A Digital Forensic Readiness Framework for South African SME's

D. Barske
Dept. Information Systems
University of Cape Town
Cape Town, South Africa

A. Stander
Dept. Information Systems
University of Cape Town
Cape Town, South Africa

J. Jordaan
Dept. Information Systems
University of Cape Town
Cape Town, South Africa

Abstract—**In this digital age, most business is conducted electronically. This contemporary paradigm creates openings for potentially harmful unanticipated information security incidents of both a criminal or civil nature, with the potential to cause considerable direct and indirect damage to smaller businesses. Electronic evidence is fundamental to the successful handling of such incidents. If an organisation does not prepare proactively for such incidents it is highly likely that important relevant digital evidence will not be available. Not being able to respond effectively could be extremely damaging to smaller companies, as they are unable to absorb losses as easily as larger organisations.**

In order to prepare smaller businesses for incidents of this nature, the implementation of Digital Forensic Readiness policies and procedures is necessitated. Numerous varying factors such as the perceived high cost, as well as the current lack of forensic skills, make the implementation of Digital Forensic Readiness appear difficult if not infeasible for smaller organisations. In order to solve this problem it is necessary to develop a scalable and flexible framework for the implementation of Digital Forensic Readiness based on the individual risk profile of a small to medium enterprise (SME).

This paper aims to determine, from literature, the concepts of Digital Forensic Readiness and how they apply to SMEs. Based on the findings, the aspects of Digital Forensics and organisational characteristics that should be included in such a framework is highlighted..

Keywords: Forensic Readiness,Computer Crime, Computer Security, Information Security, Cyber Crime, Security Policies and Procedures

I. INTRODUCTION

According to Sommer[9] organisations often underestimate how often they will be called upon to give account of activities surrounding their ICT systems.

Examples of possible triggers are:

- Reducing the impact of computer-related crime.
- Dealing effectively with court orders to release data.
- Demonstrating compliance with regulatory and legal requirements.
- Producing evidence to support company disciplinary issues.
- Supporting contractual and commercial agreements.
- Proving the impact of a crime or dispute.

An organisation that is not properly prepared for such an event could find itself unable to defend its position. This situation can be the result because of the following reasons:

- The required evidence does not exist.
- The evidence has been contaminated by the way it was handled.
- The evidence was collected in an unacceptable manner.

It is therefore important that management take the requisite steps to avoid finding itself faced with these potentially devastating scenarios. The key to avoiding these situations is to have plans in place that will produce reliable digital evidence before it is required.

II. DIGITAL FORENSICS

Digital forensics is 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" [13].

When considering this definition of digital forensics, the scientific process that constitutes digital forensics can be separated into distinct steps. These are:

- Ensuring that there is proper legal authority to conduct the search and examination

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

- Ensuring that the correct chain of custody is kept for the evidence
- Only using forensic tools that have been validated
- The use of imaging and hashing functions to acquire evidence
- The examination and analysis of the evidence
- Quality assurance to ensure that the examination and analysis, and the results thereof, are repeatable by another examiner
- Reporting of the findings
- Possible testifying as an expert witness in legal proceedings. [5]

Digital forensics is not concerned mainly about computers and computer networks, but is rather mainly concerned with forensic procedures, rule of evidence, and other legal processes as they pertain to computers and computer networks [12].

III. DIGITAL FORENSICS READINESS

Tan [10] was the first to suggest the concept of forensic readiness to meet the objectives for systems used in digital investigations in order to maximize an environment's ability to collect credible digital evidence and to minimize the cost of forensics during an incident response.

Rowlingson[8] describes the organizational forensic readiness goals as follows:

- To enable an organisation to gather evidence legally without interfering with business processes.
- To gather evidence targeting potential crimes and disputes.
- To allow computer forensic investigations to continue in proportion to the incident.
- To minimize interruption to the business from any investigation.
- To ensure that evidence has a positive impact on the outcome of any legal action.

