0039

Tu, Y.K., Kellett, M., Clerehugh, V., & Gilthorpe, M.S. (2005). Problems of correlations between explanatory variables in multiple regression analyses in the dental literature. *British dental journal*, *199*(7), p.457. DOI:10.1038/sj.bdj.4812743

Tuli, F. (2010). The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives. *Ethiopian Journal of Education and Sciences*, *6*(1).

van Niekerk, J.C., & von Solms, R. (2003) Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach, in Proceedings of ISSA 2003, 3rd Annual IS South Africa Conference, Johannesburg, South Africa, 9-11 July 2003.

Varol, M. (2011). Assessment of heavy metal contamination in sediments of the Tigris River (Turkey) using pollution indices and multivariate statistical techniques. *Journal of Hazardous Materials*, *195*, pp.355-364.

Vermesan, O., Eisenhauer, M., Sunmaeker, H., Guillemin, P., Serrano, M., Tragos, E.Z., Valino, J., van der Wees, A., Gluhak, A. & Bahr, R. (2017). Internet of Things Cognitive Transformation Technology Research Trends and Applications. *Cognitive Hyperconnected Digital Transformation; Vermesan, O., Bacquet, J., Eds*, pp.17-95.

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal*, *15*(4), pp.407-426.

Von Schomberg, R. (2011). Towards responsible research and innovation in the information and communication technologies and security technologies field

Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P. and Hai, H.D. (2018). Recent challenges, trends, and concerns related to IoT security: An evolutionary study. In *Advanced Communication Technology (ICACT), 2018 20th International Conference on* (pp. 405-410). IEEE.

Waheed, M., Kaur, K., Ain, N. & Sanni, S.A. (2015). Emotional attachment and multidimensional self-efficacy: extension of innovation diffusion theory in the context of eBook reader. *Behaviour & Information Technology*, *34*(12), pp.1147-1159.

Wall, J.D. & Singh, R. (2018). The Organization Man and the Innovator: Theoretical Archetypes to Inform Behavioral Information Security Research. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(1), pp.67-80.

Wang, C., (2011), November. Application of virtual reality technology in digital tourism. In *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on* (pp. 537-541). IEEE.

Ward, V. (2018). AI could spot eye disease more accurately than doctors, study suggests. *The Telegraph.* Available from https://www.telegraph.co.uk/news/2018/02/05/ai-could-spot-eye-disease-better-doctors-study-suggests/ [Accessed 12 November 2018]

Whitman, M.E. and Mattord, H.J. (2012). *Roadmap to information security: For IT and infosec managers*. Cengage Learning.

Williams, B., Onsman, A. and Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine*, *8*(3).

Witt, M. & Robra-Bissantz, S. (2012). Sparking Motivation and Creativity with" Online Ideation Games". In *GI-Jahrestagung* (pp. 1006-1023).

XIao-yang, Y. (2011). Study on Development of Information Security and Artificial Intelligence. In *Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on* (Vol. 1, pp. 248-250). IEEE.

Yarwood, G.A. (2011). The pick and mix of fathering identities. *Fathering: A Journal of Theory, Research, and Practice about Men as Fathers*, *9*(2).

Yeh-Yun Lin, C. & Liu, F.C. (2012). A cross-level analysis of organizational creativity climate and perceived innovation: The mediating effect of work motivation. *European Journal of Innovation Management*, *15*(1), pp.55-76.

Yong, A.G. & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in quantitative methods for psychology*, *9*(2), pp.79-94.

Yoo B, Donthu N, & Lenartowicz T. (2011). Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. Journal of International Consumer Marketing. 2011 May 1;23(3-4):193-210.

Zamanzadeh, V., Ghahramanian, A., Rassouli, M., Abbaszadeh, A., Alavi-Majd, H. & Nikanfar, A.R. (2015). Design and implementation content validity study: development of an instrument for measuring patient-centered communication. *Journal of caring sciences*, *4*(2), p.165.

Zhai, C. (2011). B2B e-marketplace adoption in China: From the perspective of innovation diffusion theory and network externalities. In *Service Systems and Service Management (ICSSSM), 2011 8th International Conference on*(pp. 1-5). IEEE.

