Investigating the Factors that Influence Digital Forensic Readiness in a South African Organisation

A Research Dissertation presented to

The Department of Information Systems

University of Cape Town

by

Mninawe Albert Mankantshu

(MNKMNI001)

In partial fulfilment of the requirements for Master of Commerce in Information Systems Degree (INF5004W)

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this dissertation "Investigating the Factors that Influence Digital Forensic Readiness in a South African Organisation", from the work(s) of other people has been attributed, and has been cited and referenced.

3. This dissertation "Investigating the Factors that Influence Digital Forensic Readiness in a South African Organisation", is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's work, or part of it, is wrong, and declare that this is our own work.

6. I have not falsified or manufactured any data, and declare that all data was ethically collected.

Signed by candidate

Signature:

Date: 29 May 2014

Signature Removed

Name: Mninawe Albert Mankantshu

Dedication

This thesis is dedicated in loving memory of my father who has since passed away, may his soul rest in peace. He was always very proud of my achievements in life.

Acknowledgements

The successful completion of this task would have never been possible without the support, advice, assistance and encouragement of others. I would like to record my sincere thanks and appreciation to the following:

Firstly I would like to thank my supervisor, Dr Jacques Ophoff, for his invaluable supervision, guidance and support. The journey has certainly been an enriching one, and I have gained much from his wisdom and insight.

Secondly thanks to Professor Mike Kyobe for his encouragement and guidance in my initial departure for this journey.

Thanks to all the UCT department of Information Systems staff whom I interacted with for guidance and advice.

Thanks to Annet Prinns for her administrative support and efficiency.

Thanks to my wife, Nokuzola Portia, and my daughters, Zenande and Azizipho, for their understanding, patience, encouragement and continued support.

Thank you also to my mother, brothers and sisters who have never stopped believing in me – God bless you!

And to all those who willingly gave of their time to be interviewed for this study, I am very grateful for your input; thank you.

Finally, I thank my Lord and Saviour Jesus Christ; without Him, I am nothing.

"The Lord is my Shepherd".

Mninawe Albert Mankantshu

Johannesburg

May 2014

Abstract

Computer crimes affect the bottom line of organisations across the globe. The ability of criminals to exploit organisational systems and avoid prosecution is a concern for most organisations. This is due to the increased use of information and communication technology (ICT) by individuals and organisations. The rapid growth of ICT has affected our communication and information exchange. These advances have not only influenced the way we conduct our daily activities, but has also led to new opportunities, risks and challenges for technical and legal structures. Unfortunately, some individuals and groups have decided to use these ICT advances in order to engage in criminal activities, such as cybercrime. The increase of cyber-related crimes puts a lot of pressure on law enforcement agencies and organisations across the globe to produce credible digital forensic evidence.

The rise in the number of fraudulent transactions and risks associated with ICT advances has also resulted in increased security awareness by both the public and private sectors. Some organisations have developed defensive as well as offensive strategies to deal with ICT security incidents. This process is referred to as digital forensic readiness. In order to enhance an organisation's capability to be digital forensic ready, certain proactive and reactive activities need to be performed by the organisation. Digital forensic readiness in an organisation is influenced by various factors. The identification of these factors could assist organisations to successfully design and implement a digital forensic ready environment.

The purpose of this study is two-fold: firstly, to investigate factors that influence digital forensic readiness in a South African organisation and secondly, to determine how and to what extent these factors influence digital forensic readiness in the organisation.

Case study data within an organisation was collected using two methodologies. Primary data included transcribed semi-structured personal interviews with employees of a large financial services organisation. Secondary data included existing literature on digital forensic readiness and data from the organisation's policy documents.

An extensive literature review revealed four primary factors influencing digital forensic readiness: corporate governance, forensic policy, legal and ethical requirements, as well as technology and infrastructure. Thematic analysis of the case study data indicated that

the four factors significantly influence digital forensic readiness. Another finding revealed differing opinions regarding the establishment of a digital forensic laboratory.

The most important recommendation resulting from this study is that, the South African organisation under study should establish a well-defined forensic policy that will mandate and provides guidelines for forensic investigations. The organisation should ensure more effort is given to cyber-crimes training and awareness. Another recommendation is that the organisation needs to ensure that their evidence meets legal requirements and that their legal professionals are trained in digital forensic procedures.

Table of Contents

Chapter 1: Introduction

Computer crimes have become a common problem in most organisations across the globe. The concern for these organisations is the ability of criminals to exploit systems and avoid prosecution. A number of international and local financial scandals, where investors and creditors lost huge amounts of money due to fraudulent activities, have been reported (PWC, 2009). Some of the cases are highlighted in the next section below.

1.1 Background

The extent of fraud cannot be underestimated as it impacts on the bottom line of companies. The need for organisation to limit such losses is inevitable. To illustrate the extent of this problem consider the following cases.

The first case is that of Fidentia, where funds were reported missing from the Fidentia Asset Management Group to the value of close to R1-billion (IOL new, 2008). In 2007, the company was placed under curatorship by the Financial Services Board (FSB). FSB inspectors claimed that the Fidentia group had misappropriated client funds and made numerous misrepresentations to clients. The man at the centre of the controversy was Fidentia's executive chairman, James Arthur Brown, who persuaded people to invest in his firm and is alleged to have squandered the R1,2 billion on a salary of R400 000 a month, by buying a Ferrari car, a palatial mansion, and soccer, rugby and cricket teams (IOL news, 2007).

The next case is that of increased fraud within the life insurance industry. The South Africa life insurance industry paid out life cover benefits of more than R175, 6 billion to life cover beneficiaries in 2009. A study that was conducted by PriceWaterhouse Coopers (PWC) in 2009 on life insurance fraudulent claims revealed that “economic crime has significantly been on rise” (Global Economic Crime Survey, 2011, p.3). PWC defines economic crime as is an illegal act (or constantly evolving set of acts), generally committed by deception or misrepresentation (fraud) by someone who has special professional or technical skills, for the purpose of personal gain or to gain an unfair advantage over another individual . Economic crimes include cybercrime, commercial crime, white collar crime, fraud and corruption (PWC, 2009).

A survey that was conducted by the Association for Savings and Investment South Africa (ASISA) in 2011 confirmed the trend in the life insurance industry (Fan News, 2011).

According to the ASISA, death and funeral claims were the largest contributors to insurance fraud statistics in South Africa. In 2011, the Association of Certified Fraud Examiners also conducted a study to try to understand and measure the impact of fraud on organisations. According to their findings, a typical organisation loses 5% of its annual revenue due to fraud (ACFE report 2010).

Information communication technology (ICT) has played a role in perpetuating this problem and making it harder to detect security incidents (KPMG survey, 2009). The rapid development of technology has enhanced the criminal's ability to perform, hide and/or assist in unlawful or unethical activity (Grobler and Louwrens, 2006). The rise in crimes committed using technology put a strain on law enforcement agencies and businesses. This has resulted in courts no longer requiring evidence to be paper-based, but also accepting digital evidence. This poses a challenge to normal forensic investigation, and the need for digital forensics became inevitable (Grobler and Louwrens, 2006). The need for organisations to obtain concrete digital evidence has become paramount for a successful criminal prosecution (Tushabe, 2004). In order to be successful in prosecuting the criminals, organisations need to perform certain proactive, active and reactive activities. This will enable them to be digitally forensic ready (Carrier and Spafford, 2003). Digital forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence while, at the same time, minimising the cost of an investigation (Rowligson, 2004).

1.2 Problem Statement and Research Questions

Despite various efforts to curb digital crimes in organisations across the globe, digital crimes continue to be on the increase. The literature promotes the proactive collection of digital evidence in order to increase the successful prosecution rate. Digital forensic readiness is seen as a direct response to the ever-changing environment of combating cyber-crime (Grobler and Louwren, 2007). Any organisation that underrates the need for digital forensic readiness might find itself unable to link the attacker to the forensic incident or lack sufficient evidence to prove a fraudulent transaction (Rowlingson, 2004). It is critical for companies to be digital forensic ready and be able to provide digital evidence whenever it is required by law enforcement agents (Grobler, 2010).

While South African organisations are perceived to be adopting certain elements of a digital forensic readiness program, not all are fully implementing or embracing it (Whyte,

etl.al.2010). To illustrate this, a certain life insurance company in the Western Cape has a fully-fledged and operational digital forensics laboratory on their premises, whereas some other organisations see this as an unnecessary cost to bear. A number of factors influence organisations' willingness to implement a digital forensics program.

The main research question is: What are the factors that influence the implementation of digital forensic readiness in a South African organisation? In addition to the main research question, the following two sub-questions are posed:

1. How do these factors influence digital forensic readiness in a South African organisation?
2. To what extent do these factors influence digital forensic readiness in a South African organisation?

1.3 Scope of the Research

Technology developments, such as internet, have resulted in companies being exposed to a number of criminal activities. According to the Global Economic Crime Survey (2009), life insurance companies are hardest hit by cyber-crime. The role players in South Africa include companies that provide short- and long-term insurance cover. Long-term insurance provides life cover and funeral covers. The long-term insurance industry is dominated by three players: Old Mutual, Sanlam, and MMI Holdings. MMI resulted from the merger of Metropolitan Life Insurance and Momentum Insurance. A single South African life insurance company has been identified and used as a case study for the purpose of this study.

Life insurance organisations in South African tend collect evidence after an incident has occurred and these results in huge financial losses. These organisations do not have a comprehensive approach to proactively collect evidence, and efforts to proactively gather evidence within these organisations are fragmented. The reason for this is that these organisations do not have a framework that will assist them in implementing a digital forensic program that will enhance their ability to proactively collect evidence. A practical aim of this study is to contribute to addressing this problem.

1.4 Rationale and Value of the Research

The business community around the world is greatly affected by digital crimes and is losing huge sums of money due fraudulent activities. South Africa's financial sector is not

immune to this problem and has been the victim of some these criminal activities. In order for organizations to be successful in reducing fraud and digital crimes, they need to be proactive and implement measures that will assist them in collecting and capturing digital evidence in advance; this process is regarded as digital forensic readiness (Rowlingson, 2004). Grobler, Louwren, and Von Solms (2010) noted that there is a need for organisations to have a comprehensive framework that will assist them in implementing a digital forensic readiness programme. In order to implement a successful digital forensic readiness program, organisations need to first understand the factors that influence digital forensic readiness.

The study seeks to identify the factors that influence digital forensic readiness in a South African organisation and to provide insight into how and to what extent these factors influence digital forensic readiness. This new insight will serve as a contribution to the information systems' body of knowledge.

The study will be of benefit to those involved in protecting an organisation's information assets, and in detecting and monitoring any security threats to the organisation; this includes the board of directors. The results of the study could assist South African companies to re-examine and update their existing digital forensic readiness initiatives.

1.5 Overview of the Dissertation

The dissertation is presented in several chapters. Chapter 1 provides an introduction by presenting an overview, problem statement, research questions, delineation, and rationale for conducting the study. The purpose of this chapter is to indicate the research problem and to provide an explanation why the study is worth conducting.

Chapter 2 provides a literature review of digital forensics, history and developments of digital forensics, definitions, and digital investigation methodologies. The chapter also looks at the concept of digital forensic readiness and its organisational aspect, motivations for implementing digital forensic readiness and costs of implementing it, drivers of digital forensic readiness, frameworks for implementing digital forensic readiness, and a proposed digital forensics readiness model that can be used by South African organisations in identifying the factors that needs to be considered when designing and implementing a digital forensic readiness program.

Chapter 3 provides a brief overview of the research philosophy and the research methodology. The purpose of this chapter is to explain how the research approach adopted is congruent with the nature and the aims of the research. The research methodology outlines the method, approach and strategy used by the researcher in collecting data , type of data collected, and instruments used in collecting that such data. It also enables the researcher to collect only data that is relevant to the study and draws the boundary for study. In addition, Chapter 3 outlines how ethical issues have been addressed by the researcher.

Chapter 4 provides an analysis and interpretation of the raw data. The chapter give a detailed description of the sample and empirical findings. The sample description indicates the type of participants and why they were selected for the study. The purpose of this chapter is also to make sense of the collected data and to confirm reality as experienced by the participants.

Chapter 5 concludes the study and provides a summary of the most significant findings of the study. This chapter also discusses the findings in the context of the literature of theory and the lessons learned from the findings. Chapter 5 serves to confirm whether or not the theory is contrary to reality. This chapter indicates what have been the contributions and the limitations of the study. This chapter also provides some recommendations for organisations based on the findings of the current study as well as what future study can focus on.

Chapter 2: Literature Review

In this chapter, an overview of digital forensics is presented. The chapter provides definitions as well as the history and development of digital forensics. An overview of digital forensic readiness and some definitions of digital forensic readiness are presented. The chapter provides a motivation for why organisations need to implement a digital forensic readiness program, costs of implementing digital forensic readiness, and drivers of digital forensic readiness within an organisation. A conceptual model has been developed to highlight significant factors that influence digital forensic readiness.

2.1 Digital forensics

The use of digital devices such as computers, cell phones and tablets has become ubiquitous in most communities. The increased use of these devices to commit fraud has triggered the need for organisations to conduct digital forensic investigations. These forensic investigations are referred to as digital forensics. Digital forensics is used by organisations for both criminal investigation and internal investigation, especially in cases where there are computer security breaches or electronic transaction disputes (Poope and Labuschagne, 2012).

2.1.1 Definition of Digital Forensics

There is no agreement on the definition of digital forensics; hence several definitions of this concept have been identified from the existing literature.

McKemmish (1999) defined forensic computing as the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.

Digital forensics is also defined as the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, and use of validated tools, repeatability, reporting, and proper expert witness presentation(Zatyko, 2007).

Grobler and Louwrens (2006) define digital forensics as the efficient use of analytical and investigative techniques for the preservation, identification, extraction, documentation , analysis and interpretation of computer media which is digitally stored or encoded for evidentiary and/or root cause analysis and presentation of digital evidence derived from digital sources for the purpose of facilitation of events found to be criminal or helping to

anticipate unauthorised action shown to be disruptive to planned operations. For the purpose of this study this definition has been adopted.

2.1.2 History and Development of Digital Forensic

Before the twentieth century, the courts in US relied on the 1923 common law Frye rule to base their judgements which never considered the scientific evidence as good enough to prosecute criminals (Scientific evidence& Forensics Science, 1993). In June 1993, the US Supreme Court handed down a landmark decision on admissibility of scientific evidence in a court of law (Scientific evidence& Forensics Science, 1993). The case involved the plaintiff, Daubert and Merrel Dow Pharmaceuticals Incorporation, over a dispute that the Merrel Dow product, called Benedictine which was alleged to be causing limb defects in children whose mothers used the product during pregnancy (Forensics Science Guide, 2001). After numerous deliberations, the Supreme Court unanimously agreed that the 1975 rules of evidence superseded the 1923 common law Fye rule and that scientific evidence should be used in a court law in the US (Forensics Science Guide, 2001).

During 1978, a number of computer crimes were recognised. At this time, crimes that involved the use of computers were dealt with by using traditional and existing laws. Until the 1980's, governments struggled to redefine the law to fit computer crimes; thus it was difficult to prosecute these cases (Florida Computer Crimes Act, 1978). The increase in computer crimes forced the US government to pass a law in order to deal with these crimes. In the state of Florida, for example, the first Computer Crimes Act was passed into law to deal with unauthorised modification or deletion of electronic data (Volonino and Anzaldua, 2008).

In late 1980's, US federal laws began to incorporate digital forensics. The FBI in the US started creating the Magnetic Media Program, which later became the Computer Analysis and Response Team (Volonino and Anzaldua, 2008). The first digital forensic investigation was that of Cliff Stoll who pursued the hacker, Markus Hess, in 1986. In his investigation, Stoll used computer and network forensic techniques to investigate the case. Although Stoll was not a specialised examiner, most of the forensic examinations since have followed this approach (Volonino and Anzaldua, 2008).

In 1993, the FBI hosted an international conference on computer evidence; the conference was attended by 70 representatives from various US federal agencies and

state representatives as well as international law enforcement agencies. It was at this conference where it was agreed that standard practice for computer forensics were lacking and that they needed to be improved and standardised. It was also during this period that audio and video technologies started moving from analogue to digital form. The computer forensic practitioners started to question whether the same principles of computer forensics should be applied all types of digital forensic evidence (Chatz, 1995).

