A conceptual model for digital forensic readiness

Antonio Pooe: Student
University of South Africa
1 Preller Street, Muckleneuck Ridge, Pretoria, South Africa
antonio.pooe@gmail.com

Professor L Labuschagne: Executive Director of Research
University of South Africa
1 Preller Street, Muckleneuck Ridge, Pretoria, South Africa
llabus@unisa.ac.za

Abstract—**The ever-growing threats of fraud and security incidents present many challenges to law enforcement and organisations across the globe. This has given rise to the need for organisations to build effective incident management strategies, which will enhance the company's reactive capability to security incidents.**

The aim of this paper is to propose proactive activities an organisation can undertake in order to increase its ability to respond to security incidents and create a digitally forensic ready workplace environment.

The study constitutes exploratory research, with the use of a systematic literature review as a basis to identify activities relating to a digitally forensic ready environment.

While much has been written about how organisations can prepare to respond to security incidents, findings show an absence of a digital forensic readiness model. This paper concludes by presenting such a conceptual model.

This study contributes to the greater body of knowledge on the design and implementation of a digital forensic readiness programme, aimed at maximising the use of digital evidence in an organisation.

Keywords - digital forensic readiness; computer forensics; data integrity; digital evidence; incident handling; empirical research

I. INTRODUCTION

White-collar crime is a term that has had common occurrence in the news. To explain it, consider the following cases. Towards the end of 1999, the South African government signed contracts totalling R30 billion to modernise its defence equipment. The project, "which promised billions of Rands in export and local sales, has not happened" [1]. On another matter, it was reported that Randgold & Exploration was subject to "massive fraud" equal to R1.5bn by its former CEO Brett Kebble, who misappropriated funds, forged documents and was involved in imprudent deal making, according to a forensic investigation [2]. While these types of cases do not form part of a typical law enforcement agent's daily work, they do depict the gradually decaying ethical fibre of modern-day society. Speculations were that these elaborate crimes would end with Enron, and that the business community would use the lessons learned and better manage this great risk [3]. However, this has not been the case. Many other organisations such as WorldCom, Health South, Adelphia and Tyco suffered the same tragedy [4]. In trying to understand and measure the impact of fraud on organisations, the Association of Certified Fraud Examiners released findings of a study that a typical organisation loses 5% of its annual revenue to fraud [5]. In other studies, South Africa was found to have the second-worst white-collar crime rate in the world [6].

The inherent risk of increased technical sophistication in modern crimes makes these security incidents harder to detect, thereby potentially creating more damage [7]. Additionally, technology now plays a central role in facilitating and enhancing the sophistication of modern security incidents [8]-[9]. Over the past decade, well-understood procedures and methodologies have evolved within computer forensics digital evidence collection [10]-[11]. Kenneally and Brown [10] further note: "Computer forensic autopsies are no longer performed on single machines with small data storage capacities. Rather, the scope for potential evidence has expanded to networks of interconnected computers, each with vast storage capacities containing potential artefacts of legal relevance". Available literature relating to digital forensic readiness (DFR) addresses various technical components of this concept, but none brings all the components into one framework [12]-[15]. The need for a consolidation of research efforts in creating frameworks and models that help to address recent threats was recently identified by Garfinkel [9], who states that "without a clear strategy for enabling research efforts that build upon one another, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of computer forensics products will be unable to rely on the results of forensic analysis".

This paper investigates recent challenges that technology presents with regard to the reliance and admissibility of electronic evidence in a court of law. A systematic literature review was used to gather relevant information and this data is critically analysed in order to identify gaps and to improve upon them.

A section dedicated to explaining the scientific research method adopted in this paper is presented next. This is followed by a section on the application of the said research method, in reviewing existing literature relating to digital forensics. Preceding the conclusion is a section that presents the conceptual model for DFR.

II. RESEARCH METHOD

A systematic literature review was used. Unlike conventional literature review, a systematic review follows a predefined protocol. It is defined as a way to "identify, evaluate and interpret the available research that is relevant to an issue or discipline, or phenomenon of interest of a specific research domain" [16]. Systematic reviews require the researcher to systematically collect all the search on a given

topic, select studies according to pre-determined quality criteria, abstract the same information from each included study, display the results in evidence tables and interpret the results in view of the totality of the evidence [17].

A. Scoping

The scope of our research was limited to material available on the University of South Africa Online Library [18]. This library is said to be one of the largest libraries in Africa, best endowed with information sources in access of 1,5 million. The library also subscribes to an increasing number of electronic journals, which are available at all times to Unisa students [18]-[19].