Zhang, X., Yu, P., Yan, J. & Spil, I.T.A. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: a case study in a primary care clinic. *BMC health services research*, *15*(1), p.71.

Zhao, Z., & Dai, Y. (2012). A New Method of Vulnerability Taxonomy Based on Information Security Attributes. In *Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on* (pp. 739-741). IEEE.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), pp.583-592. Available from: http://www.sciencedirect.com/science/article/pii/S0167739X10002554 [Accessed 3 August 2018]

Zyskind, G. & Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

ANNEXURE A: SURVEY QUESTIONNAIRE

QUESTIONS RESPONSES 185

Section 1 of 9

Survey Questionnaire

This questionnaire is designed to obtain feedback from you regarding your experience and perception of information systems adoption and information security risks. The results from this survey will be used establish whether there is a relationship between antecedents of systems innovation and information security risks.

Taking part in this survey is completely voluntary and anonymous, you may at any stage, without prejudice, withdraw your consent and participation in the study. The questionnaire consists of 9 sections and should take no more than 15 minutes to complete.

To participate on this questionnaire, click on the appropriate option where applicable or complete where required. Please ensure that you complete all the questions and that you participate only once. When evaluating a question please answer from your own perspective.

Thank you for taking time to complete this survey. Should you have any questions please feel free to contact Steven Botsime on 011 689 3880 or botsimems@gmail.com

I have been informed of consent and declare myself prepared to participate in the study. *

- ◯ I Agree

Section 2 of 9

SECTION A: DEMOGRAPHIC DETAILS

The purpose of this section is to gather demographic information which will be used in testing the validity and reliability of the data as well to analyse the relationship with other variables.

1. Which title best describes your area of work? *

- Chief Information Officer
- Information Security
- IT Governance Specialist
- Systems/Web Developer
- Business Analyst
- Systems Analyst
- IT Consultant
- Network Specialist
- IT Student
- Information Management Specialist
- Server Administration
- Database Administrator
- IT Support
- Help Desk Operator
- Other...

2. What is your Level of Employment? *

- ○ Intern
- ○ Admin
- ○ Technical/Functional Level
- ○ Middle Management
- ○ Top Management
- ○ Other...

3. How long have you been working with Information Systems? *

- ○ 0 – 3 Years
- ○ 4 – 7 Years
- ○ 8 – 10 Years
- ○ > 11 Years

4. What is your Level of Education? *

- ○ Matric/ Grade 12
- ○ National Diploma
- ○ Bachelors or BTech
- ○ Honours
- ○ Masters
- ○ Doctoral
- ○ Other...

5. In which sector is your organisation? *

- Public Sector
- Private Sector
- Parastatal
- Non-Proffit Organisation (NPO)

Section 3 of 9

SECTION B: RELATIVE ADVANTAGE

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

RA1. I'm likely to use a new system if it functions better than an existing one. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

RA2. New systems are likely to enhance productivity better than old ones. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

RA3. New systems are more likely to be aligned to my work compared to old ones. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

RA4. I work faster when using new systems compared to older ones. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

RA5. I'm likely to adopt a new system if it "looks" and "feels" better than old ones. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

Section 4 of 9

SECTION C: COMPLEXITY

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

C1. I'm likely to continue using a new system if it is user friendly. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

C2. I'm likely to keep using a new system if it simplifies my work. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

C3. I'm discouraged to continue using a new system if I do not know how it works. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

C4. It is easier to adopt a new system if it does not give frequent errors. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

C5. I often consult a user manual when using a new system. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

Section 5 of 9

SECTION D: INDIVIDUAL FACTORS

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

IF1. I'm just not motivated to use new systems. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

IF2. I don't have enough technical skills to be able to use new systems. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

IF3. I generally don't understand how new systems work. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

IF4. I often need training before I can effectively use new systems. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

IF5. I just don't like fiddling with new systems and technology. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

Section 6 of 9

SECTION E: ORGANISATIONAL FACTORS

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

OF1. Organisational policies place restrictions on how systems can be used *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

OF2. My organisation does not invest enough on development of new systems. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

OF3. The current organisational culture does not support systems innovation. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