In 1995, the International Organisation on Computer Evidence was formed. In 1996, the FBI conference was held again, this time in the Netherlands. In December1997, an international conference was held in Moscow and it was attended by the G8 countries. At this conference, it was declared that a law enforcement agency needed to be trained and equipped to address high tech crimes. The Scientific Working Group on Digital Evidence was subsequently formed in 1998(Palmer, 2001). The first academic work on digital forensics started during the 1980's and 1990's and it involved the likes of Collier and Spaul, Sommer and Spaford. There was little literature on digital forensics during the 1990's but, since 21st century; digital forensic publications and conferences have grown tremendously. From the year 2000, the need for standardisation in the digital forensic field could not be ignored any more as courts started to recognise the importance of computer evidence (Meyers and Rogers, 2004). A number of bodies and agencies that were involved in the forensic field responded to the need for standardisation and some have published guidelines that need to be followed when conducting digital forensics. In 2001, the first Digital Forensic Research Workshop (DFRW) was held. In the following year, the International Journal of Digital Evidence was available; this was followed by the International Journal of Digital Investigation in 2004. In 2002, the Scientific Working Group on Digital Evidence (SWGDE) published a paper called "Best Practice for Computer Forensics" (SWGDE, 2002). In 2005, the first annual IFIP working group 11.9 on digital forensic conference was held. Needless to say, the literature on digital forensic has increased dramatically.

2.2 Digital Forensics Readiness

Digital forensic readiness is a discipline within the field of digital forensics (Danielson and Tjostheim, 2004). In today's digital age, most digital crimes are committed through the use of advanced technologies and, therefore, there is a need for the organisations to be digital forensic ready in order to deal with these kinds of crimes. According

Rowlingson (2004), any organisation that underrates the need for digital forensic readiness might find itself unable to link the attacker to the forensic incident or lack sufficient evidence to prove fraudulent transaction. It is imperative for organisations to be ready to provide evidence whenever this is required by law enforcement agents (Grobler, 2010).

2.2.1 Definition of Digital Forensics Readiness

Tan (2001) defined digital forensic readiness as having two objectives. The first objective is to maximise an environment's ability to collect credible digital evidence. The second objective is to minimise the costs of forensic investigation during an incident response. This definition is more focused on the technical aspect of digital forensic readiness.

Danielson and Tjostheim (2004) defined digital forensic readiness as focusing on adapting organisations and configuring of their systems to proactively collect and preserve potential evidence for potential use later. They view digital forensic readiness as encompassing the general preparation for incident response, such as specifying the resources that need to be allocated to different types of incidents. Digital forensic readiness is viewed as a field within the field of digital forensics (Danielson and Tjostheim, 2004).

Rowlingson (2004) defined digital forensic readiness as the ability of an organisation to maximise its potential to use digital evidence while at the same time minimising the cost of an investigation. According to Rowlingson (2004), the two main objectives of digital forensic readiness are to maximise an environment's ability to collect credible digital evidence and to minimise the cost of forensics during an incident response; these are the same objectives as those of Tan (2001). Rowlingson (2004) made a distinction between the technical and organisational aspects of digital forensic readiness. For the purpose of this research, the researcher adopted Rowlingson's definition of digital forensic readiness.

Hoolachan and Glisson (2010) stated that digital forensic readiness is the ability that an organisation can pre-empt the occurrence of a crime by preparing the environment in advance and in doing this, an organisation will benefit not only in instances where prosecution becomes an issue, but also in limiting their own business risks.

2.2.2 Motivation for Digital Forensics Readiness

Prior research has focused on several reasons for an organisation to achieve digital forensic readiness. These are presented below:

2.2.2.1 Evidence for legal action

The collection and preservation of digital evidence in advance serves as a support mechanism for criminal prosecution, internal disciplinary actions and also for legal defence (Rowlingson, 2004). Digital forensic readiness improves the prospect for successful legal action. It also enhances the company's interaction with the legal authorities (Grobler, 2010).

2.2.2.2 Compliance

Digital forensic readiness serves to demonstrate that the organisation is compliant with legal and other regulatory requirements. Digital forensic readiness serves to demonstrate that the organisation has practiced due diligence to protect its image as digital crime can damage the organisation posture (Rowlingson, 2004).

2.2.2.3 Employee deterrence

The ability of an organisation to be prepared to gather and use evidence can serve as a deterrent to criminals (Barske, Stander and Jordaan, 2010). According to Barske, et.al (2010), digital forensic readiness allows staff in the organisation to know what the organisation's attitude is towards the policing of corporate systems. In this case, policy documents serve as guides (Rowlingson, 2004). The staff will be able to hear through rumours what type of crimes may have been successfully or unsuccessfully committed, and what action may have been taken against those staff members (Rowlingson, 2004).

2.2.2.4 Business continuity

Digital forensic readiness indirectly supports business continuity management after an incident or disaster has occurred (Danielson and Tjøstheim, 2004). According to Danielson, et.al (2004), digital forensic readiness allows minimal disruption to the business in the event of an incident. Digital forensic readiness reduces the cost and time for internal investigations because evidence would have been collected in advance. It also assists in providing information about transpired events (Danielson, et.al, 2004).

2.2.2.5 Disciplinary hearings

The foremost issue in understanding the need for forensic readiness is a risk assessment. Digital forensic readiness can support employee sanctions based on digital evidence, for example, by proving violation of an acceptable use policy e.g. information security policy (Rowlingson, 2004).

2.2.2.6 Effective utilisation of resources

Digital forensic readiness ensures that processes, procedures, and technological resources are utilised to comprehensively gather digital evidence and enable a cost effective and successful investigation (Grobler, et.al, 2010).

2.2.2.7 Other benefits

Digital forensic readiness helps to shorten the investigation process which saves the company time and money that would have been spent on gathering evidence after the fact. Digital forensic readiness serves as the last line of defence after all other security measures have failed; for example, if an incident has occurred, digital forensic techniques are called in to establish evidence of what went wrong (Danielson, et.al, 2004).

2.2.3 Costs of Digital Forensics Readiness

According to Barske, Stander and Jordaan (2010), organisations need to be aware that there are costs associated with digital forensic readiness. They have identified the following costs:

- When an organisation is implementing a digital forensic readiness program, it is expected to update its current policies and, in some instances, to establish new policies. This can result to some additional expenses which the organisation needs to budget for.
- All employees would need to be made aware of the digital forensic readiness program and some employees would need additional training.
- In order to have a successful digital forensic readiness program, a company must obtain legal advice to confirm that the program will be legally compliant with both local and international laws and best practices.
- The implementation of a digital forensic readiness program requires the organisation to develop an in-house digital forensic examination and analysis capability.

In addition to the above costs associated with the implementation of digital forensic readiness, Rowlingson (2004) also identified the following costs:

- Securing of storage for potential evidence will result in increased costs
- Developing an in-house DFI capability, if required
- Enhancing capability for evidence retrieval
- Systematic gathering of potential evidence

The general consensus is that the benefits outweigh the costs and thus digital forensic readiness is desirable in organisations.

2.2.4 Drivers of Digital Forensics Readiness

The previous studies focused on several reasons for an organisation to achieve digital forensic readiness; these are discussed below:

2.2.4.1 Legal/Regulatory aspects

According to Landman (2002), the laws that govern forensic activities require one to be aware of the legal implications of any investigation. Landman (2002) recommended that security professionals must consider both their policies and their technical actions in the context of a legal framework. For example, before you monitor and collect data related to computer intrusion, you must be authorised to do so by the administrator (Landman, 2002). According to Landman (2002), organisations are required to prove that their investigation processes comply with computer security best practices. In 2003, the South African government passed a law called the Electronic Communications and Transactions Act (ECT Act, 2003). The Act has certain requirements for determining the admissibility of a digital document or digital evidence in a court of law. The Act placed the reliability of evidence in the manner in which that evidence was recorded and communicated and how the integrity of the data was maintained, and the manner in which the originator or author of the record was identified (ECT Act, 2003). The Act aims to assist large organisations to be able to identify and capture the evidence and also to assist organizations in implementing a digital evidence record management system and electronic document management system (Grobler and Louwren, 2007).

According to the King III codes on corporate governance, it is the responsibility of top management to ensure that the security position of the organisation is preserved at all times (King report III, 2009). Top management is expected to ensure there are proper

control measures to protect the resources and assets of their companies. The report requires companies to have a dedicated information security policy in place and that information security should be part of corporate governance (King III report, 2009).

In US, the Sarbanes-Oxley Act of 2002 requires companies to develop plans and policies to prevent and to investigate a variety of types of fraud (Richardson, 2005). According to section 302 of the Sarbanes-Oxley Act of 2002, CEO's, CFO's and CIO's have the responsibility of signing off the effectiveness of internal controls. In order to assist these people, digital forensic readiness looks at information on the corporate network as part of compliance. CIO's will be able to use digital forensic processes to prove that regular checks have been performed (Grobler and Louwrens, 2007).

2.2.4.2 Regulatory requirement

The regulatory environment around sensitive data protection has become more rigorous, diverse and complex. The number of existing regulations and standards mandate explicit response to information security incidents (ISO 177799, 2003). According to ISO177799 (2003) which is an international standard for information security, the digital evidence that must be produced in court must be of international standard. According to Section 8-01-03-02 of ISO77799, incident response procedure should manage the analysis and the identification of the root causes, implementation of remedies in order to prevent reoccurrence, collection of audit trails and similar evidence, manage the communication team, and report the incident to the relevant authorities (ISO 177799, 2003).

2.2.4.3 Cross-departmental collaboration

The legal department requires confirmation that the organisation's investigation is compliant with local laws and regulations (Whyte, et.al, 2011). It is expected of the digital forensic examiner to consider their technical investigations within the context of the law as these can have serious consequences (Thomas, 2004). It is therefore important for anyone who is involved to be aware of the legal implications of the forensic activities (Thomas, 2004).

Digital evidence is required by the human resources department when an employee is alleged of misconduct and disciplinary action is to be taken. The human resources department carries huge amounts of employee's personal information which needs to be protected at all costs and at all times (Thomas, 2004).

When a disaster has occurred in an organisation, the disaster recovery team is called for a forensic investigation (Danielson, et.al, 2004). In some organisations, the forensic competence centre is also called in to assist with the investigation to establish what happened. The teams that are responsible for risk management, risk control, and crime risk control call on a forensic examiner to assist in putting in place a risk management program after the incident has occurred and to put measures in place to prevent it from happening again (Danielson, et.al, 2004).

2.2.4.4 Other drivers

With regard to technology and infrastructure, organisations need to make sure the investigators are using acceptable tools that meet the stipulated legal requirements (Grobler and Louwrens, 2007). According to Grobler and Louwrens (2007), results generated using recognised software packages will be accepted as evidence in a court of law. An organisation needs to acquire the right software and hardware in order to implement a digital forensics readiness program. The right technology will enable it to acquire and preserve evidence (Barske, Stander and Jordaan, 2010).

With regard to training, organisations are expected to provide the investigators with relevant training that will equip them to be able to do their jobs effectively and efficiently (Poope and Labuschagne, 2012). The training could involve knowing the relevant regulations that governs digital forensics. Organisations are also expected to run awareness programs that are aimed at informing every staff member in the organisation about cyber-crimes and fraudulent activities (Whyte, et.al, 2011). The awareness programs should be aimed at empowering staff as what to do when an incident has occurred and how they should behave in order to avoid contaminating evidence (Barske, Stander and Jordaan, 2010).

2.3 Models for implementing Digital Forensics Readiness

In this section, emphasis is placed on the aspects of digital forensic readiness in the context of an organisation.

The first person to introduce the concept of digital forensic readiness was Tan (2001). Tan's discussion focused on the importance of advanced data collection which the organisation can use later when conducting digital investigation. Tan (2001) identified the following four possible sources of incident data:

- Victim system(s) RAM, registers and raw disk
- Attacking system(s) RAM, registers and raw disk,
- Logs (from the victim and attacking systems as well as intermediary systems)
- Physical security at the attacking system (camera monitoring, etc.).

Tan (2001) stated that the cost of an incident is proportional to the amount of time it has taken to investigate it. This implies that preparedness for an incident reduces the time and cost to investigate it. Tan (2001) identified following five elements of digital forensic readiness: how logging is done, what is logged, Intrusion Detection Systems (IDS), Forensic acquisition, Evidence handling. Tan (2001) recommended that a chain of custody documents should exist and be readily available to those responsible for responding to incidents. He also argued that the chain of custody should begin when data is first considered as potential evidence. Tan (2001) recommended that the digital forensic readiness process should concentrate on developing procedures to guide transportation, storage and examination of digital evidence. He also suggested that digital forensic readiness efforts should ensure storage capacity exists to store digital devices or digital evidence. What is important about Tan's elements is that they involve technical and non-technical aspects of digital forensic readiness.

Rowlingson (2004) proposed a "Ten Steps Approach" that describes the key activities that an organisation needs to perform when implementing a forensic readiness program. The elements of this include the following steps:

- *Define the business scenarios that require digital evidence*. This step defines the purpose of evidence collection capability and allows an organisation to determine business scenarios in which it is mostly at risk and the potential impact it has to the business. The importance of this step is that, it encourages an organisation to take an organised approach than ad-hoc approach to digital forensic readiness.
- *Identify available sources and different types of potential evidence*. This step assists an organisation to know what resources are available within the organisation from across different systems and application in order to conduct digital forensic investigation.
- *Determine the evidence collection requirements*. The purpose of this step is to ensure an organisation produces an evidence requirement statement that spells out clearly the responsibilities of those responsible for managing business risks.

Establish a capability for securely gathering legally admissible evidence to meet the requirements

- *Establish a policy for secure storage and handling of potential evidence*. This step deals with the establishment of a capacity for securing and gathering evidence legally. This step requires the organisation to ensure the evidence collected in above step to be preserved in an appropriate manner. The step forces the organisation to ensure its evidence collection procedures conform to law requirements.
- *Ensure monitoring is targeted to detect and deter major incidents*. This steps deal with the establishment of a policy for a secure storage and handling of potential evidence that will be used in future.
- *Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched*. This step requires the organisation to review the suspicious activities detected in step 6 in order to determine where a full formal investigation is warranted. The importance of this step is to guide and help the organisation to decide on how to react to suspicious activities.
- *Train staff in incident awareness so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence*. This step involves the training of employees in incident awareness, so that all those involved understand their role in digital evidence the step emphasises the importance of training staff to understand their role before, during, and after an incident.
- *Document an evidence-based case describing the incident and its impact*. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled. This step helps to support regulatory reporting.
- *Ensure legal review to facilitate action in response to the incident*. This step stresses the importance of obtaining a legal opinion when building a case and after a case has been established

Rowlingson's ten steps approach provides a comprehensive and broad framework of digital forensic readiness. The framework shows that, the scope of digital forensic readiness involves both technical and non-technical aspects for evidence collection. The framework also indicates that development and maintenance of digital forensic readiness

within an organisation requires a wide effort from multiple functional areas of the organisation.

Danielson and Tjostheim (2004) also made contribution by focusing on the importance of digital forensic readiness and key issues such as the preservation and presentation of digital evidence. The lack of clarity for organisations regarding the requirements and constraints set by the law on the collection and preservation of digital evidence has been a problem for most organisations (Danielson and Tjostheim, 2004). Danielson, et.al, (2004) also raised privacy concerns if the digital forensic readiness function is outsourced to a third party. They proposed a structured approach which they argued will be legally compliant and will take into account privacy concerns. The elements of the structure approach include:

- An analysis of legal requirements and constraints on collection and preservation of potential digital evidence in the applicable legal context
- A method for analysing the organization's need for digital evidence
- An identification and classification of potential digital evidence sources, and enumeration of technologies and processes for utilizing these sources
- Guidelines for preserving digital evidence, including processes, procedures, and suggestions as to how technology solutions can be used
- Guidance on when and how to report incidents to law enforcement, including content and formats of reports, criteria for reporting, and standardization of the interaction between affected parties and law enforcement.

These elements support Rowlingson's (2004) ten steps approach by emphasising the importance of assessing the need for digital forensic readiness by the organisation and the configuring of their systems to proactively gather digital evidence. The also support the development of guidelines for the preserving and handling of digital evidence.

The key important element in the structured approach concerns methods for analysing the potential evidence needs of the organizations. The model provides an excellent way that will help investigators to avoid confusion regarding the legal requirements, constraints and the role and responsibilities between internal and external investigators.

Endicott-Popovsky, Frincke, and Taylor (2007) made a contribution by discussing the value of an organisation's network system. Their discussion focused on the concept of network forensic readiness as a contributor to digital forensic investigation. Endicott-

Popovsk, et.al (2007) defines "network forensic readiness" (NFR) as maximising the ability of an environment to collect credible digital evidence while at the same time minimising the cost of an incident response. This definition is similar to that of digital forensic readiness offered by Rowlingson (2004). Endicott-Popovsky,et.al (2007) argued that, while organisations developed tools and techniques for digital forensic readiness, a realisation of network forensic readiness has been fragmented. In order for the network system to be forensic ready, it needs to incorporate the full spectrum of information assurance elements such as security policy, procedures, practice, mechanisms, and security awareness training, as illustrated in Figure 1.