A detailed search of relevant databases was conducted. The relevance was determined by using the library's A-Z list of electronic resources [18]. From this, only seven databases containing the most relevant material were selected and analysed further for articles and other publications. The databases were selected on the basis of being classified under the following categories:

i. Multidisciplinary;

ii. Computing;

iii. Law;

iv. Information Science; and

v. Engineering.

Furthermore, the databases that were used were the ones containing the majority of the search hit results. The search term used was "digital forensic". This keyword was used as the basis of the search as it relates directly to the topic under investigation.

Only English written material published in the last nine years (2002-2011) was considered. The reasons for this were that, firstly, Unisa's online library is available in English and secondly, English is one of South Africa's most commonly spoken language in business, politics and the media [20]-[21].

As there was no law on digital crimes in South Africa prior to the Electronic Communications and Transactions Act in 2002 [22], only articles written after promulgation of this law were taken into consideration.

The decision for reviewing only articles was based on the logic that articles usually precede books, dissertations and theses. Therefore, by looking at articles, content from the latter is also covered. The next section deals with the methodology for screening articles for inclusion.

B. Screening of articles for inclusion

Since the application of a systematic literature review was intended not only for publication purposes but also for instrumental utilisation, an additional task to increase the reliability of the screening process was undertaken. Both the authors conducted the screening process on a subset of articles independently of each other and then met together to compare results.

In order to ensure that this process was scientific, the Cohen's Kappa (K) interrater was used in measuring reliability of this process. Interrater reliability is the degree of agreement between two observers who have independently observed and recorded behaviours at the same time [23]-[24]. The basic formula for Cohen's Kappa (K) used is as computed below:

$$\text{Cohen's Kappa} = \frac{PA\ (0.77) - PC\ (0.50)}{1 - PC\ (0.50)} = 0.54$$

Where PA is the observed percentage agreement and PC is the percentage agreement expected [24].

The goal in this study was to produce a *PA* value above 75% from the total reviewed articles. This was done to ensure that all relevant articles were included for detailed review and to archive a kappa value above 0.50. The said kappa goal is generally considered to be satisfactory [23]-[24].

Both authors met to calculate the interrater reliability by calculating a percentage agreement. This process was repeated until the percentage agreement exceeded 75%. Abstracts of 459 articles were reviewed, resulting in the identification of 130 relevant articles for possible inclusion. The review process was refined further and the result was an agreement on the final 100 articles for inclusion.

The next section provides a literature overview of DFR.

III. DIGITAL FORENSIC READINESS OVERVIEW

Rapid changes and advances in technology and related crimes have given rise to the need to review and improve on digital forensic models and processes. Gravetter and Forzano [25] also make the observation that "unlike other forensic sciences, digital forensics subject matter continues to evolve, as do the techniques".

Given recent advances in technology, Bell and Boddington [26] argue that it would be imprudent and potentially reckless to rely on existing evidence collection processes and procedures. They add "conventional assumptions about the behaviour of storage media are no longer valid". Unlike traditional storage media, modern storage devices can operate under their own volition in the absence of computer instructions [10], [27]. Such operations can be highly destructive of traditionally recoverable data. This process has the potential to contaminate evidence and can obfuscate and make validation of digital evidence difficult [10].

For purposes of this study, the use of the term "traditional approaches" denotes forensic procedures undertaken from the dawn of the computer forensic practice to 2005 [10]. First, the basic concept of a traditional approach called dead forensics is explained.

A. Dead Forensics

To meet the desired goal of preserving original evidence, one of the first steps in traditional evidence collection procedures includes taking the evidence-containing computer system offline and creating a bit-stream image of the entire original evidence disk [10].

The process begins with the preservation of digital evidence by pulling the power cord, in preparation for the physical

removal of the storage device for imaging purposes. Security becomes an important consideration to ensure the logical and physical safety of the evidence. At the conclusion of the imaging process, a hashing tool is used to authenticate the forensic image. This is then followed by the analysis and reporting phases.

Recent studies show that the well-understood digital forensic procedures and methodologies are evolving [9], [11]. The scope for potential evidence has expanded from standalone computers to networks of interconnected computers, each with vast storage capacities containing potential artefacts of legal relevance, making the dead forensic process increasingly obsolete.