OF4. Organisational dynamics and politics often gets in the way of systems innovation. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

OF5. There is currently no need for the organisation to introduce new systems. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

Section 7 of 9

SECTION F: ENVIRONMENTAL FACTORS

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

EF1. My organisation has introduced new systems to keep up with industry technology advancements. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

EF2. Changes in government regulations have led to the introduction of new systems. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

EF3. My organisation has introduced new systems because of pressure from competitors and customers. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

EF4. New systems were introduced to enhance organisational competitiveness. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

EF5. Systems innovation has assisted my organisation to comply to regulations. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

Section 8 of 9

SECTION G: INFORMATION SECURITY RISKS

On scale of 1 to 5 where 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Disagree nor Agree, 4 = Agree and 5 = Strongly Agree, indicate the extent to which you agree with the following statements.

SR1. New systems bring new security threats in to the environment. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

SR2. Rapid adoption of new systems often increases system vulnerabilities. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

SR3. System innovation is likely to cause non-compliance with information security policies. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

SR4. New systems are more vulnerable to data leaks. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

SR5. Access rights are often not correctly assigned in new systems. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

Section 9 of 9

SECTION H: SYSTEMS INNOVATION

On scale of 1 to 5 where 1 = Not At All, 2 = Small Extent, 3 = Some Extent, 4 = Large Extent and 5 = Very Great Extent, indicate the extent to which you agree with the following statements.

SI1. To what extent has your organisation adopted the following technologies? *

	Not at All	Small Extent	Some Extent	Large Extent	Very Great Extent
Blockchain	○	○	○	○	○
Internet of Things	○	○	○	○	○
Big Data\Cloud C...	○	○	○	○	○
Artificial Intelligen...	○	○	○	○	○
Virtual Reality\Au...	○	○	○	○	○

SI2. My organisation has used the above systems/technologies to solve problems. *

- ○ Strongly Disagree
- ○ Disagree
- ○ Neither Disagree nor Agree
- ○ Agree
- ○ Strongly Agree

SI3. The adoption of the above systems/technologies has increased efficiency. *

- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

SI4. My organisation has transformed due to the adoption of the above technologies. *

- Strongly Disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly Agree

SI5. Adoption of the above systems allows my organisation to meet it's business objectives. *

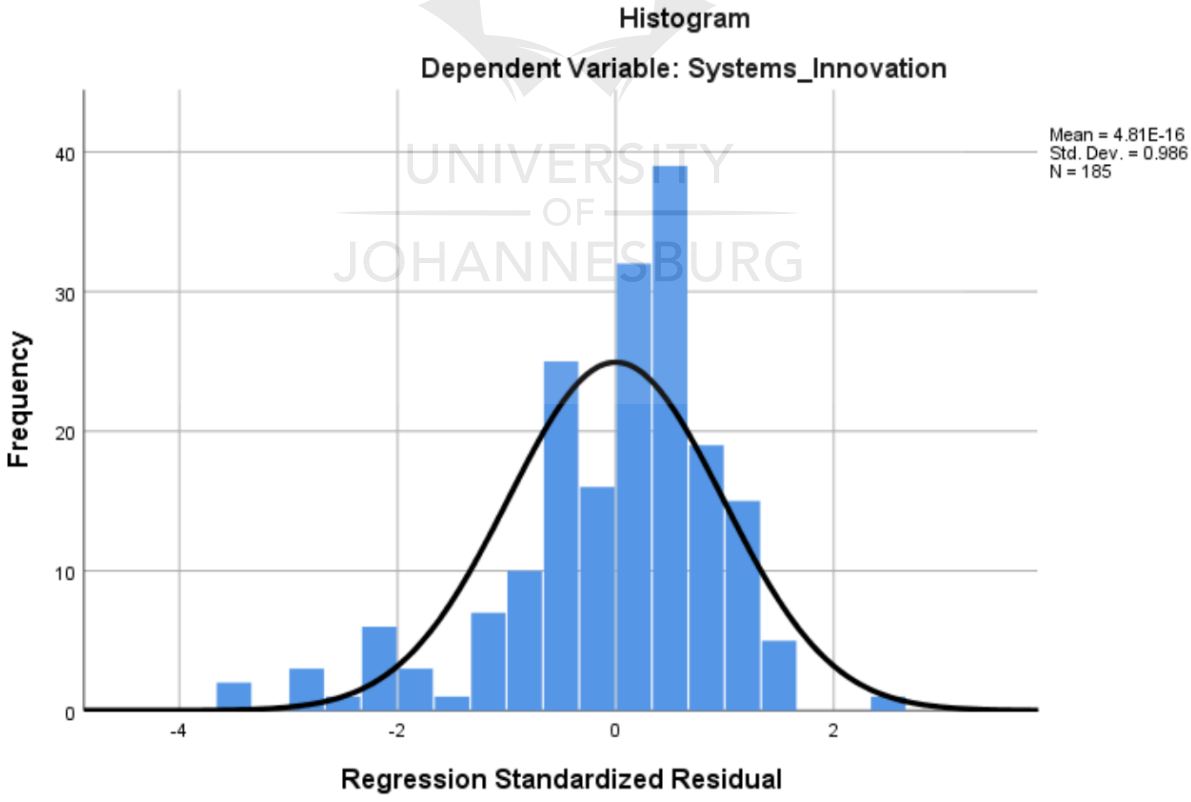
- Strongly disagree
- Disagree
- Neither Disagree nor Agree
- Agree
- Strongly agree