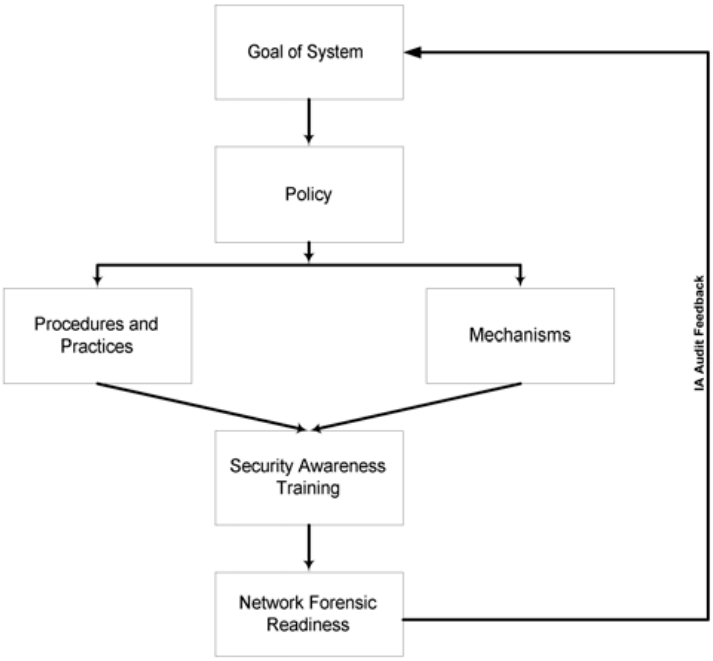

Figure 1: Network Forensic Readiness Model (Endicott-Popovsky et al., 2007)

The Endicott-Popovsky, et.al (2007) NFR framework is a more focused type of digital forensic readiness. The model emphasises the importance of taking into consideration the legal requirements for compliance with evidence collection and storage standards for courtroom admissibility when designing a system. Although the strategies and model proposed by Endicot-Popovsky, et.al (2007) are aimed at network forensic readiness specifically, they can also be applied to the complete digital forensic readiness process.

Endicott-Popovsky et al. (2007) also offered a strategic management model to assist management in developing a policy for information assurance and digital forensic readiness. The model became known as the 4R Model for accountable systems. Components include strategies for resistance, recognition, recovery and redress, as

summarised in Table 1. According to Endicott-Popovsky et al. (2007), these components can be used to ensure an adequate level of security and accountability in security breaches and to hold the culprits responsible for their actions.

Table 1: 4R Model (Endicott-Popovsky, Frincke and Taylor, 2007)

Strategy	Tools
Resistance 1. Ability to repel attacks	• Fire walls • User authentication • Diversification
Recognition 1. Ability to detect an attack or probe 2. Ability to react/ adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1. Provide essential services during an attack 2. Restore services following an attack	• Incident response • Forensics – (What) • Replication • Backup systems • Fault tolerant designs
Redress 1. Ability to hold intruders accountable 2. Ability to retaliate	• Forensics – (Who) • Legal remedies • Active defence

The most important element of this model is the redress component, which seeks to hold intruders accountable and to ensure the organisation has active defence mechanisms and legal remedies. Endicott-Popovsky,et.al (2007) also offered a methodology for embedding forensics readiness in networked systems based on the NIST Information Systems Development Life Cycle (ISDLC), which aimed to incorporate security across the lifecycle of systems development. Endicott-Popovsky, et.al (2007) argued that if information assurance is redefined to include digital forensics, then a methodology that develops secure systems should also be a vehicle for delivering forensic capability. Endicott. et,al.(2007) suggested that the design of such a system should take into consideration the necessary legal requirements for compliance, with evidence collection and storage standards for courtroom admissibility, and affect each phase of the life cycle(Endicott-Popovsky. et.al,2007, p.7).

Endicott-Popovsky, et.al (2007) applied this model to the NIST Information System Life Cycle in order to develop an implementation methodology known as Network Forensics Development Life Cycle (NFDLC)(Endicott-Popovsky, et.al, 2007,P.7). Figure 2 depicts the

analysis and modification to include additional steps that ensure embedding of digital forensic functionality.

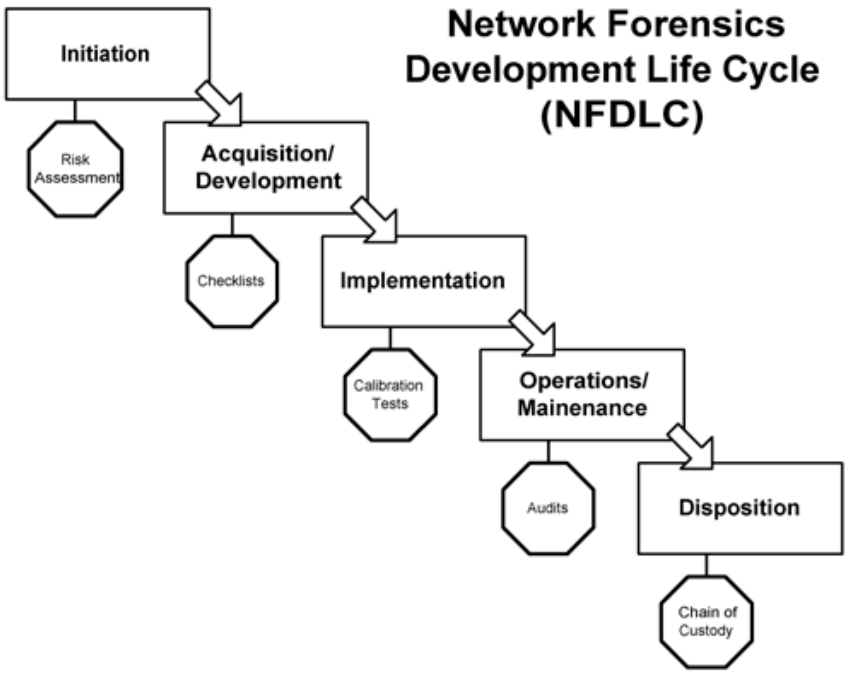

Figure 2: Network Forensic Development Cycle (Endicott-Popovsky et al., 2007)

The rapid development of technology has changed the nature of incidents and attacks on organisations (Grobler and Louwrens, 2009). Grobler and Louwrens (2009) noted that the traditional digital forensic investigation methodologies were having problems in gathering live digital evidence. They proposed comprehensive a digital forensic management framework that will:

- Prepare the organisation for digital forensic investigation by proactively identifying and making sure sound admissible evidence is available when required.
- As part of preparation, the framework will assist in restructuring relevant digital forensics processes so that they can be forensically sound.
- The other function of the framework will be to utilise digital forensic tools and techniques to enhance governance within the organisation.
- The framework will assist in gathering live digital evidence during attacks.
- The framework will assist in successfully investigating incidents, establishing the root-cause and prosecuting perpetrators (Grobler and Louwrens, 2009).

Grobler et al. (2009) argued that the previous models were unable to address the above issues. They proposed high-level framework consisted of three components: Proactive

Digital Forensics (ProDF), Active Digital Forensics (ActDF), and Reactive Digital Forensics (ReDF). The authors further identified eight goals of ProDF, such as providing and preparing the infrastructure, developing evidence management plan, digital forensic training and awareness strategy, management capability that will define and outline the role and responsibilities of both internal and external investigators. This is in line with what was suggested by Rowlingson (2004) in his seventh step. According to Grobler and Louwrens (2009), ProDF ensures an investigation proceeds at a cost that is in proportion to the incident. This is in agreement with Tan' suggestion that the amount of time spent on an investigation should be in proportion to the cost of the incident (Tan, 2001). The most prominent component of this framework is proactive digital forensic readiness.

Barske, Stander, and Jordaan (2010) developed a digital forensic readiness conceptual framework for South African Small and Medium Enterprises (SMEs). This framework is specifically relevant to the SMEs because, SMEs have limited resources (technical and/or financial) and are vulnerable to high-frequency/low impact incidents which could have negative impacts on business viability (Barske, Stander, and Jordaan, 2010). An example of this is when a company does not survive after an incident has occurred and lacks the ability to provide evidence in order to prosecute culprits, or has not been properly prepared for the incident. In some cases, SMEs are unable to afford a full forensic investigation performed by third party experts, thus limiting their access to the digital evidence (Barske, Stander, and Jordaan, 2010). Digital forensic readiness is essential and needs to be optimised by SMEs as this could be the only defence against a serious incident. Barske, Stander, and Jordaan (2010) identified the following five elements in their framework: Strategy, Policies and Procedures, Technology, Digital Forensic Response, Compliance and Monitoring. The framework has neglected the role that should be played by the legal department in designing and implementing a digital forensic readiness program. The framework does not consider the organisation's human resources as critical components of digital forensic readiness The framework also fails to acknowledge the importance of digital forensic methodology, which needs to be sound and to be in line with international best practice.

Grobler, Louwrens, and Von Solms (2010) developed a framework called A Guide to Implement Proactive Digital Forensics. The components of their frameworks are similar to those that have been identified by Barske, Stander, and Jordaan (2010) but added the

legal, people, process dimension to replace digital forensic response and compliance and monitoring comments from the above framework.

Whyte and Claims (2011) also developed a digital forensic readiness conceptual framework after examining Rowlingson (2004)'s "ten step approach" and Danielson, et.al, (2004) the "need for structure approach". They identified common themes that could be grouped into multiple themes. These are: organisational strategy, methodology, systems and events, monitor and report, legal involvement, training, policy and compliance themes. The advantage of Whyte, et.al, (2011) framework is that it utilised the aspects and strengths of both Rowlingson's ten step approach and Danielson, et.al (2004). The legal requirements are at the centre of this framework.

Poope and Labuschagne (2012) identified core activities relating to digital forensic readiness. These are: People, Process, Policy and Technology. According to Pope and Labuschagne (2012), another way of looking at digital forensic readiness is to categorise certain activities that need to be performed by an organisation if it wants to be digital forensic ready. This framework acknowledges the role of staff members in contributing towards a digital forensic readiness environment if they are trained and made aware of security incidents. The framework also emphasises the importance of a well-defined digital forensic process or methodology in ensuring the credibility of digital evidence.

2.4 Digital Forensics Readiness Dimensions

Based on the models and frameworks discussed in the previous section, this section defines four digital forensic readiness dimensions. Digital forensic readiness dimensions refer to the extent to which various factors influence organisation's readiness to deal with digital crimes. The dimensions are interrelated and complement each other in an attempt to provide a comprehensive solution to digital forensic readiness (Grobler and Louwrens, 2006). According Grobler , Louwrens, and Von Solms (2010) people, process, technology and governance form the basis of management models.

2.4.1 Corporate governance

Top management is responsible for ensuring that there are proper controls and measures to protect the organisation's posture (King II report, 2003; Sarbanes-Oxley Act, 2001). According Grobler, Louwrens and Von Solms (2010), the effective utilisation of digital forensic tools and techniques can enable management to prove due diligence with good

governance. This enables enhancement of governance structures such as, IT governance and information security governance (Grobler, Louwrens and Von Solms, 2010).

The organisational strategy dimension, according Whyte, et.al, (2011), is present in both the Barske, et.al, (2010) and Grobler and Louwrens (2006) frameworks. According Grobler, Louwrens and Von Solms (2010) in order to implement a digital forensic readiness program, it must be supported by top management. The support of top management will ensure enough resources are allocated to facilitate digital forensic readiness across the organisation (Grobler Louwrens, 2010). According to Barske, Stander, and Jordaan (2010), digital forensic readiness should be seen as a strategic decision and should form part of the organisation's strategy. The outcome of this step is an evidence collection statement that will align business risk units with incident monitoring units (Whyte, et.al, 2011).

2.4.2 Forensic Policy

The existing literature on digital forensics has recognised the need for organisations to gather and use digital evidence for the prosecution of digital crime (Rowlingson, 2004).

Yasinsac and Manzano (2002) noted that enterprise forensics policies can enhance computer and network forensics. They propose six categories of forensic policies which are aimed at facilitating digital forensic investigation. According to Yasinsac and Manzano (2002), these policies will help the enterprises to deter computer crime and to position themselves so that they can respond to attacks successfully, and thus improve their ability to conduct digital forensic investigations. The policies they proposed include: retaining information, planning the response, training, accelerating the investigation, preventing anonymous activities, and protecting the evidence (Yasinsac and Manzano, 2002). Rowlinson (2004) recommended that an organisation needs to establish policies for the securing, storing and handling of potential evidence that will be used in future. Whyte, et.al, (2011) also recommended the development of good forensic policies in order to achieve a successful digital forensic readiness program.

Whyte and Claims (2011) argued that organisations should constantly review their policies as the legislation changes or as new systems are introduced. As part of being digital forensic ready, the organisation needs to have clear guidelines on ethical behaviour, rules and guidelines for digital forensic investigation (Whyte, and Claims, 2011). The legal department is to assist the organisation's digital forensic readiness

program by ensuring it complies with both international and local laws regarding the collection and storing of comprehensive digital evidence (Whyte and Claims, 2011). This is in line with Rowlinson's (2004) tenth step about the role that should be played by the organisation's legal department. According to White and Claims (2011), the company's legal advisors need to be trained and experienced in cyber laws and the admissibility of digital evidence.

Grobler, Louwrens, and Solms (2010) view policies as building blocks to guide management in developing a framework to manage digital forensic readiness within the organisation. Endicott-Popovsky and Poope and Labuschagne (2010) also support the development of policies in preparing for digital investigation.

According to Barske, Stander, and Jordaan (2010), a digital forensics readiness program that has well-defined digital forensic policies can provide the organisation with the authority to conduct investigation, collect evidence and examine evidence within the organisation. Policies serve as a guide to assist members of the organisation to carry out their responsibilities efficiently and effectively. Failure to comply can have negative implications for the organisation (Barske, Stander, and Jordaan, 2010).

Whyte, et.al, (2011) regards policy as a critical component for a successful digital forensic readiness program. According to Whyte, et.al, (2011) policy serves as a guide on how a comprehensive evidence-based case must be built. Whyte, et.al, (2011) recommended that an organisation should understand what the implications on non-compliance to digital forensic requirements are. They also recommended that an organisation should review its policies as legislation changes or new system or technology is being in used or a new methodology has been introduced. Poope, et.al, (2010) agrees with Barske, Stander, and Jordaan (2010) and Yansisac and Manzano (2002) that the development of digital forensic policy assists the organisation to detect computer crimes.

The digital forensic process methodology supports the policy dimension in the sense that it provides procedures and guidelines needed to implement policies (Grobler, Louwrens, Solom, 2010). According to Grobler (2010), all digital forensic processes and procedures should be forensically sound and must be able to maintain the chain of evidence. Grobler (2010) recommends that organisations need to have a well-defined methodology that has comprehensive standard operating procedures. Whyte, et.al (2011) also recommended that the digital forensic methodology that the organisation selects should facilitate

uniformity and adhere to international best practice. The forensic methodology must also best fit the organisation (Whyte, et.al 2011). The digital forensic process should also inform the techniques and tools to be used in collecting digital forensic evidence (Whyte, et.al 2011).

The digital forensic process serves as a guide to meet both the regulatory requirements and the organisational policies (Poope and Labuschagne, 2012). According to Poope and Labuschagne (2012), the processes should be governed by certain policies and guiding principles to chart the course of action in the event of an incident. This component requires an organisation to have defined processes that will guide it in achieving a digital forensic ready environment. Failure to have a well-defined forensic process will negatively affect the outcome of the investigation (Poope and Labuschagne, 2012).

Stander, et.al, (2010) raised the importance of having a digital forensic management plan. Stander,et.al (2010) regards the incident response plan as the part of digital forensic readiness that seeks to assist an organisation in identifying the people and process to be followed in responding to an incident. The failure to acknowledge the importance a digital forensic response will place the organisation at risk. The organisation will not be sure whether an incident should be referred to external practitioners or if it should be dealt with internally (Stander, et.al, and 2010). This requires people in the organisation to be trained about and be made aware of digital crimes.

Rowlingson(2004) recognised the importance and role played by members for a successful digital crime prosecution. Rowlingson's (2004) eighth step stress the importance of training staff so that they can understand their role before, during and after an incident. Rowlingson(2004) recommends that whistle blowers and investigators and their names be protected and kept confidentially from any possible retaliation.

Grobler and Louwrens (2009) identified one of the goals of proactive digital forensic as developing digital forensic training and awareness strategy. They also recommend that such a training and awareness strategy be incorporated into the overall organisation training and awareness strategy.

Grobler, Louwrens, and Solom,(2010) also support the need for digital forensic training program that concentrates on the needs of different users and employees within the organisation (Grobler, Louwrens, and Solom, 2010). Organisations are encouraged to

accredit the training program with relevant qualification authorities, such as the South African Qualification Authority (SAQA), so that employees are accredited with a certain level of qualification. The more employees obtain certain level of accreditation, the more their evidence collection and procedures will be followed when applying digital forensic tools; this could result in more credible evidence. Grobler, Louwrens, and Solom (2010) also recommend that organisations should implement digital forensic awareness programmes to instil an evidence preservation culture.

Members of the organisation are critical components of a digital forensic readiness program (Rowlingson, 2004). Organisations should ensure all members of the organisation contribute towards the prevention and detection of security incidents (Poope and Labuschagne, 2012). According to Poope and Labuschagne (2012), failure to organise and equip employees with necessary tools and knowledge can ultimately impact the organisation's digital forensic readiness.