B. Live Forensics

Also known as fast forensics, this concept is defined by Reyes and Brittson [25] as "those investigative processes that are conducted within the first few hours of an investigation, that provide information used during the suspect interview phase". Due to the need for information to be obtained in a relatively short time frame, fast forensics usually involves an on-site/field analysis of the computer system in question.

Live analysis techniques use software that existed on the system during the time frame being investigated. On the other hand, dead analysis techniques don not use software that existed on the system during that time frame [28].

Avoiding contamination during the recovery process is paramount and depends on effective, error-free data recovery from digital devices. Traditionally, write-blocking hardware combined with bit-stream image copying processes served this purpose.

Some fast forensics techniques utilise Linux or other forensic boot disks to perform on-scene/site searches and data extraction. The boot disks run in memory only and mount the hard drives as read only so as not to corrupt the evidence [25].

Sutherland et al. [29] ague that "there is no way to avoid making changes, since in order to conduct a live examination it is necessary to deploy tools on the live system to capture data, and such tools will make changes to the running system".

This argument was later supported by Chan et al. [30], who found that current forensic tools are limited by their inability to preserve the hardware and software state of a system during investigation. Existing tools can overwrite evidence present in memory or alter the contents of the disk causing forensic taint, which lowers the integrity of the evidence.

On the other hand, taking a snapshot of the system can result in a phenomenon known as forensic blurriness, where an inconsistent snapshot is captured because the system is running while it is being observed. Forensic blurriness affects the fidelity and quantity of evidence acquired and can cast doubt on the validity of the analysis, making the courts more reluctant to accept such evidence [30].

From the above, the conclusion is made that neither dead nor live forensics provide sufficient assurance of non-manipulation. Therefore, if existing computer forensic procedures ultimately render evidence inadmissible, then the need for a redefinition of the methodology is paramount.

C. Digital Forensic Technical Challenges

According to Bell and Boddington [26], "these long-established, internationally accepted procedures even cover situations such as the automated recovery of court-submissible evidence which a defendant has previously attempted to delete. Indeed, the peculiarity of 'deleted, but not forgotten' data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology".

This comes from the reality that traditional hard disks have slow access speeds relative to their capacity for storage (the latter makes complete erasure very inconvenient), and from the fact that there is no performance penalty is incurred for writing over existing data (which makes complete erasure unnecessary).

This situation is in the process of changing [9]. Newer technologies such as solid-state drives (SSDs) are much faster and more complex. However, these complexities are not limited only to SSDs, but extend to other storage forms, such as raid arrays, storage area network (SAN) and network attached storage (NAS) devices.

Commensurate changes that need to be made by the digital forensic tool manufacturers to accommodate/address the new file systems, operating systems and connectivity demands also contribute to shorter lifespan of forensic tools [31]. The issue of tools and other technical resources becomes even more pertinent as anti-forensic efforts continue to increase. Anti-forensics can be defined as "the movement to exploit weaknesses in the forensic process or tools" [25].

This rising surge of anti-forensic tools and their ease of access on the internet directly impacts on any organisation's ability, or lack thereof, to respond effectively to digital crimes [32].

There is a need to find a balance between the functionality that security applications provide (eg. secure deletion) and the reverse engineering capability required from digital forensic tools. Findings show that security applications have advanced far beyond digital forensic tools, rendering some forensic tools obsolete against (anti-forensic) actions undertaken using security tools.

D. Digital Forensic Readiness

The previous section provides evidence suggesting that a mature technical environment alone is not the only factor impacting on the organisation's DFR. In this section, we explore the concept of DFR and other factors that have an impact on it.

Rowlingson [13] defined forensic readiness "as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation". Garcia [33] later modified this definition to describe forensic readiness as the "art of maximizing the environment's ability to collect credible evidence".

From the perspective of law enforcement agencies, the forensic process begins when the crime has been committed or when a crime has been discovered and reported. The concept of

forensic readiness, according to Hoolachan and Glisson [34], is that an organisation can pre-empt the occurrence of a crime by preparing the environment in advance and in doing this, organisations will benefit not only in instances where prosecution becomes an issue, but also in limiting their own business risks.

a) Policies & Procedures

The business requirement to gather and use digital evidence has been recognised in a number of studies. Rowlingson [13] notes that enterprise policies can enhance computer and network forensics. While policies are important, they alone will not guarantee an organisation's overall forensic readiness. An implementation plan (incident response) must be developed and tested.