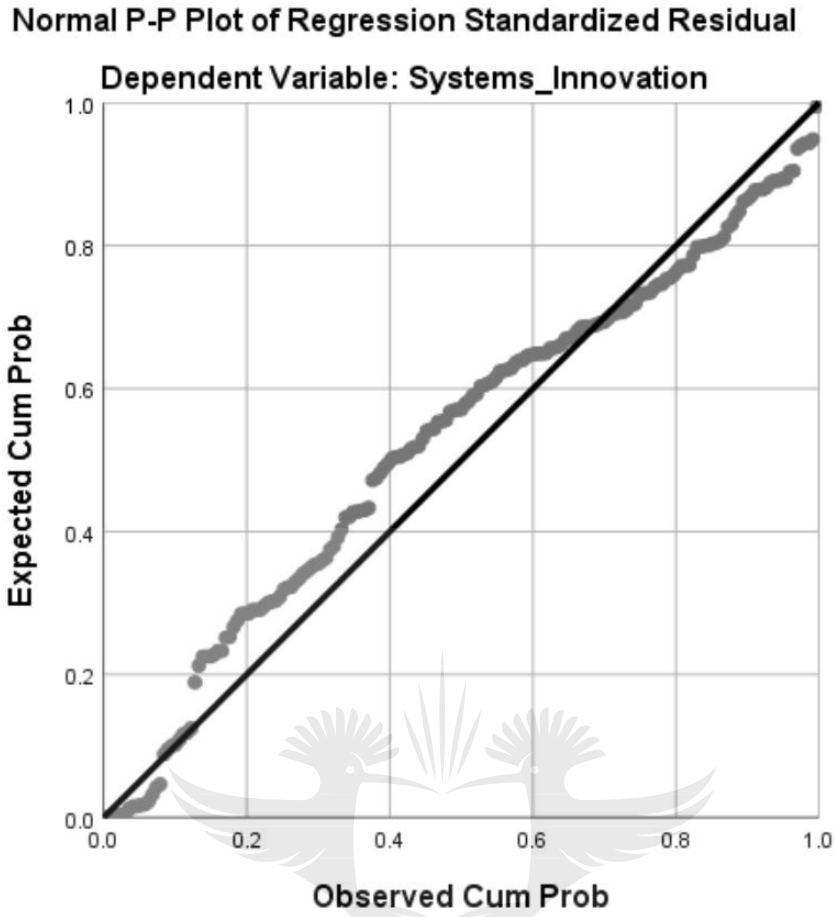
ANNEXURE B: RESIDUAL RESULTS

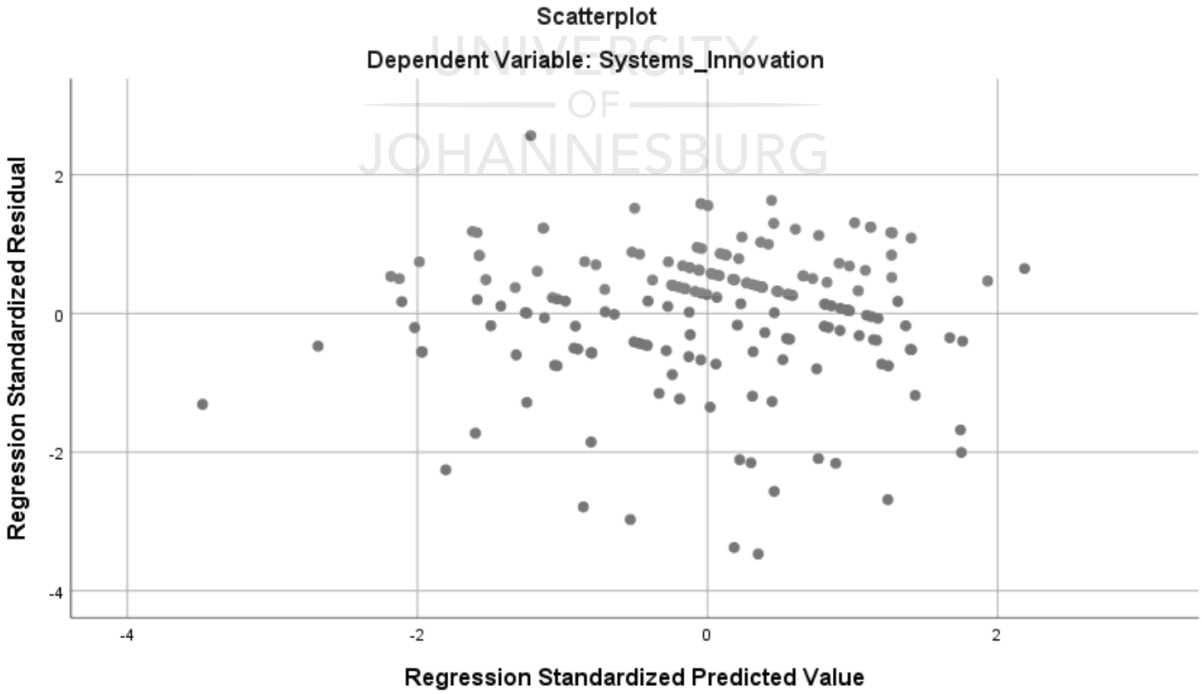
Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.0170	4.4968	3.5405	.43757	185
Std. Predicted Value	-3.482	2.185	.000	1.000	185
Standard Error of Predicted Value	.063	.313	.132	.047	185
Adjusted Predicted Value	2.1081	4.4776	3.5393	.43934	185
Residual	-2.69327	1.99267	.00000	.76556	185
Std. Residual	-3.470	2.567	.000	.986	185
Stud. Residual	-3.510	2.806	.001	1.008	185
Deleted Residual	-2.75593	2.38011	.00120	.79973	185
Stud. Deleted Residual	-3.627	2.862	-.002	1.018	185
Mahal. Distance	.213	28.957	4.973	4.937	185
Cook's Distance	.000	.255	.008	.023	185
Centered Leverage Value	.001	.157	.027	.027	185