2.4.3 Technology Dimension

When a digital crime has been committed, it will be difficult for an organisation to conduct an investigation without proper technology (Stander, et.al, 2010). According to Stander, et.al, (2010), the organisation needs to obtain technology that will be able to acquire evidence in a sound and legal manner. Tan (2001) and Stander, et.al,(2010) regard computer logs and computer servers as important sources of digital evidence which should not be ignored by the organisations.

It is important for the organisation to understand which systems and technologies house potential digital evidence and the events that require digital evidence (Whyte, et.al, (2011). This is in line with Rowlingson's(2004) suggestion that an organisation needs to conduct a risk assessment at the business level. The use of a monitoring and reporting system by an organisation to detect any security threats is important (Whyte, et.al, 2011). The intrusion detection system (IDS) plays an important role in reporting an event when certain threats are triggered (Rowlingson, 2004). The monitoring and reporting system assist organisations to understand which IDS must be obtained, how to respond to incident triggers, what format to use and when to escalate the incident (Whyte, et.al, 2011).

Poope and Labuschagne (2012) support the use of technology not only to enable business operations, but also to prevent and detect computer incidents. Poope and Labuschagne,

(2012) is in agreement with Stander, et.al, (2010) that the organisation needs to ensure the technology used is legally acceptable. Failure to comply with legal requirements will affect the admissibility of digital evidence (Rowlingson, 2004). The efforts to ensure availability and integrity of data are central to maximising the organisation's ability to collect credible evidence and to facilitate an investigation Poope and Labuschagne, 2012).

2.4.4 Legal and Ethics Dimension

Different countries have different judiciary system which governs how evidence should be gathering, handled, transported and preserved. The investigators are expected to familiar with both international and local laws and treaty requirements (Grobler and Louwrens, 2006). In South Africa for an example, the Electronic Communications Act (ECT) set specific requirements for electronic evidence to be admissible in court (ECT, 2003). When investigator is operating in a different country, it is important to determine the operating environment as different cultures can influence an investigation (Grobler, Louwrens, and Solom, 2010). According Whyte, et.al (2011) legal professionals need to be trained in cyber-law.

The consideration of ethical aspects have become an important the investigators need consider when conducting investigations. The misuse of forensic tools for personal gains, trust that is place on the investigator by employees could have negative impact to the organisation. The establishment of codes of conduct can assist the organisation to set clear guidelines on ethical behaviour (Grobler and Louwrens, 2006; Trevino, 1986).

2.5 Proposed Conceptual Model

The proposed model highlights requirements that an organisation needs to perform if it wants to be digital forensic ready. The requirements are grouped into categories/components, and under each category various sub-activities are to be performed by an organisation that wants to be digital forensic ready. These activities can further be classified into proactive, reactive and active classes. The common elements in the following model were grouped together and Figure 3 summarises the critical components in designing and implementing a digital forensic readiness (DFR) state. The arrows from the digital forensic readiness state in the diagram serve as a feedback mechanism for decision-makers to make adjustments where they are necessary.

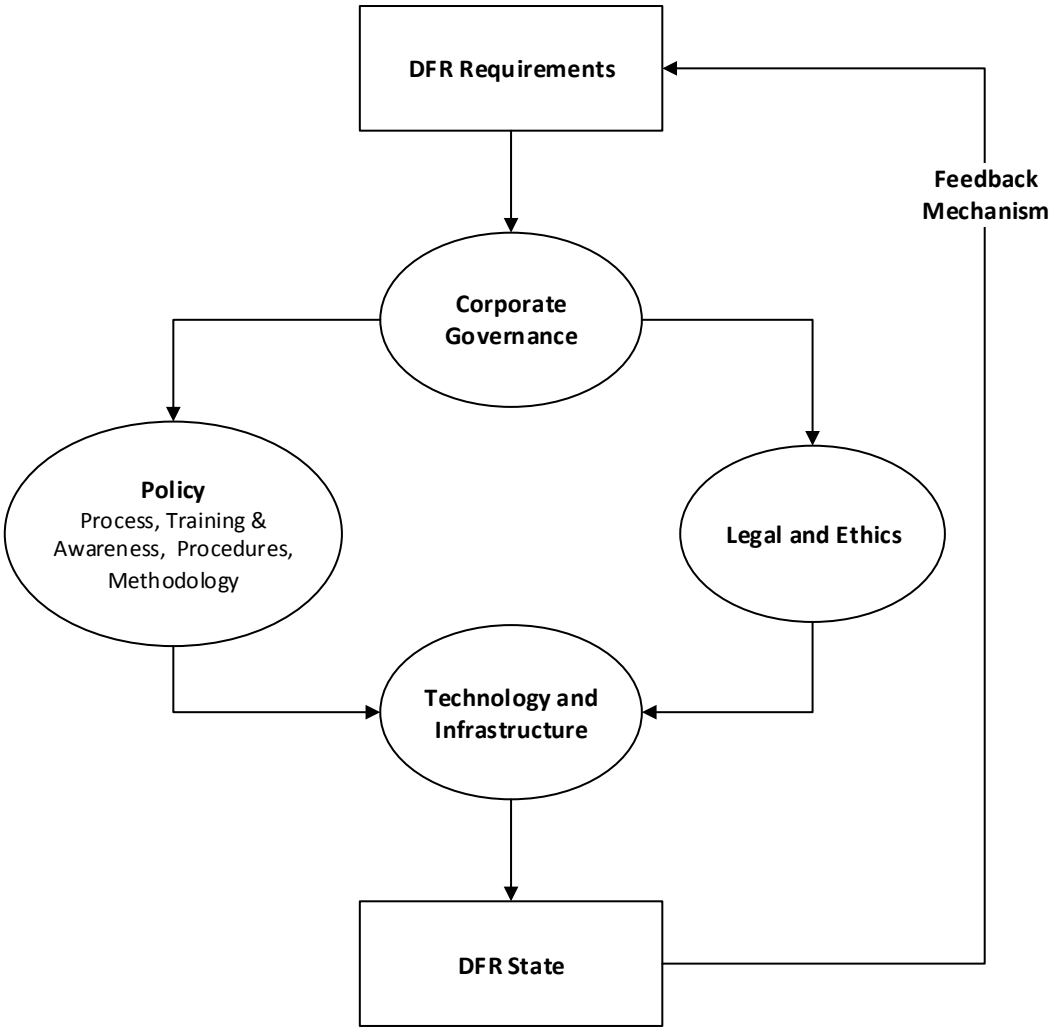

Figure 3: Factors influencing digital forensic readiness

2.5.1 Corporate Governance Category

The corporate governance dimension aim is to support the organisation's digital forensic readiness initiatives (Grobler and Louwrens, 2006). According to the King III (2009) codes on corporate governance, it is the responsibility of management to ensure that the security position of the organisation is preserved at all times. The reports require companies to have a dedicated information security policy in place and that information security should be part of corporate governance (King Report on Corporate Governance, 2009).

According to Barske, Stander and Jordaan (2010), in order for digital forensic readiness programs to be implemented successfully, top management support is needed. As part of corporate strategy, digital forensic readiness should be able to identify and understand

the kinds of legislation and regulations that are imposed upon and oblige the organisation to retain evidence/records, and thus inform what policies are needed (Barske, Stander and Jordaan, 2010).

2.5.2 Policy Category

This dimension involves the development of a general policy framework that will support and underpin the efforts of employees when conducting forensic investigations. The policy framework is needed to guide employees on procedures to be followed during an investigation so that the investigation will stand up to scrutiny in a court of law. The policy category consists of a number of sub-activities that an organisation needs to perform if it wants to be digital forensic ready; these include Process activity, People activity, and Procedures activity and Methodology.

2.5.2.1 Process

The process component involves ensuring that operational documents such as an incident response plan and a forensics methodology are in place. Von Solms, Louwrens, Reekie, and Grobler (2006) identified four activities of digital forensic process which include: securing the evidence without contaminating it, acquiring the evidence without altering it, authenticating that the recovered evidence is the same as the original seized data, and analysing the data without modifying it.

2.5.2.2 Training and Awareness of People

The organisation needs to recognise that people are the most important asset and yet the weakest link in the organisation's security chain (Rowlingson, 2004). Organisations need to develop policies that address the training of staff members and those affiliated with the organisation (Rowlingson, 2004). The training provided and the awareness created will enable employees, including investigators, to know what they must do when an incident occurs. The objective of people activity is to ensure that the human resources of an organisation all contribute towards the prevention and detection of security incidents (Von Solms, Louwrens, Reekie, and Grobler, 2006).

2.5.2.3 Procedures

The organisation needs to develop policies that address operational aspects of investigations (Rowlingson, 2004). The policy should state the manner and circumstances when evidence that has been preserved by the organisation may be

released to parties outside of the organisation, including when and how matters should be referred to by law enforcement.

2.5.2.4 Methodology

The organisation is expected to develop policies that address the handling and protection of evidence and other vital data (Rowlingson, 2004). Although various companies adopt different digital forensic investigation methodologies, it is important for an organisation to adhere to what is international best practice (ISO 17799, 2003).

2.5.3 Legal and Ethical Category

The legal dimension is responsible for ensuring that digital forensic investigators are familiar with both local and international legal requirements. The legal dimension also ensures investigators are prepared to present a case that will stand up to scrutiny in various courts of law (Thomas, 2004). It is therefore important for anyone who is involved to be aware of the legal implications of the forensic activities. The legal department is expected to assist the forensic investigation in order to ensure that all the gathered evidence is legal and will be acceptable in a court of law. (Thomas 2004)

In South Africa, the legislation and regulations requires forensic investigators to adhere to certain legislative requirements. The following sub-sections describe and explain the laws and regulations applicable in forensic investigations in South Africa.

2.5.3.1 Protection of Personal Information Act (2013)

According to the Protection of personal Information Act (2013), South African companies are required to ensure people's information is protected and preserved and to avoid having it landing in the wrong hands. The purpose of the Act is to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible person. The Act balances the right to privacy against other rights such as the right to access to information. The Act seeks to protect the free flow of information within the South African Republic and across international borders. The Act is aimed at regulating the collection and processing of personal information by both private and public bodies including the state (Protection of Personal Information Act, 2013). The Act seeks to establish principles that are in line with international law standards by prescribing the minimum threshold requirements for lawful processing of personal

information. There are the eight principles that have been established in this regard in South Africa.

2.5.3.2 Electronic Communication and Transaction ACT (2002)

The Act also seeks to promote technology neutrality in the application of legislation to electronic communications and transactions as well as ensuring that electronic transactions in South Africa conform to the international standards. According to Section 11(1) of the ECT Act, electronic data messages are given the same legal status as information that is generated in a conventional way. The Act relates to the admissibility of electronic evidence after digital forensic investigation has been conducted (Electronic Communication and Transaction Act, 2002).

2.5.3.3 RICA (2002)

The Act came into effect on 22 January 2003 after it was published in the government gazette. The Act seeks to regulate the interception of communication and associated processes such as application for and authorisation of interception (government gazette of South Africa 28075). The Act regulates the monitoring of radio signals and radio frequency as well as the provision of certain communication-related information. The Act regulates the execution of directions and entry of law enforcement agents. The Act also sets out the basis on which an employer can lawfully monitor employees' communication. It is therefore critical that South African organisations are familiar with provisions of the Act as failure to comply can result to a penalty of R2 000 000-00 or ten years imprisonment.

The organisation code of conduct sets clear guidelines on ethical behaviours. The investigator needs to make sure he or she does not misuse the trust that is placed on him or her. The establishment of codes of conduct assists in setting norms of what is an appropriate or inappropriate behaviour (Trevino, 1986). Trevino (1986) argued that collective norms can be used to guide employee behaviour in judging what is right or wrong.

2.5.4 Technology and Infrastructure Category

This dimension deals with the various tools that can be used to conduct an investigation. One of the fundamental perceptions of forensic computing is the need to ensure that the application of tools and techniques does not lessen the admissibility of

the final product. It is therefore important that the type of tools and techniques that are used as well as the way they are applied are compliant with the relevant rules of evidence (McKemmish, 1999). According McKemmish (1999), the failure to do so can result in the digital evidence being ruled inadmissible or, at the very least, being regarded as tainted. According to Thomas (2004), an organisation's legal department should assist the organisation in confirming that the technology used is compliant with the law.

The organisation operation and infrastructure play an important role in supporting the digital investigation process. For example, the establishment of a digital forensic laboratory assists in ensuring that the required digital evidence is obtained (Carrier and Spatford, 2003, and Whyte, et.al, 2011).

The proposed model is similar to that of Endicott-Popovsky, Frincke, and Taylor's (2007) network forensic readiness model. Both models highlight the need for forensic policies, procedures, practices, and mechanisms in order to be able to prosecute perpetrators of crime in the organisation while, at the same time, reducing the effort in conducting digital forensic investigations.

2.6 Conclusion

Digital forensics is utilised to conduct digital investigations that involve digital crimes or incidents in order to gather digital evidence that will be presented to a court of law for prosecution. In order to successfully prosecute those responsible for committing fraudulent activities within an organisation, it is critical for the organisations to put measures in place in order to collect evidence in advance. The literature reviewed highlighted a number of factors that have an impact organisation's digital forensic readiness. However, none of the existing frameworks provides an insight as to how and to what extent these factors influence digital forensic readiness.

The proposed model provides insight into the areas to focus on when designing and implementing a digital forensic readiness program. The application of this model leads to proper implementation of corporate governance principles, development of digital forensic policy, compliance to law when conducting digital investigations, and ensuring proper technology is used for investigations. The model will ensure collaboration within the organisation in an effort to enhance the capacity to prevent, detect and manage

incidents. It will also ensure that comprehensive, reliable digital evidence is available in the organisation whenever required. The next chapter discusses the methodology used how to investigate and answer the research questions.

Chapter 3: Research Methodology

This chapter discusses the research philosophy, design and methodology used in this study. The research methodology describes how the researcher conducted the empirical research.

3.1 Theoretical Perspective

There are two branches of philosophy that are used in information system discipline and these are ontology and epistemology. Kroeze (2011) refer to ontology as the analytical view of the fundamental nature of the universe and all its components. According to Kroeze (2011), ontology systematically describes aspects of reality. Ontology explains and describes our view on the nature of reality and specifically whether this is an objective reality that really exists or only subjective reality that is created in our minds (Flowers, 2009). According to Orlikowski and Baroundi (1991), ontology brings into perspective human rationality and social relations. In this study the researcher assumed that, the reality about how and to what extent various factor influence digital forensic readiness can be understood by interacting with the research participants. In this case, the participants were the employees of our case study organisation.

Epistemology is the philosophical field that is concerned with the nature of reality and the origin and validation of knowledge (Kroeze, 2011). Epistemology deals with beliefs about the origin, nature and limits of human knowledge (Mpazanje, 2009). It considers views about the most appropriate ways of enquiring into the nature of the world (Easterby-Smith, Thorpe and Jackson, 2008). Epistemology considers what knowledge is and what are the sources and limits of knowledge. The epistemological assumption of interpretivism is that, the findings of the study are created as the investigation is proceeding (Andrade, 2009). The researcher believed through the interview process, a new insight will be obtained as how and into what extent various factors influence digital forensic readiness in a South African organisation.

There are three commonly used research paradigms in information systems: positivist, interpretive and critical realist (Orlikowski & Baroudi, 1991). According to Orlikowski & Baroudi (1991), positivist research relies on evidence of formal proposition, quantifiable measures of variables, hypothesis testing in order to make inference about social phenomena, and a representative sample is drawn from stated population. Positivists use

quantitative data collection method (Flowers, 2009). Positivist researchers study the way the organisation has been in the past and presume that past patterns will occur in the future. Positivists tend to ignore the fact that people are actors of their physical and social reality. Positivist studies are based on the premise of prior fixed relationship with the phenomena and aim at testing theory in an attempt to increase the predictability of the phenomena (Klein and Meyer, 1999).

The interpretive paradigm is informed by a concern to understand the world as it is, to understand the fundamental nature of the social world at the level of subjective experience (Burrell & Morgan, 1979). According to Burrell & Morgan (1979), this paradigm seeks explanation within the realm of individual consciousness and subjectivity. This is done within the frame of reference of the participant as opposed to the observer of action (Burrell & Morgan, 1979). Interpretivist researchers immerse themselves in the phenomena they wish to study in order to develop an inside understanding of social realities as experienced by the subjects of the study. Interpretivist researchers begin their study with a broadly defined research problem that will guide their observations during the research process (Collis and Hussey, 2009). According to interpretivists, meaning is constructed and, over time, is constantly reconstructed by individuals or groups and resulting in different interpretations. Interpretivists believe that reality is relative and multiple and that there is more than a single structured way to access it (Lincoln and Guba, 1985). According to Walsham (1993), interpretive researchers aim to produce an understanding of the context of the information system as well as the processes whereby information systems influence and are influenced by the context.