According to Jaatun et al. [35], incident response is the process of responding to and handling security-related incidents involving information and communications technology infrastructure and data. Incident response has traditionally been rather reactive in nature, focusing mainly on technical issues [35]-[36]. An incident can be anything from an attack that crashes all the servers and cuts off all network communications to an intrusion that causes no actual damage but demonstrates the vulnerability of the organisation's systems [36]-[37]. In the introduction of this article, reference to examples of high-profile fraud cases relating to the South African government's arms deal, Brett Kebble's affairs while at Randgold and those of international companies such as Tyco, Adelphia and WorldCom indicate the damage a poorly managed incident can cause.

Taylor et al. [32] add that "although all security incidents should be taken seriously, they may not all have the same severity". An incident response plan should therefore define how incident severities will be determined and what this means in terms of incident handling.

b) Incident Management

David [38] suggests that before dealing with "the incidents that have been deemed worthy of treatment, there are three important steps that should be taken. First, all events should be logged, and the logging should be in as much detail as possible". This makes allowance for things such as later treatment of the non-priority items, detecting patterns leading up to incidents, and a ready source of information regarding events that are action items.

The second important step is that there should be an escalating set of responses when appropriate. The benefits derived from this step are what can be called 'quick and dirty' initial reactions to certain incidents, and provide follow-up actions if the earlier ones fail to accomplish their goals.

David [38] further suggests that "all events, even those not designated as incidents to be treated in the incident response plans, should be treated with reasonable promptness, although certainly not with the urgency associated with the more serious events".

If the above steps are not taken to stop the events of lesser importance, those initiating these events can continue doing them without fear of reprisal, and might even try more severe attacks [37]-[38].

c) Response Team

In an attempt to be proactive, many organisations form incident response teams—called computer incident response teams (CIRTs). These teams are made up of trained individuals whose goal is to be able to react speedily to occurrences of incidents [39].

Each team member covers a pre-assigned area of responsibility, thus decreasing the amount of damage and increasing the likelihood of apprehending the perpetrator of the incident [35]-[36]. An incident response manager, whose responsibility includes coordinating notifications, escalations and ensuring that the incident response team is properly assembled, usually leads this team [32].

Lamis [39] adds that "communication between team members, internal departments, and external networks is critical to creating a resourceful environment to effectively combat and handle incident responses. An organization's incident response team may require outside assistance, which costs crucial time and money to select during the incident".

While no evidence of a forensic readiness model could be found, critical components making up such a model can be extrapolated from the literature reviewed. There is a need for a consolidation of research efforts in creating frameworks and models that help to address recent threats and incidents [9]. The next section covers how reviewed literature on research efforts relating to DFR was consolidated in the development of a conceptual model for digital forensic readiness.

IV. Digital Forensic Readiness Conceptual Model

From the literature analysis, the critical components of a DFR model are summarised in Figure 1. At a macro level, core activities relating to DFR fall under four categories, namely People, Process, Policy and Technology. Within each category are sub-activities which can further be classified into proactive and reactive classes.

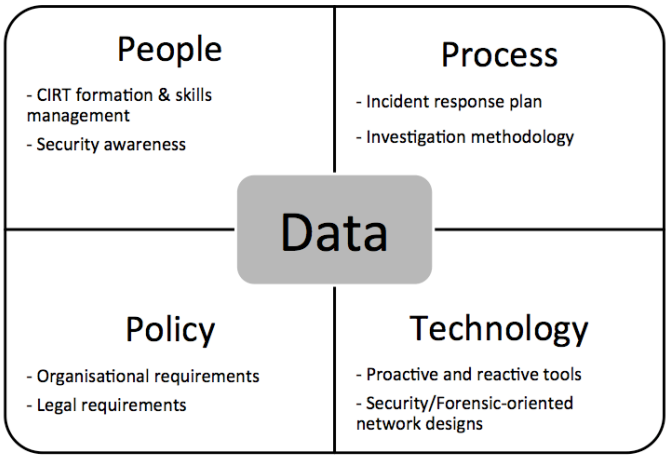

Figure 1. Digital forensic readiness conceptual model

From the above discussion, forensic readiness as explained by Rowlingson [13] was found to have two main objectives:

vi. Maximising an environment's ability to collect credible digital evidence; and

vii. Minimising the cost of forensics during an incident response.

a) People

Under the People category are many sub-activities such as the hiring of experienced CIRT members, segregation of duties and security training and awareness campaigns. Establishing a capability for securely gathering legally admissible evidence is a key component of DFR [13].