The goals can be achieved by the following:

- Configure ICT systems to proactively collect credible digital evidence for potential use. In more practical terms this objective addresses issues like logging identified activity, log file retention, time synchronization across all components, preventing unauthorized changes to systems etc.
- Adapt the organisation (policy, people and process) where required. This objective addresses such issues as creation of new policies, making changes to existing ones, training staff, reviewing employment contracts, reviewing standard procedures and defining outsourcing requirements etc.
- Minimize cost of investigations (incident response and others).
- The efficiency of an organisation's ability to deal in a forensically sound manner with an event of interest can be expressed in terms of cost. The more prepared you are the lower the cost and vice versa [11].

Although the need for digital forensics and digital evidence in organisations has been explored, as has the need for digital forensic readiness within organisations, decision makers within organisations still need to understand what is needed within those organisations to ensure digital forensic readiness.

There will be costs associated with ensuring digital forensic readiness within an organisation, and this can be significant. Some of the typical costs in implementing a digital forensic readiness program include [8]:

- Updating the organisation's policies and procedures
- Improvements in training of employees
- The systematic gathering of potential digital evidence
- The secure storage of potential digital evidence
- Preparation for events requiring digital forensic intervention
- Enhanced capability for evidence retrieval
- Legal advice
- Developing of an in-house digital forensics examination and analysis capacity

Rowlingson [8] identified ten steps needed to implement a digital forensic readiness program within an organisation :

1) Define the organisational scenarios that could potentially require digital evidence
2) Identify the available sources and different types of potential digital evidence within the organisation
3) Determine the digital evidence collection requirements
4) Establish a capacity within the organisation to securely gather legally admissible digital evidence to meet the organisation's requirements
5) Establish a policy for the secure storage and handling of potential digital evidence
6) Ensure that any monitoring of information systems resources is targeted to detect and deter major incidents
7) Identify the circumstances when a full formal investigation should be instituted of an event
8) Train members of the organisation in incident awareness so that all members involved

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

understand their role in the digital evidence process and the legal issues surrounding digital evidence

9) Document and evidence-based case which describes the incident event and its impact on the organisation

10) Ensure that there is an appropriate legal review to facilitate any actions in response to an incident

Research has provided number of models for ensuring digital forensic readiness, and although there are some slight differences, it is possible to group essential digital forensic readiness into certain thematic categories as summarized by Figure 1.

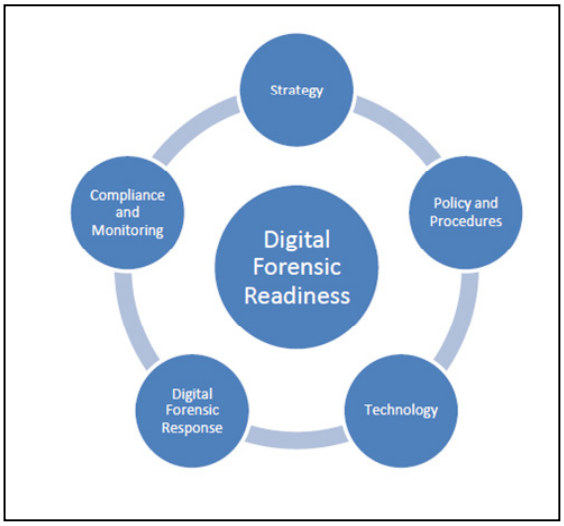

Figure 1. Components of Digital Forensic Readiness[5]

A. Strategy

The decision to implement a digital forensic readiness program must be a strategic decision for the organisation concerned, and to ensure digital forensic readiness it is crucial to maintain digital forensic readiness form a dedicated strategic objective for the organisation. If it forms part of an organisation's strategy, it will be adequately resourced and supported to ensure its success. Key components of a strategy to ensure digital forensic readiness include determining:

- Identifying and understanding what legislation and regulations impose and obligation on the organisation to retain records
- Determining which scenarios could potentially require digital evidence
- Identifying the available sources and different types of digital evidence within the organisation
- Identifying the policies needed to ensure digital forensic readiness, and the legality of evidence preservation practices
- Identify the technological and human resources required to ensure digital forensic readiness
- Ensure sufficient funding the set up and maintain the digital forensic readiness program [5]

B. Policies and Procedures

Every organisation need some form of policies and procedures in place to guide members of the organisation with regards their actions and activities. To ensure digital forensic readiness within an organisation, policies will need to be designed and put in place to enable and ensure this.