The critical realist approach takes aspects from both positivist and interpretivist approaches. The realists believe that the real structure exists independent of human consciousness, but is socially created (Flowers, 2009). Saunders, Lewis, and Thornhill (2007) argue that knowledge of our reality is a result of social conditioning. According to the realist approach, reality may exist in spite of science or observation.

Based on the ontological and epistemological assumptions above, the interpretive paradigm seemed to be suited to address the research questions in this study. The study adopted an interpretive approach. The goal of this study was to understand the factors that influence digital forensic readiness and to explain how these influence digital

forensic readiness in the context of a South African organisation. The researcher did not perceive that, it is a question of causality but rather the meaning individuals attached to the concept of digital forensic readiness.

This study adopted an interpretive approach. The goal of this study is to understand the factors that influence digital forensic readiness and to explain how these influence digital forensic readiness in the context of a South African organisation The study does seek to understand causality but rather the meaning individuals attach to the concept of digital forensic readiness is what is important in this study.

The researcher believes that by interacting with the study participants, a new insight will be obtained as how and to what extent various factors influence digital forensic readiness in a South African organisation. The researcher also believes that, during the interview process, a new knowledge will be obtained as to how the various factors are aligned to influence digital forensic readiness.

The epistemological assumption of interpretivism is that the findings of the study are created as the investigation is proceeding (Andrade, 2009). Based on the issues raised above, the interpretive paradigm seems to be suited to address the research questions in this study.

The study employed the inductive approach to theory because it moves from specific observation to broader generalisation and theory development. The inductive approach helps the researcher in deciding how to categorise data that emerge from field notes, interviews and documents (Wilson, 2010).

3.2 Research Methodology

This study followed a qualitative research methodology, because the qualitative method is regarded as being able to glean in-depth information from the study participants. Qualitative research assists the researcher to understand people within their social as well as their cultural contexts (Easterby-Smith, 1991). In qualitative research, the researcher selects the sample purposefully rather than randomly. Qualitative methodology regards people as participants as opposed to quantitative positivists who regard people as objects. Qualitative research findings are reported descriptively by using words (Mutch, 2005). The goals of the qualitative method are not to generalise but to describe or explain what is happening. The aim of the qualitative method is to establish

the socially constructed nature of reality. The other aim is to stress the relationship between the researcher and the study subjects (Denzin & Lincoln, 1994). The qualitative researcher seeks to achieve an insider's view by talking to the study participants or by observing their behaviour in a subjective manner (Welman, Kauger and Mitchell, 2012). In qualitative studies, the researcher's subjectivity is regarded as something that cannot be eliminated but the researcher is seen as an instrument in the data collection process (Maree, 2010).

3.3 Research Method

From Myers (2009), a case study approach was identified as a suitable method to conduct the qualitative interpretive research. Based on the requirement to obtain an in-depth understanding of the factors that influence digital forensic readiness and how factors influence digital forensic readiness in a South African organisation, the interpretative case study was selected. The research used a single case of a South African life insurance company.

The case study seeks to understand or explain a contemporary real-life situation, specifically when the boundaries between contexts are not evident and in which multiple sources of evidence are used (Yin, 2003; Ghauri & Grønhaug, 2005; Sekaran, 2003). Case study research can be divided on the basis of single and multiple case studies (Yin, 2003; Ghauri and Grønhaug, 2005; Sekaran, 2003).

The case study is commonly used in information systems research due to the fact that it is appropriate for studying organisational systems (Yin, 1994). According to Yin (2009), a case study is an empirical inquiry that investigates real-life context, especially when the boundaries between the phenomenon and the context are not clearly evident and in which multiple sources of evidence are used. Case studies are used when a researcher is addressing either a descriptive or an exploratory issue or both, i.e. what, how or why an event is happening or happened (Landsberger, 2000). Case study research design is useful when a researcher is answering the how and why questions regarding the phenomenon. Because the case study is conducted in a natural setting, it enables the researcher to grasp a holistic view of the phenomenon (Orlikowski & Baroudi, 1991).

However, case studies have been accused of lacking rigour. Case studies provide little basis for generalisation because of the small number of participants. According to Yin

(1984), case studies are also difficult to conduct due to massive amounts of documentation. Case study research is criticised for lacking rigour and for not displaying statistical properties of research (Yin, 1994). Having noted the case study criticisms, the researcher tried to ensure all evidence relating to the findings was fairly reported. This was done by creating case reports immediately after the interviews in order to avoid information decay. This also enabled the researcher to avoid massive and unreadable documents (Wilson, 2010).

3.4 Case Site

The site the researcher selects should be suitable and feasible to conduct the study (McMillan & Schumacher, 2001). The site identified for the purpose of this study was at South African Life Insurance Company. The organisation is one of the largest life insurance companies in South Africa. The selected site was suitable and easy to access.

The company has almost 10,000 employees. The company has a separate IT, auditing, forensic and risk management departments. The various departments collaborate when an investigation has to be conducted. The company is aware of digital forensic readiness. The case study company is referred to as XYZ Company to in order protect its identity. XYZ Company was selected because the researcher previously worked for the company and permission to conduct the study within this company was easily obtained by the researcher. The researcher has a fair understanding of the organisational culture in the company; in addition, he knows some of the company decision makers.

The following people were identified and selected to participate in this study; purposive sampling was adopted to select the participants:

- Head of Forensic Department
- Forensic Manager
- Forensic Intelligence Officer
- Corporate Governance Executive
- Chief Information Security Officer (CISO)

More information regarding the above participants is provided in Chapter 4, Table 2.

3.5 Data Collection

Data was collected using two methodologies: the primary data collection and secondary data collections methods. Primary data are new data that are gathered for the research

project. Secondary data, on the other hand, include data that are available from other sources such as, books, magazines, company documents, internet and journals (Struwig & Stead, 2009).

3.5.1 Primary Data

Primary data in this study was collected using semi-structured interviews as a data collection tool. The interviews are a key ways of accessing the interpretation of participants in the field (Walsham, 2006).

The semi-structured interviews enable the researcher to understand the constructs that the interviewee used as basis for his or her opinions and beliefs about a particular matter. The researcher used the semi-structured interviews to develop an understanding of the participant's world (Collis and Hussey, 2009). The reason for using semi-structured interviews is because they allow the participants to respond freely. Semi-structured interviews help the researcher to focus on the research area. Semi-structured interviews also allow the researcher to examine verbal and non-verbal communication (Wilson, 2010).

The interviews were arranged and limited to 30-45 minutes to ensure quality information was obtained and to prevent participants from getting tired or bored. Before the start of the interview, the researcher first explained the nature and the purpose of the study. The purpose of this was to get the interviewee to feel less apprehensive about what was to follow. The researcher clarified all the issues relating to anonymity and confidentiality (Wilson, 2010). This was to encouraged participants to fully cooperate and to provide quality and detailed information. The researcher avoided using threatening words or words that are unfamiliar to the respondent. In cases where the interviewees were showing signs of resistance to answer a particular question, the researcher dropped that question and found an alternative question to address a particular issue. The interviews were conducted at the work premises of the participants.

The interviews were recorded and permission to do so was obtained from the participants. This was to ensure the researcher was adhering to good ethical behaviours in conducting the research (Struwig and Stead, 2009). The interview recordings enable the researcher to return to the transcripts later for an alternative form of analysis and are useful for picking up quotes when writing the research report. The most important

benefit of interviews is that they free the researcher in order to concentrate on engaging with the participant (Walsham, 2006).

The semi-structured interview questions consisted of general and specific questions, included open-ended questions. The benefit of open-ended questions is that they allow respondents to respond in more detail. Open-ended questions can provide some interesting qualitative findings which may lead to new insight for future research. In order to gain maximum information, the researcher probed the interviewee by asking questions that require the interviewee to elaborate on his or her statements (Collis and Hussey, 2009).

The researcher developed the interview guide to assist in collecting data. The instrument was validated by piloting the interviews with colleagues (Mpazanje, 2009, Collis and Hussey; Struwig and Stead, 2009). The researcher acknowledged his biases, beliefs and background might affect or distort data and research findings. The researcher entered the research site with necessary care and engaged with the participants in an open and enthusiastic manner; this was to gain maximum trust from the participants.

The interviews were supplemented by other forms of data collection, such as media publications, internal documents, direct observation, web-based data from e-mails and the company website.

3.5.2 Secondary Data

The secondary data collected included reviewing the existing literature on digital forensic readiness and the organisation's documents to gain more insight. The company's communications newsletter was reviewed to validate whether the company conducts an awareness program on fraud and digital crime. The newsletter reviewed did indeed confirm that the company is constantly making staff aware of the dangers of sharing and compromising passwords. The other documents that were reviewed were the organizations forensic and fraud policy as well as the information security policy. Both these documents confirmed that the organisation is serious about collecting evidence and prosecuting those found guilty as well protecting the company's information assets.

3.5.3 Research Timeframe

Cross-sectional studies enabled the researcher to examine empirical material at one point (Hendricks, 2005). The cross-sectional design was appropriate because it enabled the

researcher to complete research in the given time limitation. The data collection was done from mid-August 2013 to mid-September2013.

3.6 Data Analysis

Qualitative data was analysed using non-quantifying data analysis methods. Qualitative data analysis is usually based on an interpretative philosophy that is aimed at examining meaningful and symbolic content of the qualitative data. It seeks to establish how participants make meaning of a specific phenomenon by analysing their perceptions, attitudes, understanding, knowledge, values, feelings, and experiences in order to approximate their construction of the phenomenon (Maree, 2010).

3.6.1 Data Analysis Strategy

Content analysis is a systematic approach to qualitative data analysis. Content analysis strategy identifies and summarises written information such as books, brochures, written documents and transcripts. It is a process of looking at the data from different angles with a view to identify key concepts in the text and to help one to understand and interpret raw data. Content analysis is an inductive and iterative process where the researcher looks for similarities and differences in the text that would corroborate or disconfirm theory (Maree, 2010).Through this strategy, the researcher was able to identify the similarities between theory and practice as well as to use the analysis to compare it with theory. Collis and Hussey (2009) referred to content analysis as a method by which selected items of qualitative data are systematically converted to numeric data. Content analysis strategy was utilised to analyse the collected qualitative data. The strategy enabled the researcher to interpret the analysed the transcriptions. The strategy is suitable for the interpretive inductive approach because it has enabled the research to identify similarities or contradictions within the transcriptions. The strategy enabled the researcher to confirm or not what has been indicated in the literature. The analysis also enabled the researcher to interpret and explain the extent to which the identified factors influence digital forensic readiness in a South African organisation.

3.6.2 Data Analysis Process

The recorded data from the interviews was first transcribed by the researcher. Based on the discussion above, the content analysis was found suitable for analysing data as the researcher was looking at summarising data in order to interpret it. The researcher

determined the coding units such as words or themes that were found in the interview recordings or notes. Maree (2010) defines coding as a process of reading carefully through the transcribed data, line by line, and dividing it into meaningful analytical units. The process of coding involves finding meaningful segments of the text in the transcript and assigning a code to signify that particular segment. The coding approaches include inductive and priori. In the case of inductive coding, the codes are developed by the researcher by directly examining the data. In such a case, the researcher lets codes emerge from the data. The priori approach, on the other hand, involves developing codes before examining the current data. This involves identifying certain codes from the empirical studies dealing with the researcher's topic. The researcher did this while conducting the literature review (Maree, 2010).

For the purpose of this study, the priori coding approach was used. This enabled the researcher to identify the themes before categorising data in advance and the search data for these topics. The researcher started to identify concepts that relate to the research topic before categorising the raw data; these provided direction for what the researcher was going to look for in the data. Such concepts emerged from the literature review: how the existence of forensic policy has been emphasised as an important contributing factor in successful prosecutions. The researcher turned this into a category for data. From the interview transcript, the researcher was able to find codes that relate directly to this category.

3.7 Reliability and Validity

After every interview session, the researcher spent some time adding notes. By so doing, the researcher was avoiding information decay. This was also to ensure that all the evidence pertaining to the findings was fairly reported (Mpazanje, 2009). The researcher justified the research findings by addressing issues relating to its reliability. Reliability is concerned with the manner in which raw data is transformed into an analysable format. It involves transcribing and coding of data. In addressing reliability, the researcher considered how his inference that has gone into transcript and into set of codes. By so doing, the reader will be able to determine whether the researcher's interpretation can able to be relied upon (Lee and Lings, 2008).

With regard to internal validity which Guba and Lincoln (1994) referred to as credibility, the researcher considered various ways to assure that the conclusions are valid. To do

that, the researcher audio taped and took notes during the interviews with the participants (Guba and Lincoln, 1994). Credibility is concerned with whether the research was conducted in a manner in which the subjects of the study were correctly identified and described (Guba and Lincoln, 1994).

Triangulation was one way the researcher used to enhance the validity of the findings. Triangulation entails collecting material in as many different ways and from as many diverse sources as possible. This helped the researcher to "hone-in" on a better understanding of a phenomenon based on different angles, e.g. interviews, company documents, newspapers, journal articles etc. (Terre Blance, Durrheim and Painter, 2007).

In order to ensure findings are consistent with the theory, company documents such as the forensic fraud and information security policies were reviewed. These confirmed what the literature indicated. For example, the forensic policy of organisation XYZ spells out what the Forensic Department should be doing with regard to forensic investigations. After the interviews were complete, the transcripts were submitted to the participants to correct any possible errors. The findings were also submitted to the case study company for comment and for their interpretation and conclusion. The oral comments from the case study organisation also agreed with the findings, especially on the need for a fraud awareness drive that must be driven from the top down.

The other method the researcher used was respondent validation, which involves taking the early results back to the research participants to confirm whether the researcher is on the right track (Lee and Lings, 2008).

Transferability is another issue that the researcher considered with regard to the findings. Transferability refers to whether the research findings can be applied to another situation that is similar in order to permit generalisation (Collis and Hussey, 2009). The researcher considered whether the findings based on organisation XYZ can be used to generalise about the factors that influence digital forensic readiness in a South Africa organisations. To provide transferability, the researcher provided an in-depth description of the research methodology, such that any person contemplating the application of the same study in another setting would have a sufficient base for the comparison of similarities (Kyobe, 2012).

Dependability refers to the replication of the study in the traditional sense, and how to achieve it. The researcher has kept a justifiable and organisable record of data, findings and interpretations (Kyobe, 2012). The researcher ensured the research process was systematic, rigorous and well documented, ensuring that the same method could be utilised for future research.

3.8 Ethical Considerations

Ethics in research refers to conducting a study on moral grounds. Ethics provides the researcher with a code of moral guidelines to be followed in order to conduct research in a morally acceptable manner (Struwig & Stead, 2009).

Participation in this research was voluntary. The researcher informed participants that they are free to decline participation in this study as the study is for educational purposes. Formal consent to conduct the study was obtained from the life insurance company, as well as from the University of Cape Town Ethics Committee.

In order to observe confidentiality, the researcher requested the participants not to provide their names. The name of the organisation where the research interviews were conducted has not been revealed. The researcher has discussed the findings of the research project with the management of the company to ensure that it is a true reflection of the situation under study. This was also to give management the opportunity to comment on the research findings.

3.9 Limitations of the Research

One limitation was the lack of availability of chosen participants as the planned time of data collection coincided with the working hours of the participants. Organizational culture, privacy and trust issues also affected the research process, because the researcher was requested to sign a non-disclosure agreement with the organisation.

The study focused on a single South African life insurance company that was used as a case study to conduct the study. The researcher assumed that the respondents would have enough knowledge about digital forensics readiness and would be able to clearly articulate answers to the interview questions. The participant's limited knowledge of this concept has affected the manner in which they were able to express themselves in response to the interview questions. The other limitation of this study is that, the results of the study may not be generalizable. The participants for the study were selected from

the case study company and did not include subjects outside this company. The participants included both junior and senior staff members from the case study company. The purpose of this was to narrow the scope of the study because a huge sample would have required more time to collect data.

3.10 Conclusion

In this chapter, the philosophical paradigm was discussed. The chapter also indicated that the study followed a qualitative approach and the research strategy used was a case study strategy.

The following chapter presents the analysis of the collected qualitative data as well the analysis technique used in this study. The following chapter will also provide the reader with descriptions of the sample, empirical findings and a discussion of the findings.

Chapter 4: Analyses, Research Findings and Discussion

The purpose of this chapter is to present and analyse the research data obtained through the literature review, interviews and observations. Chapter 4 will also give a detailed description of the sample, empirical findings and discussion of the findings.

4.1 Sample Description

The selection of respondents for the qualitative research was that they should be a member of the company's incident response team, as they have knowledge of the manner in which forensic investigation is conducted within the organisation. The selected respondents were in a position to answer more detailed questions regarding factors that influence digital forensic readiness in the organisation because of previous exposure to incidents of unethical behaviour in the company. Most of the respondents held leadership positions in the organisation and represented the Forensics Department, IT Department, and Corporate Governance Department. Five interviews were conducted for this study. The composition of the respondents was four men and one woman. Semi-structured face-to-face interviews were used to collect the primary data. The primary data gathered during the semi-structured personal interviews are discussed and analysed in the following sections. Table 2 below provides biographical details of the respondents.