The objective is to ensure that the human resources of an organisation all contribute towards the prevention and detection of security incidents [14].

Research suggests that building a response team should involve many different organisational departments such as legal and public relations [32], [39]. These additional parties sometimes include external parties who provide support and have skills that may not be present in the organisation.

External parties should also be readily available to provide assistance to internal teams in the event of an incident [36]-[37].

Although the variety of staff involved generally varies depending on the magnitude of the investigation, Hoolachan and Glisson [34] argue that "there are a multitude of people who need to understand the correct protocol within a digital investigation". Failure to organise and equip human resources with the necessary tools and knowledge can ultimately negatively impact the organisation's forensic readiness.

Developing and documenting processes that affect all parties involved is key in ensuring that the integrity of evidence and the reputation of the organisation remain intact, even after the incident.

b) Process

The Process category is concerned with activities that ensure the integrity of evidence. This includes ensuring that operational documents such as an incident response plan and a forensic methodology are in place [34]. This is critical as it provides the organisation with an implementation guide to meeting the requirements set by regulatory framework and organisational policies.

Von Solms et al. [14] summarise the four key activities of the digital forensic process:

i. Securing the evidence without contaminating it,

ii. Acquiring the evidence without altering or damaging the original,

iii. Authenticating that the recovered evidence is the same as the original seized data, and

iv. Analysing the data without modifying it.

The procedures for evidence acquisition and preservation can be simple, rapid and effective, saving time and money [40]. The complexities of modern network environments, however, demand that organisations define the details well ahead of time. Failing to preserve the integrity of data on a victim or attacking systems in a timely manner will negatively affect the outcome of the investigation.

It is therefore important to have defined processes that guide the organisation in achieving a digitally forensic ready environment. Furthermore, these processes should be governed by certain policies and guiding principles to chart the course of action in the event of an incident.

c) Policy

Rowlingson [13] notes that enterprise policies can enhance computer and network forensics. In addition, he proposes six categories of policies to facilitate digital forensic investigations. These categories are designed to help enterprises deter computer crime and position themselves to respond to successful attacks by improving their ability to conduct investigations. The six categories of policies that facilitate digital forensic investigations are:

viii. Retaining information – Policies that relate to the storage of information by an organisation;

ix. Planning the response – Policies that guide the organisation's plans to respond to various incidents and situations;

x. Training – Policies that address the training of staff members and those affiliated with the organisation;

xi. Accelerating the investigation – Policies that address operational aspects of investigations;

xii. Preventing anonymous activities – Policies that address the organisation's proactive efforts against the risk of fraud; and

xiii. Protecting the evidence – Policies that address the handling and protection of evidence and other vital data.

Grobler and Louwrens [15] argue that digital forensics policies may augment some information security policies, suggesting that interdependencies between policies will exist. As such, these policies must not be developed in silos, but should inform one another.

While policies are important, they alone will not guarantee an organisation's overall forensic readiness. Technology is the ultimate enabler, ensuring that People have proactive and reactive tools to implement as guided by Policy and defined Processes.

d) Technology

An organisation needs to ensure that appropriate technology is used not only to enable business operations, but to also prevent and detect computer incidents.

To provide more clarity on the role of technology or system forensic readiness, Tan et al. [40] present the idea of system forensic readiness as one part of overall enterprise forensic readiness. It is critical for organisations to know their sources

of potential evidence and to determine what currently happens to the potential evidence data [13].

Evidence preservation is not only affected by technical factors. Tan [12] argues that non-technical factors for consideration also include:

xiv. How logging is done;

xv. What is logged;

xvi. Intrusion detection systems (IDSs);

xvii. Forensic acquisition; and

xviii. Evidence handling.

According to Doherty and Liebesfeld [31], more private investigators are declining various digital forensic work because the needed and required tools are very expensive and have a short lifespan, due to the increasing and changing variety of digital devices available on the market each year.

The issue of tools and other technical resources becomes even more pertinent as the anti-forensic efforts continue to increase. Anti-forensics, as explained above, can be defined as "the movement to exploit weaknesses in the forensic process or tools" [25]. It can also involve the various acts of hiding data from the forensic exam. Older techniques were as simple as running a simple script to perform a touch command on every file to alter file attributes (date and time stamps), or deleting log and temporary files [41].