a. Dependent Variable: Systems_Innovation



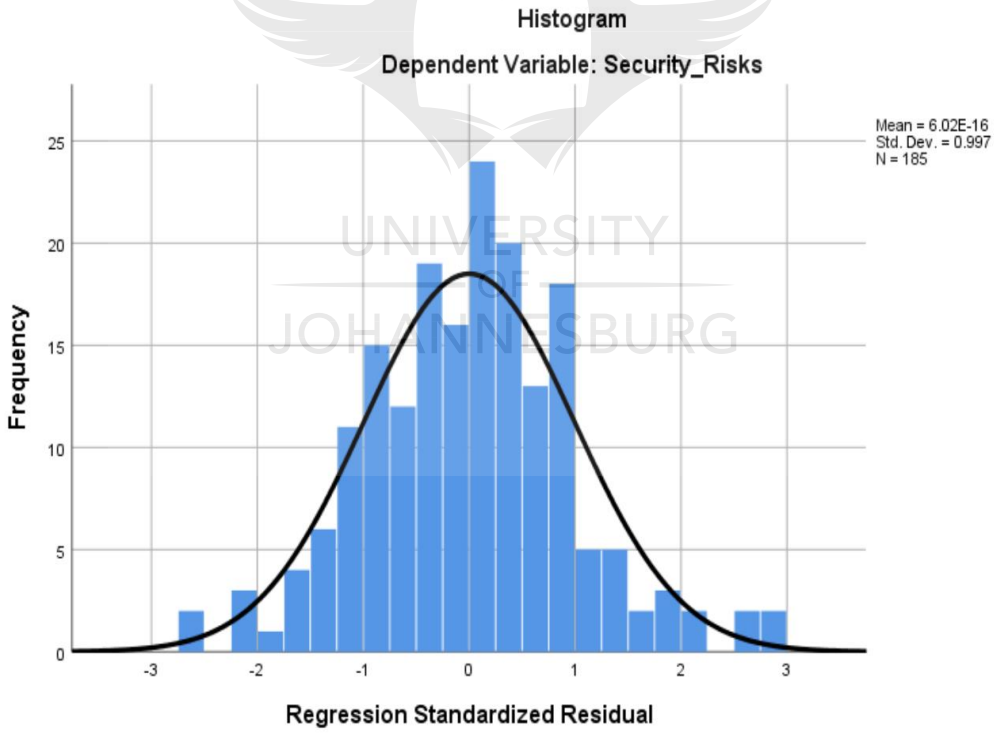


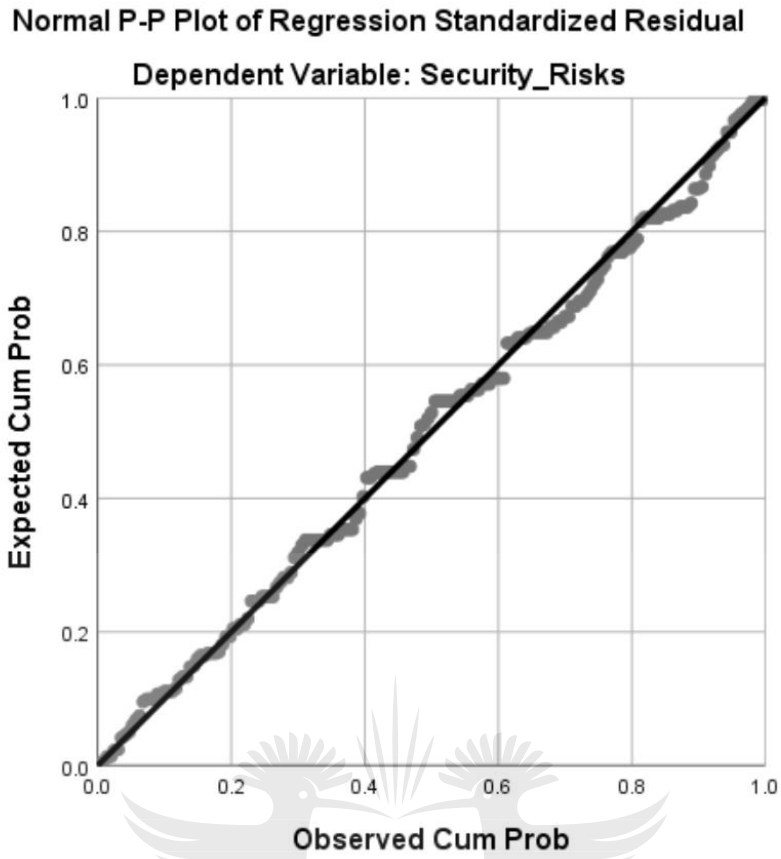


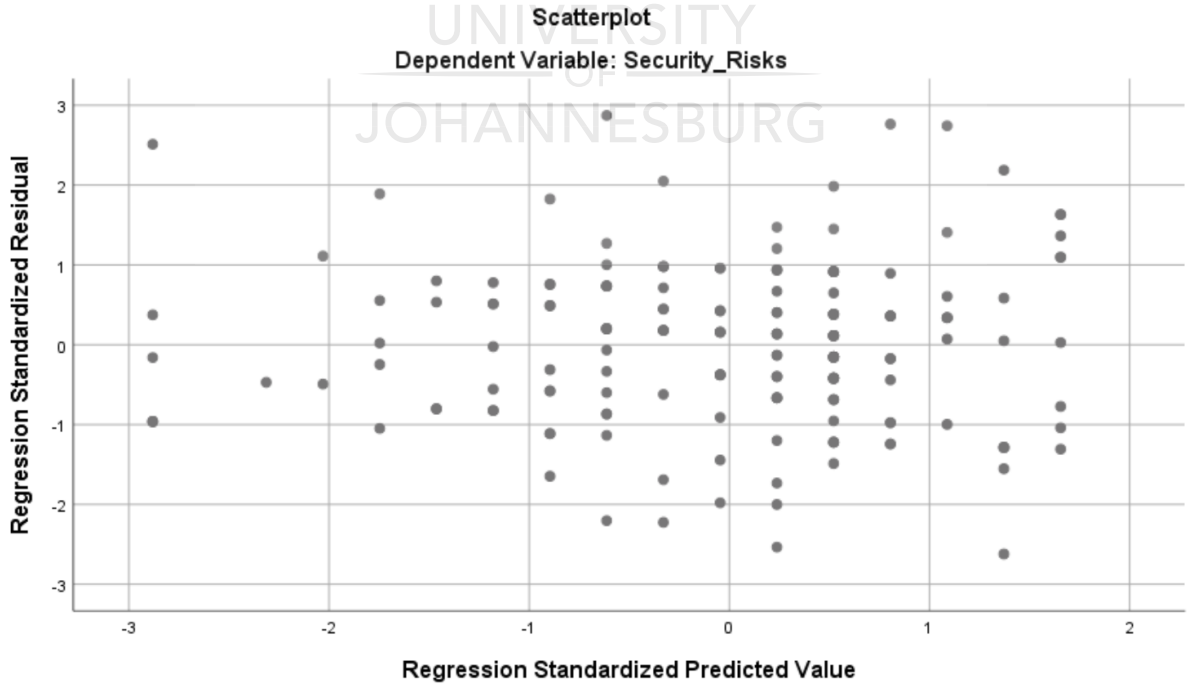
Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.7198	2.9789	2.8843	.05712	185
Std. Predicted Value	-2.881	1.655	.000	1.000	185
Standard Error of Predicted Value	.055	.168	.074	.024	185
Adjusted Predicted Value	2.6197	2.9991	2.8842	.05822	185
Residual	-1.96267	2.15069	.00000	.74660	185
Std. Residual	-2.622	2.873	.000	.997	185
Stud. Residual	-2.642	2.884	.000	1.003	185
Deleted Residual	-1.99383	2.16683	.00016	.75594	185
Stud. Deleted Residual	-2.687	2.943	.001	1.010	185
Mahal. Distance	.002	8.301	.995	1.643	185
Cook's Distance	.000	.177	.006	.015	185
Centered Leverage Value	.000	.045	.005	.009	185

a. Dependent Variable: Security_Risks







ANNEXURE C: LANGUAGE EDITING CERTIFICATE

EDITING CERTIFICATE

I hereby confirm that I have proof-read, formatted, and edited the style, layout, references, and language of the dissertation to be submitted to

College of Business and Economics: University of Johannesburg

by

Mogotsi Steven Botsime

entitled

Conceptualising antecedents of systems innovation on information security risks

Note: The edited work described here may not be identical to that submitted. The author, at its sole discretion, has the prerogative to accept, delete, or change amendments made by the editor before submission.

Signed: _____

Date: 30 January 2019

Professional EDITORS' Guild

Associate Member

Membership number: NTS001

Masetuka Ntsoereng
Director: Bohlale Info Solutions
email: stukks06@gmail.com
cell: 0720542144/0825641512

Language and technical editing
Text and layout formatting
Proofreading
Academic style formatting

www.editors.org.co.za www.bohlaleis.co.za