Table 2: Biographical details of respondents

Respondent	Position In The Company	Years In This Position
A	Forensic Intelligence Officer	15
B	Head of Information Security	17
C	Corporate governance Executive Manager	10
D	Head of Forensics Dept.	20
E	Forensic Manager	18

4.2 Qualitative Data Analysis and Findings

The researcher conducted five interviews and then manually transcribed them. The initial analysis involved the manual noting and counting down of themes that emerged from each interview. The collected data was then processed using Microsoft Excel. This was done by capturing the number of themes per interviewee in Microsoft Excel and creating bar chart.

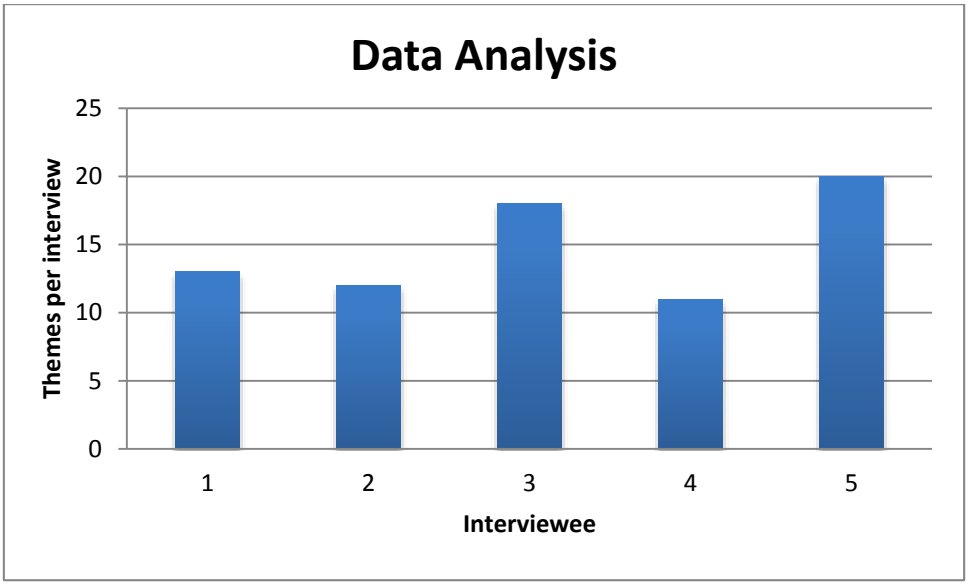

Figure 4: Initial data analysis

Figure 4 indicates themes that emerged per interview. The diagram also shows that more themes emerged from the participants who are more concerned with forensic investigation. The interviews were carried out during normal business hours and could have contributed to fewer themes emerging than from other participants.

The objective of this study was to determine the factors that an organisation needs to consider when designing and implementing a digital forensic readiness program. The themes that were considered as important were drawn up and reflected in the thematic network map, illustrated in Figure 5.

The thematic map affirms that the organisation considers the factors that were identified in the literature as important when designing and implementing digital forensic readiness. The themes covered forensic policy, corporate governance, legal and ethics as well as technology and infrastructure.

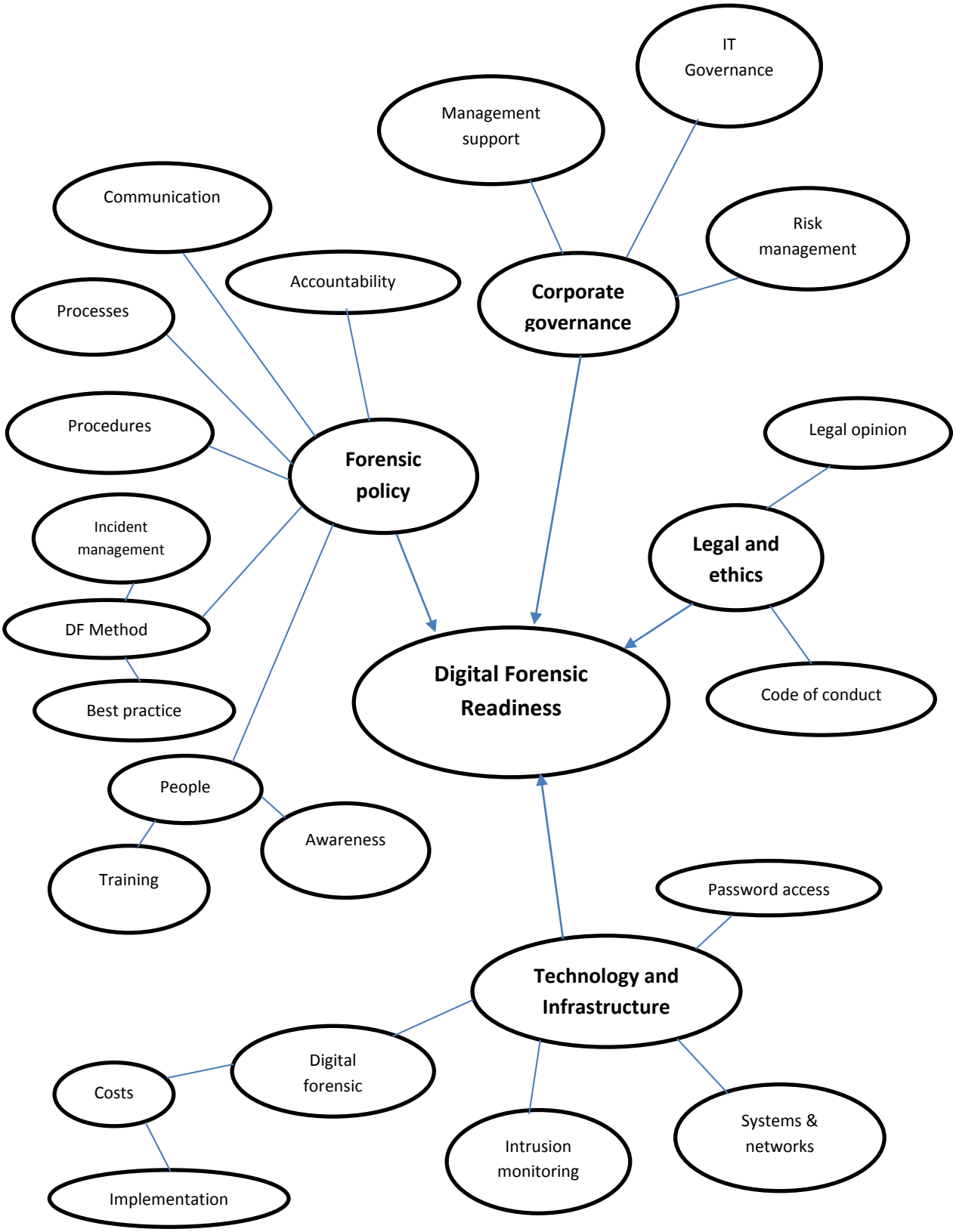

Figure 5: Thematic Analysis Map (Braun & Clarke, 2006)

4.3 Discussion

Various factors were reported as having a significant influence on digital forensic readiness. The following sections discuss these factors in the context of the findings and the lessons learned in this study as well as implications thereof for a South African organisation that wants to be digital forensic ready.

4.3.1 Corporate Governance and Strategy

The success of digital forensic readiness depends on top management support (Grobler and Louwrens, 2010). The recognition of the importance of digital forensic readiness by top management influences the allocation of finances and other resources that are aimed at protecting the organisation's resources (Barske at al., 2010; Whyte et al., 2011).

The findings show that the purchase of an expensive monitoring system was supported by top management. Without top management buy-in, it is difficult to implement any digital forensic readiness initiative, because some of these initiatives are expensive. The approval for the purchase of such a system is an indication that top management acknowledges the need to proactively collect digital evidence.

"The tool that Forensic Department acquired two years back cost the organisation a lot of money and top management approved. It is because they know the value of that system to the organisation" (Respondent B).

According to the literature on corporate governance, top management is responsible for protecting the organisation's security posture (King report II on Corporate Governance, 2009). Corporate dimension includes strategic, tactical and operational management requirements (Grobler, Louwrens and Von Solmms, 2010). The literature further states that IT infrastructure, applications and information of the organization is the responsibility of top management. Top management must make sure there are proper controls and measures to protect the assets of the organisation (Sarbanes-Oxley Act, 2002, and King 2 Report on Corporate Governance, 2003).

The general sentiments among participants were that corporate strategy encourages the establishment of various committees that will deal with risk issues and fraud related matters. This is in line with the literature regarding the role of top management (King 2 Report on Corporate Governance, 2003). The data reveals that there are IT Governance, Enterprise Risk, Corporate Governance, and Information Security Committees that have been set up to look at the issues of risks and threats the organisation may face. This is an

indication that the organisation security posture is taken seriously by top management. The responses from two participants confirm this:

"Top management have realised that being ready is an important thing and can't get it wrong" (Respondent A).

"Digital forensic readiness is addressed in a number of committees and forums" (Respondent C).

4.3.2 Policy

Forensics policies help organisations to detect computer crimes and to be able to position them so that they can respond to an attack successfully (Yasinsac and Manzano, 2002). According to Barske, Stander and Jordaan (2010), policies serve as a guide for employees in carrying out their work functions. All respondents confirmed that the company has a forensic policy. They also confirmed that the policy is available on the company's intranet for the employees. The general understanding among the respondents is that the policy forms part of the organisation's broader commercial crime, anti-money laundering and staff misconduct policy frame. The policy serves as a guiding tool for all the employees in the organisation. This shows that the organisation communicates its policies to everyone in organisation. This concurs with the response from participants, below:

"Group policy stipulates behavioural aspects of what group forensic team will be doing and what business units will be doing" (Respondent C).

"It is a broad policy in terms of where the responsibilities and accountabilities regarding general investigation etc. In terms of action steps by the individual, that obviously relates to their objectives and Key Performance Indicators (KPIs)" (Respondent D)

Landman (2002) recommended that security professionals must consider both their policies and their technical actions in the context of a legal framework. For example, before you monitor and collect data related to computer intrusion, you must be authorised to do so by the administrator (Landman, 2002). Well-defined forensic policy provides the organisation with the authority to conduct a forensic investigation in a legal manner (Barske, et.al, 2010). The findings indicate that forensic investigators are authorised by the top management to conduct investigation where it's necessary. This is confirmed by a comment made one of the participants:

“We are mandated by the board and it comes from top management down. Based on our mandate, we don’t have to ask permission to investigate. If there deem a need to investigate, we will investigate” (Respondent E).

In the process of data collection, the researcher also analysed company documents such as the group forensic service charter, fraud and risk policy, newsletter and the information security policy. According to the forensic charter, the group forensic services have the responsibility of delivering a centralised, independent and objective forensic service to the group. The charter also specifies the action tasks that group forensic service needs to undertake, such as formulation of a policy framework that defines roles and responsibilities as well as the processes to be adopted in dealing with fraud and risk related matters, e.g. forensic investigation. This is in line with the literature; organisations need to develop forensic policies that assist employees in carrying out the mandates (Grobler, Louwrens, and Von Solms, and Whyte, et.al, 2011). The findings reveal that the forensic department works independently and investigates whatever is to be investigated. This concurs with comments of one of the participants who said:

“So basically we are sitting from the outside and looking inside. So nobody can say to me you can’t investigate this and you can only investigate that. So in a sense we are seen to be independent, which also add a lot of value to it” (Respondent E).

The development of good forensic policies improves the success of a digital forensic investigation (Yasinsac and Manzano, 2002; Whyte, et.al, 2011). The findings show that a forensic policy is in place to define procedures to be followed when theft or fraud is suspected or committed. This is also in line with prior research indicating that forensic policy guides investigators when conducting forensic investigations (Yasinsac and Manzano, 2002).

“The policy procedure serves as guide when an incident has happened and an investigation has to be taken” (Respondent A).

The results of this study show that it is critically important that organisations establish a forensic policy that sets clear standards and guidelines for conducting forensic investigations. Failure to have a well-defined forensic policy might result in the organisation not having something to fall back on when something goes wrong during and after the investigation process. The presence of a forensic policy ensures that a standardised approach to investigation and adherence to both legal and regulatory

requirements. However, having guidelines and policies is not sufficient, as employees might not be aware of them. It is therefore important that these are well communicated to all employees and are understood by those involved in forensic investigation work. Organisations should have regular independent audits and checks in place to ensure that forensic procedures are followed at all times. Organisations should also ensure that forensic policies are reviewed once a year as legislation and regulation change (Whyte and Claims, 2011).

4.3.2.1 Training and Awareness

It is stated in the literatures that the organisation training's forensic policy empowers the investigators to perform their duties efficiently and effectively (Grobler ,Louwrens, and Von Solms,2010; Whyte, et.al, 2011). On the other hand, the awareness initiatives encourage staff members to be vigilant and to contribute positively towards fraud and crime fighting programs (Rowlinson, 2004; Poope and Labuschagne, 2012). The training and awareness initiatives influence the extent to which the members of the organisation contribute towards the fight against fraud and crime. The data shows that forensic investigators are following policies when conducting investigations. This is confirmed by a comment made by one of the participants.

"Policy reinforces discipline in forensic investigators" (Respondent D).

The organisation communicates some of their awareness initiatives through its newsletters. The researcher analysed the contents of the newsletter to establish whether awareness is being addressed in it. Awareness on the protection of password features in the organisation's newsletter. The findings show that some awareness initiatives are being conducted but not as rigorously as indicated in the literature. This concurs with the response from three participants:

"There's no big drive from strategic point of view that I'm aware of" (Respondent A)

"At the moment, we don't run any awareness campaigns" (Respondent C)

"We believe in spending 80% on what is relevant and 20% on what is not important to forensic unit" (interviewee D). This implies that staff not involved in forensic work, such as receptionists, are not regarded as important in contributing towards fraud fighting and reduction.

The problem that the researcher identified in the case study organisation is the lack of a big drive for forensic training and awareness initiatives. The organisation's forensic

training and awareness initiatives are only focusing on employees who are involved in forensic investigation work. This is confirmed by respondent D above. The problem with this approach is that those who are not involved in forensic work are left vulnerable to criminals. It is important that the case organisation recognise that people are both the most important asset and the weakest link in the organisation's security chain. The lack of training and awareness initiatives may also results in employees not knowing how to behave and what to do when an incident has occurred in the organisation. This is a recipe for evidence being contaminated.

According to respondent D, there is no big drive for the training and awareness initiative from a strategic point of view. This is contrary to the existing literature. In order to address this problem it is important for the case study organisation to incorporate the forensic training and awareness initiatives with the organisation's overall training strategy. This view is supported by Grobler and Louwrens (2009) and Labuschagne (2012).

The extent of fraud in South Africa's financials services, especially in the life insurance industry, requires organisations to spend more effort in conducting awareness initiatives. The Association of Savings and Investments of South Africa (ASISA) statistics of 2009 indicated that death and funeral claims were the largest contributors to insurance fraud. The statistics also revealed plus-minus R364.9 million related to fraudulent and dishonest claims, an average of R111 726 per claim (ASISA survey, 2009). Failure to embark on these initiatives might result in staff members not being aware of fraud they commit and the implications thereof.

4.3.2.2 Procedures

A well-defined forensic methodology improves an organisation's ability to collect evidence and to prosecute the culprits (Grobler and Louwrens, 2010; Whyte, et.al, 2011). Unclear and not well-documented forensic methodology may result in some confusion to the investigators. This may, in turn lead to non-adherence to proper investigation process. It is important for organisations to establish a well-defined forensic methodology which will ensure uniformity in conducting investigations and adherence to international best practices (Landman, 2002; Whyte, et.al, 2011).

The findings demonstrate that the organisation is following the international investigation best practice to improve their successful prosecution rate. The South

African courts accept digital evidence if the process followed to gather it meets the international practice of investigation (ECT, 2003). However, the majority of the participants seem to be not sure what forensic methodology is used by the organisation when conducting investigations. This is an indication of a lack of proper communication from management. The responses from two participants confirm that this is the case:

"Majority of methodology cases are dealt with by (head of forensics). He would be the right person to answer as to what kind of forensic methodology the organisation is following "(Respondent E).

"I'm not familiar with what forensic methodology is being followed by forensics department when conducting an investigation "(Respondent B).