It is therefore important to incorporate digital forensic toolsets into the overall organisational technology infrastructure. By including some aspects of DFR into the information security architecture of the organisation, it will be possible to link the source of the attack to the incident and the perpetrator [15]. This integration of digital forensics in the architecture design will help to bridge the gap between advances in security applications and challenges that digital forensic tools face.

As can be extrapolated from the definition of DFR, efforts to ensure availability and integrity of data are central to maximising the organisation's ability to collect credible evidence to facilitate an investigation [33]-[34]. Studies have also shown that DFR activities relating to data benefit organisations not only in instances where prosecution becomes an issue, but also in limiting an organisation's own business risks [13], [34].

V. Value Proposition

As discussed, the increasing sophistication of incidents can cause great harm to an organisation. While numerous organisations have policies, human resources and technical tools, many of these efforts are modelled in a way that supports business functions and not necessarily DFR.

The proposed conceptual DFR model provides a platform for proactive activities to be consolidated and concentrated to ensure collaboration within the organisation in building capacity to prevent, detect and manage incidents.

Additionally, the model can be used to provide a dashboard of all related organisational activities, classified under each of the four components of People, Process, Policy and Technology. Once complete, this classification can be used to measure the maturity of how ready the organisation is to deal with security incidents. This will further aid in reducing duplication of activities geared towards achieving DFR.

VI. Conclusion

The aim of this paper was to propose proactive activities an organisation can undertake in order to increase its ability to respond to security incidents and create a digitally forensic ready workplace environment. This was done by investigating recent challenges that technology presents with regard to the reliance and admissibility of electronic evidence in a court of law. A systematic literature review was used to gather relevant information and this data was critically analysed in order to identify gaps and to fill them.

Findings show that available literature relating to DFR addresses various technical components of this concept, but none brings all the components into one framework. The need for a consolidation of research efforts in creating frameworks and models that help to address recent threats was also discussed and the outcome is a proposed conceptual DFR model, which can be used as a tool to consolidate and integrate segregated business activities which form part of DFR. The model also identifies four critical components that are necessary to achieve DFR. In the absence of such a model, an organisation will not be able to maximise the environment's ability to collect credible evidence.

Literature reviewed shows that fraud and security incidents affect organisations across the public and private sector. This research adds value by highlighting the impact of technological advances on traditional digital forensic processes. Included is the emphasis on the sophistication of recent security incidents and the importance of a DFR model to aid organisations in aligning efforts that ensure that credible evidence can be retained during normal business operations.

A limitation of this research is that it presents only a conceptual model, which is generic in nature. Further research opportunities are in building on the proposed conceptual model by identifying the different stakeholders in an investigation process, and personalising the model to their varying environments. Additionally, sub-activities within each of the identified components of the model can be investigated in greater detail, to include testing of recent forensic and security tools that can be used to address technological advances discussed earlier in this paper.

Acknowledgment

A special thanks to the library team at the University of South Africa for their diligence in ensuring that all articles required for this study were purchased and made available on the UNISA online study resources.

REFERENCES

[1] Mail & Guardian. (2008, August). *Mbeki 'paid R30m arms-deal bribe.* [Online]. Viewed 2011 October 7. Available: http://www.mg.co.za/article/2008-08-03-mbeki-paid-r30m-armsdeal-bribe

[2] D. McKay. (2006, March). *Kebble fraud unpacked*. [Online]. Viewed 2011 October 7. Available: http://www.miningmx.com/news/archive/150120.htm

[3] T. Brazley, *Investigating While Collar Crime*, New Jersey: Pearson Education, 2008.

[4] T. Dimnik. (2010, May). *The "unified perspective" recipe for a successful compliance program*. Viewed 2011 October 7. Available: http://www.itcba.org/dynamicdata/flash/3-%20May%2020.ppt

[5] ACFE. (2010). *Report to the nation on occupational fraud and abuse*. [Online]. Viewed 2011 October 3. Available: http://www.acfe.com/rttn/rttn-2010.pdf

[6] PWC. (2009). *The 5th Global Economic Crime Survey*. [Online]. Viewed 2011 October 3. Available: http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf

[7] KPMG. (2009). *E-crime survey*. [Online]. Viewed 2011 October 3. Available: http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG(1).pdf

[8] S. Peters. (2009). *14th Annual CSI Computer Crime and Security Survey*. [Online]. Available: http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf

[9] S. L. Garfinkel. (2010, August). Digital forensics research: The next 10 years. *Proceedings of the Tenth Annual DFRWS Conference*. [Online]. 7, pp. S64-S73. Available: http://www.sciencedirect.com/science/article/pii/S1742287610000368