An area of concern is that in some organisations, top management simply ignores policies when it is convenient to do so, however in the area of digital forensics, failure to comply with policies can have negative consequences for the organisation, from case which cannot be pursued, to actual legal liability on the part of the organisation [4].

Well-defined policies, especially as they relate to digital forensic readiness, can provide the organisation with the authority to conduct investigations and collect and examine digital evidence within the organisation, and can demonstrate that the organisation is fair-minded and objective in its actions, and follows due process in all forensic matters [3].

At a minimum, to ensure digital forensic readiness within an organisation, the following policies will need to be put in place:

- A policy regarding the acceptable use of information systems resources by members of the organisation
- A policy which clarifies that all information systems resources and data contained thereon in an organisation is the property of the organisation and that no member of the organisation can claim an expectation of privacy, or claim ownership of any data thereon, and that they also consent to the monitoring of any data transmitted via those systems
- A policy which states how information systems within the organisation will be monitored
- A policy which states under what circumstances digital evidence will be preserved, and what data will be preserved
- A policy which states the periods of time that various types and categories of digital evidence will be retained, as well as the storage and secure handling thereof
- A policy which states the circumstance when internal investigations can be initiated and the actions that may be taken as part of the

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

investigation (especially as it relates to the procedures taken in conducting a digital forensic examination in response to an event, whether it is dealt with in-house, or outsourced)

- A policy which states 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 law enforcement
- A policy which sets out clearly the various roles and responsibilities with regards parties involved in preserving and maintaining evidence proactively, as well conducting an actual digital forensic examination in response to an incident
- A policy which stipulate a legal review process for any digital forensic investigation or incident

In drafting policies necessary to ensure digital forensic readiness, it is crucial that the advice of legal counsel be obtain to ensure the legality of any policies.

C. Technology

It is crucial that an organisation that implements a digital forensic readiness program acquire the necessary software and hardware to acquire and preserve digital evidence, and if needed, conduct a completed digital forensic examination.

Digital evidence will either come from logs on computer devices on an organisations information systems network, servers, or from user computers. An organisation must ensure that they have the resources to acquire this evidence in a forensically sound manner, and to store this evidence in a manner in which it is secure and its integrity is preserved. If an organisation does not make use of the correct tools to collect digital evidence in a manner that preserves its admissibility, it risks compromising its legal position [7].

1) Logs

It is important that to maximise the value of logs as potential digital evidence, that an organisation ensure an effective logging mechanism across their information systems that creates an accurate and uniform time picture, and ensures correct retention. The importance of logs as digital evidence cannot be underestimated.

2) Computers and Servers

A significant amount of digital evidence will be found on individual hard drives, and other magnetic, optical, and flash media of computers and servers within an organisation. Potential digital evidence should be identified that will be of importance to the organisation and preserved in a forensically sound manner.

3) Acquisition and Analysis

All digital evidence that is preserved as part of the digital forensic readiness program, or as a result of an incident which requires a detailed digital forensic examination and analysis, has to be acquired in a forensically sound manner which does not alter the data in any way. Traditionally digital forensic images have been made using hardware write blocker devices, which allow the evidence to be preserved without the potential of altering the evidence on the source device.

In a networked environment, there are tools available that can allow forensic images to be made in a forensically sound manner over the network, without taking the computers off the network, and they can even make forensic images of the RAM of a computer. These tools can minimise the disruptions to a network in the forensic imaging process, but are expensive, and organisations will need to weigh up the costs versus the benefits.

In addition to having an ability to acquire the digital evidence using write blocking hardware or software, it is also critical to have software that can create forensic images in a format that can be used by the major digital forensic software suites, while hashing and validating the images. If the organisation is going to conduct its own digital forensic examination and analysis in-house, it is crucial that the organisation have digital forensic software capable of performing the analysis required.

Any organisation that wants to ensure digital forensic readiness will at the very minimum need a capacity to acquire digital forensic images to use as evidence, and ensure that the persons performing this function be trained in the methodologies used, as well as the tools.

4) Evidence Storage

To ensure digital forensic readiness, an organisation will need to maintain a secure digital evidence storage capacity, either on their network, or off-line. This will have to have sufficient storage space to store the volume of evidence anticipated. Ideally, this digital evidence storage should be replicated off-site to mitigate against the risks of losing the primary digital evidence storage.