Because digital evidence is very volatile, it can easily be contaminated or compromised. According to Grobler and Louwrens (2010), it is important that digital evidence is handled correctly. The data reveals that an incident project management team is established when an incident has occurred. The team sets priorities for the project and ensures the best people from various business units are assigned for specific tasks. This is an indication that there is collaboration between various business units within the organisation. This collaboration enables the organisation to pull different expertise from various sources when investigating an incident. However, the literature states that the development of an evidence management plan should concentrate on identification, legal gathering, preservation handling, retrieving and archiving of comprehensive digital evidence (Grobler and Louwrens, 2009)

4.3.3 Legal and Ethics

The Legal Department is to assist the Forensic Department wherever possible to ensure all evidence gathered is legally acquired (Thomas 2004). The good relationship between Legal and Forensic is important to ensure that the organisation's evidence collection procedure and tools are compliant with the legal requirements. Rowlingson (2004) asserts that the Forensic Department needs to obtain legal opinion when building a case and after the case has been established. In the South African context, various legislation demands certain requirements for evidence to be admissible in a court of law. For example, the Electronic Communication and Transaction Act (2003) have certain requirements for determining the admissibility of a digital document or digital evidence in a court of law. The Act placed the reliability of evidence in the manner in which that

evidence was recorded and communicated. The Act also placed reliability on how the integrity of the data was maintained, and the manner in which the originator or author of the record was identified (ECT Act, 2003).

All respondents were in agreement that there is good collaboration between Legal, Compliance and Forensic Departments. This collaboration assists in ensuring forensic policies are aimed that are at securing and protecting the organisation's information assets. The findings confirm the importance of a good collaboration between the forensics and legal professionals. This is an indication that the organisation is serious about protecting its image and integrity.

"Collaboration is there and interaction among various business units to ensure what needs to be done is done" (Respondent D).

It is critical that the Forensics Department obtains legal opinion when building a case, as well as during and after the case has been established. This is to ensure the credibility of evidence and that it will withstand the scrutiny of the law (Rowlingson, 2004; Thomas, 2004). The findings reveal that the Forensic Department provides legal advice to legal professionals, contrary to recommendations from prior research. This is confirmed by response from two participants that the Legal Department asks the Forensic Department for opinions regarding a forensic matter:

"Forensics team give more input to legal instead legal department to give input because within our team we have experienced people with legal background" (Respondent A).

"As forensic department, we are the centre of excellence when comes to forensic matters" (Respondent E).

Although there is good collaboration between the legal and forensics teams most of the prescriptions come from the forensics team, instead of legal team. This is confirmed by respondent A above. The problem with this approach is that it is contrary to the existing theory. According to the literature the legal team needs to provide legal advice to forensic teams to ensure the evidence provided will lead to prosecution (Thomas 2004). This view is also supported by Rowlingson (2004) and Whyte et al. (2011). In order to address this problem the organisation's forensic team should only provide an opinion on the technical aspects of the forensic investigation. The legal team should have the ultimate say on whether to pursue the case further, and not the other way around. It is recommended

that if an incident has been committed outside South Africa's borders the forensic team should obtain a legal opinion before proceeding with the investigation (Rowlingson, 2004).

The findings show that compliance teams within business units in our case study organisation are playing a critical role in ensuring compliance and adherence to policy procedures. This is important because it helps to improve data integrity during investigations. The importance of the relationship between legal compliance teams and the business unit can never be underestimated as it is crucial to the success of a forensic investigation. This is an interesting finding because it indicates the importance of aligning various business units' expertise for one common goal i.e. fighting against fraud and crime.

"Business units have their own compliance teams to assist them in complying with the law requirements" (Respondent D).

It was stated in the literature that setting of ethical norms in the organisation assists in guiding employee behaviour and in having a different attitude towards fraud and corruption. In other words, codes guide employees in judge what is right or wrong (Trevino, 1986). The findings reveal that the organisation has implemented the codes of conduct for all employees. All the respondents confirm that the organisation has an ethics policy in place. However, they do not call it ethics policy but rather codes of conduct.

There is a general feeling and understanding among the respondents that codes of conduct encourage employees to do the right thing and to stay away from crime. The majority of the participants also agreed that codes reinforce compliance and to know what is or wrong. This is an indication that the organisation is serious about rooting out fraud and corruption within the organisation.

However, one of the interviewees holds a different view; he said, "I don't think codes of conduct assists in changing bad behaviour because people by nature they are either good or bad" (Respondent A).

The different perceptions regarding codes of conduct is an indication that more training is needed to explain the benefits of having codes.

The study findings also revealed that, in organisations where ethical norms are not set, there is a higher likelihood that unethical behaviour would occur either in terms of defrauding the organisation or through misrepresentation. This is an interesting finding because, in most cases, it is impossible or difficult to pick up and or identify misrepresentation of facts immediately and this result in lowering the probability of being caught. For example, the case of a life insurance organisation representative who has misrepresented information on the client's policy might not be realised for a long time and after a while the incident is then realised. The financial implications resulting from this might be huge for the organisation.

It is important for the organisation to have set codes of conduct which will serve as deterrents for unethical behaviour. South African life insurance companies need to make sure business ethics are clearly communicated throughout the organisation and are part of their corporate strategy.

4.3.3.1 Technological resources

The general logs such as access logs, internal network logs, database logs etc. are possible sources of evidence (Rowlingson, 2004). Organisations can utilise computer logs and audit trails to prove crime was committed (Tan, 2001). Tan (2001) recommended that an organisation should be keep logs for future forensic investigations. All the correspondents agreed that the computer logs password system and audit trails are utilised as potential sources of evidence. The password system is utilised to ensure only authorised people access the organisation's system. The password is granted strictly for business needs only. This indicates that the organisation acknowledges the importance of organising its technological resources, such as computer logs and audit trails, in ensuring evidence is obtainable and is stored for future use

"We rely on the IT infrastructure to extract data if there has been computer crime that has been committed" (Respondent E).

The installation of an intrusion and monitoring detection system narrows the wide-scale evidence search and saves the organisation time and money during investigation (Poope and Labuschagne 2012; Barske, et.al, 2010). The intrusion detection system plays a critical role in detecting threats to an organisation (Rowlingson, 2004). The use of relevant security technology enables the business to prevent and detect computer incidents and to ensure that evidence data is available and it is credible (Barske, et.al,

2010). All the correspondents confirmed that an intrusion detection system is installed by the company to detect any security threats that might harm the organisation. The findings demonstrate the value the organisation place on the intrusion and monitoring detection system as a tool to assist the network administrator to monitor the company's network infrastructure system. The intrusion and monitoring detection system influences the organisation's ability to monitor and detect any security threats. The findings are in line with the prior research.

In order to safeguard the company's network infrastructure from being intruded by outsiders who can cause damage and loss of company important information, it is important for the organisation to install an intrusion and monitoring detection system.

The environment where data evidence is kept needs to be protected and there should be limited access to it. This is to ensure only authorised persons are allowed access to it as this will prevent evidence from being contaminated. The protection of the environment influences the credibility of evidence (Rowlingson 2004; Yasinsac and Manzano, 2002).

The findings reveal that, through the password register system, only authorised people are allowed to access data evidence. The register keeps records of who enters the store room where evidence is kept. The respondents agreed that they used the password system to ensure only authorised people are able to access the system and evidence storage place; the password system enables the organisation to be able to see who accesses the system when and what he/she did on the system. This is an indication that the organisation is serious about ensuring evidence is credible and can stand scrutiny in a court of law. Lack of a protected environment where data evidence is kept can have a negative impact on the organisation's investigation process and successful prosecution.

"We have a separate box serve that we use to keep computer logs and this is protected environment" (Respondent B).

In order to conduct digital forensic investigations, organisations need specialised tools and/or physical hardware that will make up a digital forensic toolkit (Mckemmish, 1999). It was stated in the literature that organisations need to ensure tools and techniques used by the organisation are legally compliant. The failure to do so will result in its evidence being thrown out of court (Rowlingson, 2004; Mckemmish, 1999; Barkse, et.al, 2010; Poope and Labuschagne, 2012). Local and international laws as well as regulatory bodies

require that certain conditions be met in order for the evidence to be admissible. In South Africa, for example, the Electronic Communication and Transaction ACT of 2003 placed the reliability of evidence in the manner in which that evidence was recorded and communicated as well as in how the integrity of the data was maintained, and the manner in which the originator or author of the record was identified (ECT Act, 2003).

All the interviewees unanimously agreed that the tools used for forensic investigation are compliant with the law. The findings reveal that utilisation of legally compliant tools and techniques influence the prosecution rate. This is confirmed by the response from two participants:

"We buy software from recognised and authorised vendors." and "When we buy a forensic software, we develop a matrix to check whether they comply with the law" (Respondent A).

"If one looks at our forensic prosecution success rate of 100%, this is an indication of our tools and techniques complying with law and if they were not, our evidence brought to court would have been thrown out "(Respondent B).

The researcher also reviewed the organisation's information security policy. The objectives of the policy are to protect the organisation's information assets and support role players in implementing measures that ensure information security is achieved. The policy deals with issues relating to access control, confidentiality of information, third party access, personnel security (e.g. security roles for employees responsible for IT infrastructure), etc. The findings show the organisation is serious about protecting its information assets. This is confirmed by a comment from one participant who said:

"We have an information security framework. The framework is based ISO standard. It deals with 12 areas of information security. It outlines key things that you will need to do to protect the organisation's information assets" (Respondent B

4.3.3.2 Establishment of a forensic laboratory

It was stated in the literature that a digital forensic laboratory enables the investigators to analyse digital evidence. The investigators have the benefit of using special software tools in a protected physical environment (Whyte, et.al, 2011). However, the findings of this study reveal that the reason for not establishing digital forensic laboratory was

purely a financial one. There was a lot of unhappiness from top management regarding the costs that are associated with the establishment of such a laboratory.

Findings indicate that the organisation acknowledges the importance of having a digital forensic laboratory. However, the participants felt that costs that are associated with the running of such a laboratory are so immense. According to the participants, it is better to obtain external expertise that can perform the same functions as a digital forensic laboratory at a cheaper price. This indicates that the organisation is cost conscious about the programmes it seeks to implement. This is an interesting finding, because it is important for the organisation to determine and evaluate costs against the returns on investment of such a program.

"With regard to digital forensic lab, we considered it, but it is not worth it, because it is expensive. For me to set up a digital forensic lab will cost another R4million and to run it will cost another R2 million. We rather have an expert that will assist whenever crucial evidence is required, and cheaper. I prefer to rely on one person who has all the expertise and cost me less than setting DF lab" (Respondent D)

"Digital forensic laboratory is very expensive, I would not support it. For the company of this size, you need to invest heavily to cover everything; the capital outlay would be massive" (Respondent E).

4.4 Conclusion

This chapter presented the findings of the qualitative research. The results indicate that digital forensic readiness is taken serious by the organisation and is regarded as an important element in the successful fighting of fraud and digital crimes within the organisation.

According to the majority of the respondents, it is important to have codes of conduct in the organisation as these help employees to know what is right and wrong, and to be able to comply with both the country's legal and regulatory requirements.

In general, the results indicated that the factors identified in this study do influence digital forensic readiness in a South African organisation.

The qualitative findings were generally in congruence with the literature presented in Chapter 2. There were, however, some exceptions such as the majority of the respondents not agreeing with the establishment of digital forensic laboratory. They cited the huge

costs that are associated with such as facility i.e. establishment costs as well as the running costs.

In the next chapter the summary, conclusions and pertinent recommendation of this study are presented.

Chapter 5: Conclusion

Given the extent of fraud and digital crimes affecting organisations globally and especially in South Africa, the hope of this study was help to provide insight into the factors that influence digital forensic readiness in a South African organisation. The study also hoped to provide insight into how and to what extent those factors influence digital forensic readiness in a South African organisation as well as how they are aligned to influence digital forensic readiness. The new insight would enable the organisation to review its state of digital forensic readiness and see how effective its existing measures are in assisting it to gather digital evidence and to protect its information assets. A comprehensive literature review (Chapter2) was conducted in order to identify as many factors as possible that could influence digital forensic readiness in organisations. Substantial research was also conducted on digital forensics, digital forensic methodologies and digital forensic readiness frameworks that are adopted by organisations. A digital forensic readiness conceptual model (Figure 3) depicted the factors influencing digital forensic readiness.

Given the nature of the problem statement and the research questions posed in this study, a phenomenological interpretivist research paradigm was adopted. The qualitative data collection was performed by means of semi-structured personal interviews, and was supported by secondary document analysis.

5.1 Revisiting the Research Questions

Findings of this research study are summarised according to the following research questions:

5.1.1 What are the factors that influence digital forensic readiness in a South African organisation?

The first research question was subsequently accomplished. The research findings confirmed that the following identified factors influence digital forensic readiness in a South Africa organisation: corporate governance, forensic policy, legal and ethics as well technology and infrastructure.

The data from the interviews also confirm that these factors are relevant and important when designing and implementing digital forensic readiness program.

The other factor that emerged from data interviews is staff previous experience. The data indicates that this factor plays an important role as the lessons learned from previous incidents are ploughed back to the organisation. This, therefore, enables the organisation to be vigilant about certain incidents and to implement proactive measures to fight fraud and crime. This insight will enable a South African organisation to incorporate the above factors when it wants to design and implement a digital forensic readiness program. The establishment of a digital forensic laboratory does not seem to be a prerequisite for digital forensic readiness. This is interesting and is contradictory to prior research.

5.1.2 How and to what extent do these factors influence digital forensic readiness?

The forensic policy specifies what the responsibility of the Forensic Department should be and mandates the investigator to investigate cases. The existence of forensic policy in an organisation ensures that proper forensic processes are followed when gathering evidence and that the evidence is credible. The policy assists the organisation to comply with both legal and regulatory requirements. The policy also encourages the development of training and awareness initiatives which will assist staff members to contribute towards the organisation's effort in fighting fraud and crime.

The collaboration between the Legal and Forensic Departments ensures that every aspect relating to the incident investigation is been taken into account and that evidence will be accepted in the court of law. The Legal Department provides opinion and advice on whether the process followed is legally acceptable. The Legal Department also assists in confirming whether forensic policies, tools and techniques are legally compliant.

The organisation's ethical policy plays an important role in establishing the codes of conduct. The organisation codes of conduct assist employees to know what is right and wrong and to do right by staying away from fraud and crime. In other words, the ethics codes of conduct serve as deterrents for unethical behaviour.

The manner in which an organisation's technological resources are organised influences how the organisation will go about capturing and preserving digital evidence. The environment where evidence is kept influences the integrity and credibility of evidence. If the environment is not kept safe and protected, evidence can be questioned and regarded as contaminated; it could then be rejected by the court. The tools and techniques are other factors that influence the organisation's successful investigation and prosecution; they determine how evidence will be gathered and presented in court.

The organisation's well-defined forensic investigation methodology influences uniformity in conducting investigations. A well-defined methodology assists the investigators to follow and adhere to international best practices and to ensure compliance to legal requirements

The support and involvement of top management has a strong influence in the establishment and implementation of the digital forensic ready environment. If this support is not obtained, the organisation's financial resources will not be available for such an environment. The involvement of top management in digital forensic initiatives ensures the establishment of policies and committees that will ensure there are proper control measures to protect the resources and assets of their organisation.

5.1.3 How these factors are aligned to influence digital forensic readiness?

The development of policies such as forensic policy, information security, ethics policy is aligned to address issues relating forensic investigation, information security management and risk as well as the employee ethical conduct. The forensics policy stipulates what needs to be done when conducting forensic investigations, while the information security policy ensures the organisation's information assets are protected and safeguarded. The organisation's ethics policy ensures the organisational values are maintained i.e. adhering to zero-tolerance towards fraud and crime.

Legal services within our case study organisation are decentralised. There is legal team is sitting within the Forensic Department in this case study organisation. The purpose of this is to establish a good working relationship among the two teams. A stronger relationship means that, when an incident occurs, both teams will pull their resources to ensure evidence is legally obtained and that the culprits are prosecuted. The legal compliance teams are established within business units. This is to ensure everybody in the organisation complies with organisational policies and that adherence to legal requirements is always maintained.

The computer logs, audit trails and the password system register are organised to such an extent that evidence is captured and preserved. This is to ensure evidence is available when require for an investigation.

The forensic investigation methodology is aligned with the forensic policy. The methodology operationalises the aspects of the forensic policy i.e. the forensic policy stipulates what needs to be done and the methodology specifies how it should be done.

Top management involvement ensures that the organisation has proper control measures to protect the resources and assets of their companies. Through an integrated framework, various policies are developed to manage and protect the organisation's information security and risks.

5.2 Contributions of the study

The successful design and implementation of a digital forensic readiness program depends on a number of factors. The developed conceptual model in Chapter 2 summarises the most important factors a South African organisation needs consider when it wants to create a digital forensic ready environment. It also helps them to understand the issues that are involved when designing a digital forensic readiness program. Over and above, the model presents a view on the current state of knowledge regarding digital forensic readiness.

5.2.1 Findings

The findings indicated that the identified factors (corporate governance, forensic policy, legal and ethics as technology and infrastructure) significantly influenced the state of digital forensic readiness. In order to design and implement a successful digital forensic readiness environment a South African organisation needs to consider these factors. The alignment of these will ensure good collaboration from various business units.