[10] E. E. Kenneally, and C. L. T. Brown. (2005, February). Risk sensitive digital evidence collection. *Digital Investigation*. [Online]. 2, pp. 101-119, Available: http://www.sciencedirect.com/science/article/pii/S1742287605000290

[11] P. Cooper, G. T. Finley and P. Kaskenpalo. (2010, June). Towards standards in digital forensics education. *Proceedings of the 2010 ITiCSE Working Group Reports*. [Online]. 10, pp. 26-30. Available: http://0-delivery.acm.org.oasis.unisa.ac.za/10.1145/1980000/1971688/p87-cooper.pdf?ip=163.200.81.46&acc=ACTIVE%20SERVICE&CFID=80236719&CFTOKEN=73481127&__acm__=1336017593_fdcfb3197899faba4a384fcf3d289e65

[12] J. Tan. (2001, July). *Forensic readiness*. [Online]. Available: http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

[13] R. Rowlingson. (2004). *A ten step process for forensic readiness*. [Online]. Available: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

[14] S. von Solms, C. Louwrens, C. Reekie, and T. Grobler. (2006). A control framework for digital forensics. *IFIP Advances in Information and Communication Technology*. [Online]. 222, pp. 343-355. Available: http://0-www.springerlink.com.oasis.unisa.ac.za/content/978-0-387-36890-0/#section=684286&page=12&locus=45

[15] C. P. Grobler, and C. P. Louwrens. (2007). New approaches for security, privacy and trust in complex. *IFIP International Federation for Information Processing*. [Online]. 232, pp. 13-24. Available: http://0-www.springerlink.com.oasis.unisa.ac.za/content/r82m17v470581t34/?MUD=MP

[16] T. Sobh, and K. Elleithy, *Innovations in Computing Sciences and Software Engineering*, New York: Springer, 2010.

[17] T. A. Lang, *How To Write, Publish, & Present in the Health Sciences: A Guide for Clinicians & Laboratory Researchers*, 2nd ed., Philadelphia: American College of Physicians, 2010.

[18] University of South Africa. (undated). [Online]. Viewed 2011 December 11. Available: http://www.unisa.ac.za

[19] K. M. Ramalibana. (2005, December). *An investigation into the effectiveness of the staff development policies and programmes of the Unisa Library*. [Online]. Available: http://uir.unisa.ac.za/handle/10500/5/browse?order=ASC&rpp=20&sort_by=1&etal=-1&offset=20&type=title

[20] V. Webb, *Language in South Africa: The Role of Language in National Transformation, Reconstruction and Development*, Amsterdam: John Benjamins, 2002.

[21] South Africa. (2012, March). *The languages of South Africa*. [Online]. Viewed 2012 April 12. Available: . http://www.southafrica.info/about/people/language.htm

[22] S. K. Kabanda, I. Brown, V. Nyamakura, and J. Keshav. (2010). South African banks and their online privacy policy statements: A content analysis. *SA Journal of Information Management*. [Online]. 12 (1). Available: http://www.sajim.co.za/index.php/SAJIM/rt/printerFriendly/418/0

[23] P. Mathews. *Sample Size Calculations: Practical Methods for Engineers and Scientists*, Ohio: Mathews Malnar and Bailey Inc, 2010.

[24] J. F. Gravetter, and L. B. Forzano, *Research Methods for the Behavioral Sciences*, 3rd ed., California: Wadsworth, 2009.

[25] A. Reyes, and R. Brittson, *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*, Waltham: Syngress Publishing, 2007.

[26] G. Bell, and R. Boddington. (2010, July). Solid state drives: The beginning of the end for current practice in digital forensic recovery. *The Journal of Digital Forensics, Security and Law.* [Online]. 5 (3), pp. 5-32. Viewed 2011 June 9. Available: http://0-www.proquest.com.oasis.unisa.ac.za/ .