D. Digital Forensic Response

There is no doubt that digital forensics is needed for various tasks within an organisation, and all organisations should maintain some form of digital forensics capacity to deal with issues as diverse as investigating crimes and inappropriate behaviours of staff, reconstructing computer security incidents, and supporting due diligence with regards internal and external audits [6]. If an organisation does not have a capacity such as this it places the organisation at risk.

Digital forensic readiness should address the response by the organisation to an event that actually requires digital forensic investigation, which is a purely reactive process, in a proactive manner. This is done by identifying the people and processes that will have to be followed in responding to an incident. What is significant with regards the response to an incident from a digital forensic readiness point of view is whether or not the response will be dealt with in-house, or outsourced. While resources within the organisation with a responsibility to respond to incidents of this nature can react quickly, if this function is outsourced, better planning needs to be done. If the work is to be outsourced, an organisation cannot

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

wait until an incident takes place which requires investigation, and then begin sourcing external practitioners. It is important that an organisation that does not maintain an in-house digital forensics capacity, at least identify an external service provider and enter into a service arrangement, which will ensure that they can react rapidly once and incident has been discovered.

E. Compliance and Monitoring

Once a digital forensic readiness program is in place, it must be monitored, and complied with or else risk the failure of the entire digital forensic readiness program. This can be achieved by having all members of the organization acknowledge that they understand all the policies and procedures, and the running of regular awareness sessions.

In addition to the above, regular audits of the program must be done, and action instituted in any cases of non-compliance.

.

IV. SMALL AND MEDIUM BUSINESS

The definition of a small to medium enterprise varies greatly depending on the region and context in which one is discussing, South African business is no different. The proposed research will define a small to medium enterprise (SME) according to a the South African National Small Business Act's small business schedule [1]. This schedule defines various requirements, such as turnover, number of employees, etc, which are primarily differentiated according to the business's industry. The proposed research will deal with SMEs from various industries and will ensure that the specifications detailed in the Act are adhered to. However, for the purposes of succinctness and clarity, the research will make use of a generic definition by aggregating variables across industries. Therefore, a South African small to medium enterprise shall be according to the following:

A small to medium enterprise (SME) is defined as any independent, non-governmental business entity employing less than 200 employees, with an annual turnover under R50 million [1].

V. VULNERABILITY

Small to Medium Enterprises (SME) are particularly at risk to high-frequency / low impact incidents as their limited resources (both financial and technical) are likely to increase the relative impact such an incident would have on the organisation's business's viability. For example, a smaller business is less likely to survive an R8mil Intellectual Property (IP) fine (a typical IP fine resulting from employee downloading films from file-sharing website).

A second example is where a company cannot recover losses after an incident due to lack of evidence, or the cost of obtaining such evidence might be out of reach if the company was not properly prepared for the incident. The recovery of losses is a real possibility that is often ignored while planning responses to criminal incidents, but any recovered loss is immediately added to the bottom line of the organization and planning for recovery should therefore receive serious attention during the planning of forensic readiness.

The smaller organisation is also less likely to be able to afford a full forensic investigation performed by third party experts, thus limiting their access to the digital evidence that would allow the business to prove their innocence (as well as supporting the identification of those responsible).

The requirement for forensic readiness within an organisation is determined through the potential risks which pertain to that organisation regarding information security. These risks are generally determined by assessing the potential threats to an organisation's data, as well as the value of that data to an organisation and its customers (Rowlingson, 2004). However, determining commonly accepted concepts and methods by which this assessment can effectively and efficiently occur have proven problematic in both business and literature [2]. It should be noted that many of these risk assessments neglect lower level scenarios, such as transactional or internal disputes, resulting in an incorrectly established risk profile [9]. This can lead to ambiguous or inaccurate information regarding an organisation's digital evidence requirement [8].

VI. ORGANISATIONAL CHARACTERISTICS

There is no simple solution to determine the forensic readiness needs of an organization and much more research is needed to determine an optimal model for this purpose. Some of the more important characteristics that influence the digital forensic readiness strategy are the following:

- Number of employees
- Access to financial instruments
- Public profile of company
- Industry type
- Information Technology skills available in company
- Funds available for a readiness program

A. Number of employees

A high number of employees will obviously increase the risks for criminal incidents. This is however no clear indicator of criminal activity, as the type of work conducted will have a strong influence on the possibility of that type of activity.