The existence of corporate governance structures in the case study is in line with the existing literature on protecting the organisation's assets. According to the King II report (2003) and Sarbanes-Oxley Act (2001), it is the responsibility of top management to ensure that there are proper controls and measures to protect the organisation's position.

The case study organisation follows a well-defined forensic policy when conducting forensic investigations. Following a well-defined policy has assisted the organisation to improve their prosecution rate. This is congruent with the existing opinions that policies serve as a guide to assist members of the organisation to carry out their responsibilities efficiently and effectively (Barske, Stander, and Jordaan, 2010).

The organisation of technological resources is utilised by the case study organisation to ensure that the evidence acquired is forensically sound. The technology and tools used by our case study organisation is compliant with the legal requirement, hence their cases have never been rejected in court. This is also congruent with the existing literature that organisation need to make sure the tools and techniques to gather evidence is legally compliant.

The major finding in this study is the disagreement with literature on the establishment of a digital forensic laboratory by an organisation. Although the existing literature emphasises the importance of establishing such a laboratory in practice the establishment costs seem to be the determining factor. According to the case study organisation the set up and running costs are huge. The organisation is of the opinion that it is more cost effective to hire someone who has the same expertise, than the digital forensic laboratory can offer. This is not in line with the literature as a financial decision determines whether such a laboratory is worth establishing. This finding means that organisations need to consider and evaluate all the costs that are associated with each of the identified factors when designing and implementing a digital forensic ready environment.

With regard to the legal dimension the case study complies with the legal requirements when conducting an investigation. This is in line with the existing opinions that failure to adhere to the legal requirements may lead to a poor prosecution rate. However, the organisation slightly deviates from existing theories regarding the acquisition of legal opinion from legal professionals. This deviation is not in line with existing literature and this might a problem in future.

5.2.2 Relevance of the Research Methodology

A contribution has thus been made by gathering in-depth qualitative data which would not otherwise have been obtained if a quantitative approach had been used. This is because some in-depth information does not lend itself to acquisition by means of quantitative research.

The qualitative research paradigm has enabled the researcher to explain how and to what extent the identified factors influence digital forensic readiness in a South African organisation. It has also enabled the researcher to explain how these factors are aligned to influence readiness. Using the quantitative approach would not have enabled the

researcher to explain the above influence and alignment. The qualitative case study approach also enabled the researcher to interact with the participants in their environment and this provided the researcher with a better understanding of the situation and phenomenon.

According to the researcher's best knowledge, there has been no other research or study that has been conducted on this specific topic with regard to South African organisations. Because of this, the researcher was unable to compare the current findings with any of the existing research work.

5.3 Limitations

The study attempted to contribute to the body of knowledge relating to digital forensic readiness in South African organisations. Although specific areas pertaining to the successful implementation of digital forensic readiness were explored, a greater understanding of the factors that influence digital forensic readiness has been attained; new opportunities for future research have also been identified. As a result, limitations of the present study and recommendations for future studies are suggested below.

The use of a single organisation in this study has been a limitation because experiences of other organisations might have been different from our case study organisation. The experiences of the Small Medium Enterprises (SME's) might be different to those of big organisations. For example, SME's might find it difficult to have a legal department within their organisation that could assist them to ensure they comply with digital forensic legal requirements. The costs associated with the establishment of such a department are huge and SME's cannot afford them. Also the costs of establishing a digital forensic laboratory make it difficult to establish it within their premises.

The extent to which the sample of the qualitative study represents the population is questionable; maybe more interviews from different organisations could have revealed a different set of data. A future quantitative study is recommended in order to supplement the current study. However, the researcher is of the opinion that because the case study company is large enough, it is possible to generalised findings.

5.4 Recommendations

It is important that the South African organisation should establish a well-defined forensic policy that will mandate and provides guidelines for forensic investigations. It is

also important that the organisation should review its forensic policy once a year as legislation and regulations changes. For example, with the signing into law of the Protection of Personal Information (POPI) Act, South African organisations need to ensure their forensic policies are aligned with it (Protection of Personal Information Act, 2013). It is recommended that such a policy should assist in developing a forensic training and awareness program. The lack of a big drive for training and awareness initiatives in the case study organisation is a concern that top management needs to address urgently. This training initiative should also be directed to legal professionals so to be better equipped to deal with any cyber-crime relate cases.

The extent of fraud in South African organisations, especially in the financial services sector, requires constant training of staff and conducting of fraud awareness initiatives. It is therefore important for the South African organisation to spend more effort in conducting awareness initiatives to educate their employees about digital crimes.

Although the forensics team has better insight regarding digital crimes it is important to obtain a legal opinion before pursuing prosecution. The reason for this is that some cases might involve residents from other countries. The legal team should play a lead role at all times. This is to ensure the case(s) is winnable in a court of law.

Although the literature emphases the establishment of a digital forensic laboratory within an organisation, it is important for the organisation to determine and evaluate costs against the returns on investment of such a program.

Lastly, the implementation of digital forensic readiness initiative requires top management buy-in. It is therefore important that those responsible for forensics, risks, and information security convince top management about the dangers of not implementing readiness initiatives.

While not the focus of this study, it would be interesting to measure the relationship of the identified factors that influence digital forensic readiness and to develop a measuring instrument that will empirically test the relationships of these factors as described in the conceptual model. A further study could also focus on the implementation of the recommendations put forward in this study pertaining to the factors influencing digital forensic readiness in South African organisations.

5.5 Concluding Remarks

The successful implementation of a digital forensics readiness program in South African organisations calls for the consideration of factors influencing digital forensic readiness in organisations. An understanding of the factors that influence digital forensic readiness enables organisations to be able to develop and implement success digital forensic readiness program.

References

Andrade, A.D. (2009). Interpretive Research Aiming at Theory Building: Adopting and Adapting the Case Study Design. The Qualitative Report, 14(1), 42-60.

ACFE Report to the Nation on Occupational fraud & Abuse, 2006. Available on: www.acfe.com : Accessed on 16/08/2012

Blaikie, N. (1993). Approaches to Social Enquiry, 1st Ed, Polity Press, Cambridge.

Barske, D., Stander, A., & Jordaan, J. (2010). A Digital Forensic Readiness Framework for South African SME's": ACCSSED ON 05/06/2012 FROM icsa.cs.up.ac.za/issa/2010/Proceedings/Full/30

Burrell, G. & Morgan, G. (1979). Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life. Heinemann, London.

Chatz, B. (1995) Digital Evidence: Representation and Assurance: Available on: www.iaac.org.uk/ media/Digital investigation 2012pdf: Access on 08/06/2012

Collis, J. & Hussey, R. (2009). *Business Research*:A practical guide for undergraduate and Postgradute students. 3rd ed. Palgrave Macmillan Division of St. Martin's Press LLC,175 fifth Avenue, New York ,NY 10010.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (3rd Ed.). Thousand Oaks: Sage Publications Inc.

Creswell, J. W., & Clark, P. (2007). Designing and Conducting Mixed Methods Research. Thousand Oaks, CA: Sage Publication.

Creswell, J. W. (2005). Educational Research: *Planning,Conducting,and Evaluating Quantitative and Qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson Education.

Creswell, J. W. (2006). *Qualitative Inquiry Research Design* 2nd ed: Choosing among five approaches. Upper Saddle River, NJ: Pearson Education.

Denzin, N. K. (2005). Emancipatory discourses and the ethics and politics of interpretation, in: Denzin, N.K. & Lincoln, Y.S. (Eds) *Handbook of qualitative research* (3rd ed) (Thousand Oaks, CA, Sage Publications).

Denzin, N. & Lincoln, Y. (2003). The discipline and practice of Qualitative Research ,in Denzin, N. & Lincoln, Y. (eds) Collecting and Interpreting Qualitative Research Materials,2nd ed, SAGE Publications,Inc., Califonia,pp.1-45

Danielsson, J. & Tjostheim, I. (2004). The Need for a Structured Approach to Digital Forensic Readiness. IADIS International Conference e-commerce (pp.417-421), Lisbon: International Association for Development of the Information society

Easterby-Smith, M., Thorpe, R., & Lowe, A. (1991). Management Research: An Introduction. Sage Publication, London, pp: 23-25.

Easterby-Smith, M., Thorpe, R., & Jackson, P. (2008) *Management Research*, 3rd ed, SAGE Publications, Ltd., London.

Flowers, P. (2009). Research Philosophies-Importance and Relevance. MSc By Research, Leading Learning and Change, Cranfield School of Management.

Glaser, B. (1992). Emergence v Forcing Basics of Grounded Theory Analysis. Sociology Press, Mill Valley, CA

Ghauri, P. & Grønhaug, K. (2005). *Research Methods in Business Studies, A Practical Guide,* 3rd Edition. Pearson Education limited.

Guba, E. G., & Lincoln, Y. S. (1989). Fourth Generation Evaluation. Newbury Park, CA: Sage Global Economic Crime Survey PWC, 2009. Available on: www.pwc.com/en_GX/gx/economic-crimes : Accessed 15/09/2013

Growler, C. P., Louwrens B., & Von Solms, S. H. (2010). A framework to guide the implementation of Proactive Digital Forensics in organisations: ACCESSED ON 15/06/2012 FROM ieeexplore.ieee.org/iel5/5437532/5437988/05438018.pdf?

Grobler, C. P., & Louwrens, B. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice: In Venter, H., Ellof, M., Labuschagne, I., Eloff, J. & Von

Solms R. (Ed.), New Approaches for Security, Privacy and Trust in Complex Environments (pp,13- 24). New York: Springer

Grobler, C. P., & Louwrens, B. Digital Forensics (2006). A Multi-Dimensional Discipline. In Ellof, J., Labuschagne, L., Elloff, M., & Venter, H. (Ed.), proceedings of the ISSA 2006 from Insight to Foresight Conference. Pretoria: University of Pretoria 2006.

Grobler, C. P., & Louwrens, B. (2009). High level integrated view of digital forensic, proceedings of the ISSA 2009. Available on: www.icsa.cs.up.ac.za : Accessed on 12/10/2012.

Hatch, M. J., & Cunliffe, A. L. (2006). *Organization Theory*, 2nd Ed, Oxford University Press, Oxford.

Hendricks, D. (2005). An Investigation into the Consensus Surrounding Information Systems Project Success. Department of Information Systems, University of Cape Town, South Africa.

Hudson, L. A., & Julie, L. O. (1988). Alternative Ways of Seeking Knowledge in Consumer Research: *Journal of Consumer Research,* 14 (March), 508–21

Fidentia Scandal, IOL news, 2007. Available on: www.iol.fidentia-scanda-iol-news-2007: Accessed 12/10/2012

Key sectors, 2008. *South Africa info Available on:* southafrica.info/business/ economy/sectors/financial.htm: Accessed 21/11/2012

King II Report on Corporate Governance, (2002). Available www.iodsa.co.za : Accessed on 08/11/2012

King III Report on Corporate Governance, (2009). Available www.iodsa.co.za : Accessed on 08/11/2012

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Quarterly, 23 (1), 67-94.

Kroeze, J. H. (2011). Interpretivism in Information Systems: A Postmodern Epistemology? Sprouts: Working Papers on Information Systems, 11(171). ISSN1535-6078.

Kyobe, M. (2012). A multi-theoretical approach to measuring student awareness of electronic abuse in online social networks. (Work in Progress). Department of information Systems, University of Cape Town.

Lee, N., & Lings, I. (2008). *Doing Business Research* : A guide to theory and practice 1st Ed. Sage Publications Ltd, 1Oliver's Yard, 55 City Road. London, ECIY ISP.

Leech, N. L. and Onwuegbzuie, A. J. (2009). A typology of mixed method research designs. School of Education, University of Colorado at Denver and Health Science Centre. Qual Quant (200) 43:265-275 DOI 10.1007/s11135-79105-3

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. Beverly Hills,CA: Sage.

Maree, K. (2010). First steps in Research. 5th Edition: Van Schaik Publishers.1064, Arcadia Street. Hatfield Pretoria.

McKemmish, R. (1999). What is forensic computing: Trends and issues in crimes and criminal justice (118).

Meyers, M. D. (2009). Qualitative Research in Busisness and Management. Los angeles,CA: Sage.

(Mpazanje, F. (2008). Towards understanding as-lived experiences in

Information Systems projects: An Actor-network Theory perspective. University of Cape Town, Department of Information Systems, South Africa.

Neil. J. (2007). *Qualitative versus quantitative research: Key points in a classic debate*. [Online].Available: http://wilderdom.com/research/QualitativeVersusQuantitativeResearch.html : Accessed on 15/11/2012

Onwuegbzuie, A. J. & Johnson, R. B. (2006). The Validity Issue in Mixed Research Mid-south Educational Research Association. Research in the schools, 2006 Vol.13,No.1, 48-63.

Orlikowski, W. J. & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. Information Systems Research, 2 (1), 1-28.

Palmer, G. (ed.) (2001). A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 6 November 2001. Available on : http://www.dfrws.org/dfrws-rm-final.pdf:Accessed 06/05/2012.

Poope, A. & Labushcagne, L. (2012). A conceptual model for digital forensic readiness University of South Africa.1 Preller Street, Muckleneuck Ridge, Pretoria, South Africa

Protection of Personal Information Act, 2013. Available on www.saica.co.za : Accessed 10/12/2013

RICCA Act, (22 January 2002). Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. Order No. 24286. Available from: http://www.info.gov.za/acts/2002/a70-02/ :Accessed 15/08/2012).

Roberts, P. et al (2006). Reliability and Validity in Research. Arts & Science Clinical Research,Education. 2006 Vol. 20, No.44, 41-45.

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence, pp1-28 2004

SABS ISO/IEC1779, (2001). SABS edition ,South African Standard, Code of practice for Information Security Management ,South African Bureau of Standards.

Sarbanes-Oxley Act in 2002. USA: Available on: www.frwebgate.acess.gpo.gov.: Access on 15/10/2013.

Sarantakos, S. (2005). *Social Research*, 2nd edition, Palgrave Macmillan.

Saunders, M., Lewis, P. & Thornhill, A. (2003). *Research Methods for Business Students,* Harlow, London: Pearson Education Limited (3rd Ed.).

Scientific Evidence& Forensics Science, (1993). Scientific Evidence& Forensics Science since Daubert: Maine Decides to sit out the dance: Available on: http://www.mainlaw.edu/academics/law: Accessed on 15/05/12

Sekaran, U. (2003). *Research Methods for Business, A Skill Building Approach*, 2nded, John Wiley & Sons, New York, NY.

Smith, L. T. (2006). Choosing the margins: The role of research in indigenous struggles for social justice, in: N. K. Denzin & M. D. Giardina (Eds) *Qualitative inquiry and the conservative challenge: confronting methodological fundamentalism* (Walnut Creek, CA, Left Coast Press).

Struwig, F. W. & Stead, G. B. (2009). *Planning ,Designing ,and Reporting Research*. 5th Ed. Pearson Education,Forest Drive Pinelands ,Cape Town.

Tan. J. (2001). Forensic Readiness, Stake Inc., 2011, Available at http://www.atstake.com/research/reports/acrobat/stake_forensic_readiness.pdf. Accessed on: 15/06/2012

Trevino, L. K. (1986). Ethical decision making in organisations: A person-situation interactionist model. *Academy of Management Review*, 11(3):601-617.

Van Geunen, C. (2010). Unethical Decision Making and Behaviour in the life Insurance of South Africa. Nelson Mandela University, Port Elizabeth, South Africa

Volonino, L. & Anzalldual, R. (2008). Computer forensic Act: Available: www.dfrws.org/2011/proceedings : Accessed on 19/09/2012.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. European Journal of Information Systems, 4, 74 – 81.

Walsham, G. (2002). Interpretive Case Studies in IS Research: Nature and Method in: *Qualitative Research in Information Systems,* M.D. Myers and D. Avison (eds.). London: Sage Publications

Walsham, G. (2006). Doing interpretive research, European Journal of Information Systems, 15, 320–330.

Wilson, J. (2010). *Essentials of Business Research* : A Guide to doing your research project.1st ed. Sage Publications Ltd, 1Oliver's Yard, 55 City Road. London, ECIY ISP.

Yin, J. (2006). China's Second Long March: A Review of Chinese Media Discourse on Globalization. *Review of Communication*, *6*(1/2), 32-51.

Yin, R. K. (1984). Case Study Research: Design and Methods. Beverly Hill, Calif : Sage Publications.

Yin, R. K. (1989). Case Study Research: Design and Methods, Newbury Park, Canada: Sage Publications.

Yin, R. K. (1994). Newbury Park, Canada: Sage Publications, Yin, R. K. (2006), “Case Study Research: Design and Methods”, Newbury Park, Canada: Sage Publications.

Yin, R. K. (2009). Case Study Research: Design and Methods*. 4rd ed. Thousand Oaks*: Sage Publications.

Zatyko, K. (2007). Defining Digital Forensics. Forensic Magazine, 4 (1), pp. 18-22, 2007, 978-1