[27] F. Chen, D. A. Koufaty, and X. Zhang. (2009). *Understanding intrinsic characteristics and system implications of flash memory based solid state drives*. [Online]. Available: http://www.cse.ohio-state.edu/hpcs/WWW/HTML/publications/abs09-2.html

[28] B. D. Carrier. (2006, February). Risks of live digital forensic analysis. *Communications of the ACM - Next-generation cyber forensics* [Online]. 49 (2), pp. 1-38. Available: http://0-dl.acm.org.oasis.unisa.ac.za/citation.cfm?id=1113034.1113069&coll=DL&dl=ACM

I. Sutherland, J. Evans, T. Tryfonas, and A. Blyth. (2008, April). Acquiring volatile operating system data tools and techniques. *ACM SIGOPS Operating Systems Review*. [Online]. 42 (3), pp. 65-73. Available: http://0-dl.acm.org.oasis.unisa.ac.za/citation.cfm?id=1368506.1368516&coll=DL&dl=ACM&ticket=ST-263623-X2KUjNq4oUAqGKcSq5E5-cas

[29] E. Chan, S. Venkataraman, F. David, A. Chaugule, and R. Campbell. (2010, December). Forenscope: A framework for live forensics. *Proceedings of the 26th Annual Computer Security Applications Conference.* [Online]. 26, pp. 307-316. Available: http://0-dl.acm.org.oasis.unisa.ac.za/citation.cfm?id=1920261.1920307&coll=DL&dl=ACM&ticket=ST-263647-PHrEuXLsz0pJNKsP4ULH-cas

[30] E. Doherty, and J. Liebesfeld. (2008, May). Proposing a digital forensics grange. *Security*. [Online]. 45 (5), pp. 32-33. Available: http://0--proquest-.umi-.com-.oasis-.unisa-.ac-.za/pqdweb-?did=1480181371-&sid=1-&Fmt=3-&clientId=27625-&RQT=309-&VName=PQD

[31] C. Taylor, B. Endicott-Popovsky, and D. A. Frincke. (2007, September). Specifying digital forensics: A forensics policy approach. *Digital Investigation*. [Online]. 4 (1), pp. 101-104. Available: http://0-www.sciencedirect.com.oasis.unisa.ac.za/science/article/pii/S1742287607000461

[32] J. Garcia. (2005, September). *Proactive and reactive forensics*. [Online]. Available: http://jessland.net./Docs.php

[33] S. A Hoolachan, and W. B. Glisson. (2010, May). Organizational handling of digital evidence. *Proceedings of the Conference on Digital Forensics, Security and Law.* [Online]. pp. 33-44. Available: http://0-proquest.umi.com.oasis.unisa.ac.za/pqdweb?index=0&did=2287434051&SrchMode=1&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1336062547&clientId=27625

[34] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tondel, and O. H. Longva. (2009, March). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*. [Online]. 2 (1-2), pp. 26-37. Available: http://www.sciencedirect.com/science/article/pii/S1874548209000043

[35] L. Shinder, and M. Cross. (2008, June). Chapter 12 – Understanding cybercrime prevention. *Scene of the Cybercrime*, 2nd ed., [Online]. pp. 505-554. Available: http://0-www.sciencedirect.com.oasis.unisa.ac.za/science/article/pii/B9781597492768000121

[36] T. V. Lillard, C. P. Garrison, C. A. Schiller, and J. Steele. (2010, June). Chapter 9 – Incorporating network forensics into incident response plans. *Digital Forensics for Network, Internet, and Cloud Computing — A Forensic Evidence Guide for Moving Targets and Data*. [Online]. pp. 221-274. Available: http://0-www.sciencedirect.com.oasis.unisa.ac.za/science/article/pii/B9781597495370000090

[37] J. David. (2000, February). Incident response. *Network Security*. [Online]. 1999 (11), pp. 15-18. Available: http://www.sciencedirect.com/science/article/pii/S1353485800800057

[38] T. Lamis. (2010, October). A forensic approach to incident response. *Information Security Curriculum Development Conference*. [Online]. pp. 177-185. Available: http://dl.acm.org/citation.cfm?id=1940975&dl=ACM&coll=DL&CFID=80322195&CFTOKEN=98528235

[39] T. Tan, T. Ruighaver, and A. Ahmad. (2003, November). *Incident handling: Where the need for planning is often not recognised*. [Online]. Available: igneous.scis.ecu.edu.au/proceedings/2003/forensics/pdf/08_final.pdf

[40] J. Wiles, T. Alexander, S. Ashlock, S. Ballou, L. Depew, G. Dominguez, A. Ehuan, R. Green, J. Long, K. Reis, A. Schroader, K. Schuler, and E. Thompson. (2007). Chapter 2 - Digital forensics: An overview. *Techno Security's Guide to E-Discovery and Digital Forensics*. [Online]. pp. 33-63. Available: http://www.sciencedirect.com/science/article/pii/B9781597492232500066