It cannot be assumed that employees without access to financial systems cannot conduct criminal activity that can be traced with digital forensics. It is for example possible that such staff can steal stock and that the activity can be traced by surveillance and access systems.

A single accountant handling a company can also be a weak link that can destroy important information or have easy access to bank accounts.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

B. Access to financial instruments

It is obvious that if more staff have access to financial instruments, there is a higher likelihood of fraud or other forms of financial crime.

C. Public profile of the organisation

Organisations like financial consulting firms who are responsible for the handling of assets that belong to the public are normally more dependent on public opinion than for instance a company that manufactures general goods.

Such organizations need to handle incidents quickly and efficiently in order to minimize bad publicity with the resulting losses.

D. Industry type

The industry type is likely to be a strong predictor of the risk an organization faces. A diamond mine or financial firm is likely to have a higher incidence of criminal activity than for instance an engineering firm that manufactures steel goods due to the higher value and ease with which stolen items can be turned into cash.

E. Information Technology skills available in company

If the organization has Information Technology skills available in house, it might be possible to multiskill some staff to handle incidents or at least prepare for it. This could mean a saving on outsourcing costs and a faster response to incidents.

F. Funds available for a readiness program

The funding available for a digital forensic readiness program can play an important role in the strategy selected. To develop an in house capacity for the handling of incidents can be a costly exercise and could play a determining role in the decision to outsource such services.

There are many other organizational characteristics that could play a role in the development of a digital forensic readiness program and an attempt should be made to find a unique and optimal solution for each organization.

VII. CONCLUSION

Many factors determine the strategy for digital forensic readiness in small to medium sized companies. As it is more difficult for smaller organizations to absorb the losses caused by criminal and related incidents, it is important that the digital forensic readiness of such organizations is optimized, as it could be the only defense against the demise of the organization in the case of a serious incident.

REFERENCES

[1] Department of Trade and Industry (DTI). *National Small Business Act.* Retrieved February 9, 2010, from http:/www.dti.co.za/smmb.pdf, 1996.

[2] Endicott-Popovsky, B., & Frincke, D. "Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations". *workshop on information assurance: computer forensics.* West Point, NY: United States: IEEE, 2006

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

[4] Imtiaz, F. "Enterprise Computer Forensics". *Proceedings of the 4th Australian Digital Forensics Conference* (pp. 29-35). Perth: Edith-Cowan University, 2006.

[5] Jordaan, J. "The case for digital forensic readiness", Unpublished, 2009.

[6] Kent, K., Chevalier, S., Grance, T., & Dang, H.. "Guide to Integrating Forensic Techniques into Incident Response". Gaithersburg: National Institute of Standards and Technology,2006.

[7] Patzakis, J., Mann, S., & LaBancz, M.. "Computer Forensics in the Global Enterprise". 1st Australian Computer, Network & Information Forensics Conference. Perth: Edith-Cowen University,2003.

[8] Rowlingson, R.. "A Ten Step Process for Forensic Readiness". *International Journal of Digital Evidence* ,pp1-28, 2004.

[9] Sommer, P. (2009). *Directors' and corporate advisors' guide to digital investigations and evidence.* Retrieved 03/12, 2009, from http://www.iaac.org.uk/Portals/0/DigitalInvestigationsGuide.pdf

[10] Tan, J. "Forensic readiness*"* (Technical. Cambridge USA: @stake, Inc. doi:17/01/2001

[11] Taylor, C., Endicott-PoPousky, B., & Frincke, D. A.. "Specifying digital forensics: A forensic policy approach". *Digital Investigation, 4*, pp101-104. Retrieved from ScienceDirect database, 2007.

[12] Vacca, J. R. "Computer Forensics: Computer Crime Scene Investigation" (2nd ed). Boston: Charles River Media, 2005.

[13] Zatyko, K. "Defining Digital Forensics". Forensic Magazine , 4 (1), pp. 18-22, 2007.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE