A DIGITAL FORENSIC INVESTIGATIVE MODEL FOR BUSINESS ORGANISATIONS

Jock Forrester and Barry Irwin (CISSP)

SNRG

Department of Computer Science
Hamilton Building, Rhodes University, Grahamstown, 6139
Email: J.Forrester@ru.ac.za, B.Irwin@ru.ac.za

ABSTRACT

When a digital incident occurs there are generally three courses of actions that are taken, generally dependant on the type of organisation within which the incident occurs, or which is responding the event. In the case of law enforcement the priority is to secure the crime scene, followed by the identification of evidentiary sources which should be dispatched to a specialist laboratory for analysis. In the case of an incident military (or similar critical infrastructures) infrastructure the primary goal becomes one of risk identification and elimination, followed by recovery and possible offensive measures. Where financial impact is caused by an incident, and revenue earning potential is adversely affected, as in the case of most commercial organisations), root cause analysis, and system remediation is of primary concern, with in-depth analysis of the how and why left until systems have been restored.

Traditional investigative models follow the general process of: identify the incident, secure the scene and/or evidence, analyse the evidence, generate a report on the findings and present the outcome. This approach is more suited towards law enforcement than to the business world.

The business environment lends itself to an approach similar to that of the military, namely to be able to identify the incident, patch the necessary system(s) and continue earning revenue. The only addition is that the business is more likely to want to press charges in a court of law than launch a counter offensive.

In the generic investigative model, there is little leeway for a business's incident responders to satisfy the need to return the systems to operational status as quickly as possible whilst preserving the necessary evidence and has to be able to mount a successful prosecution. These two goals can be mutually exclusive as a thorough investigation needs time and during this time the business will loose revenue by not having its system live.

The model presented in this paper builds on the traditional investigative model as prepared by the Digital Forensic Research Workshop (DFRWS) and provides a mechanism to conduct the two potentially mutually exclusive processes in parallel.

KEY WORDS

Digital Forensics, Investigative Models, Incident Response, Investigation Objectives

A DIGITAL FORENSIC INVESTIGATIVE MODEL FOR BUSINESS ORGANISATIONS

1 INTRODUCTION

After an incident has been identified within a business organisation it needs to be able to recover from the incident as quickly as possible in order to minimise costs incurred due to downtime.

Traditional investigative models are linear in nature and require the affected systems to be taken offline during the investigation; subsequently the organisation can potentially loose revenue. The system is typically taken offline until the investigation is complete. A digital investigation can take several months to complete, particularly in a law enforcement context.

The model presented in this paper presents a digital investigative model that allows the organisation to conduct the investigation in parallel to restoring services. Therefore the revenue stream is restored whilst the evidence is preserved to a standard that is admissible in a court of law.

Having identified the incident, the physical crime scene is secured, the digital crime scene is secured and the model splits into two parallel tasks. The investigation continues whilst the service is being restored. The original evidence is stored securely whilst alternate hardware is being used to rebuild the affected systems. The original evidence is stored either on the original hardware or the images of the original disk are stored in a forensically sound manner.

This paper examines the investigative phases of the proposed of model. The completed model will form a complete investigative framework for a business organisation. The framework will provide guidelines ranging from forensic readiness initiatives, leveraging of IT governance programs, policies and procedures to implement within the South African legal environment, and an investigative model.

Once work on developing the full model is complete, it will be validated by analysing incidents from case studies and industry. The outcomes of the models used in the investigation will be compared to the outcomes of the proposed model.

2 CURRENT INVESTIGATIVE MODELS

Four existing investigative models are reviewed. Three of the models highlight different goals of an investigation and they each present a different methodology to achieve those goals. The DFRW produced Table 1 which illustrates the different and sometimes conflicting goals of a digital investigation, depending on the investigating entity.

In Table 1 the objectives and environment of an investigation for law enforcement, military and business organisations are listed. In a law enforcement investigation, there is a more relaxed time frame in which an investigation can be conducted. This is in contrast to an investigation conducted in a military or business context in which prosecution is a secondary objective. In a business environment, however, prosecution may become a primary objective depending on the severity of the incident and the costs incurred.

Due to this potential clash in objectives an organisation needs to be able to restore services with minimal cost incurred to the business as well maintain an irrefutable and sound investigation process.

The models summarised below each highlight aspects that will be incorporated into the proposed model. Four models are described; the first is from the military's perspective, the second is a model described by the DFRW which forms the basis for the majority of the existing models. The next model is the one described by the United States Department of Justice and is used

exclusively by law enforcement agencies. The final model reviewed highlights the importance of the surrounding physical circumstances when conducting a digital investigation.

AREA	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military Operations	Continuity of Operations	Prosecution	Real Time
Business and Industry	Availability of Service	Prosecution	Real Time

Table 1: Defining investigation objectives [3].

2.1 The Military's Perspective

Military Cyber Forensics is defined by Giordano and Maciag as follows [1]:

- "The exploration and application of scientifically proven methods to gather, process, interpret, and utilize digital evidence in order to:
  - Provide a conclusive description of all cyber-attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration.
  - Correlate, interpret, and predict adversarial actions and their impact on planned military operations.
  - Make digital data suitable and persuasive for introduction into a criminal investigative process".

The concept of computer forensic analysis with regard to military operations is based on intrusion detection [1] as protecting the military's information infrastructure requires the real time identification, assessment and analysis of incidents. In addition to the real time nature in which the investigation is conducted, the target computer cannot be quarantined or taken offline as with law enforcement models or sometimes that of business investigative models.

The results of the real time investigation play a pivotal role in the military's tactical decision making process. This process is also called the OODA Loop (Observe-Orient-Decide-Act) [1].

"The goal is to 'get inside of the adversary's OODA cycle' by continually reducing the amount of time it takes for our military to observe and respond to the enemy's actions so that the adversary's ability to react is outpaced by our military actions" [1]. See Figure 1 depicts a graphical interpretation by the authors of this paper.

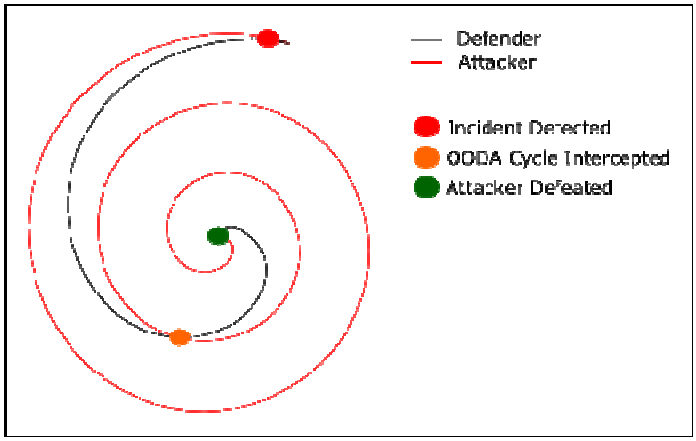

Figure 1: Graphical view of the Military's OODA cycle [1].

This is achieved by the recovery, preservation and analysis of many potential sources of digital evidence from a vast array of networked devices. Ideally the results of the investigation need to be available immediately after the attack or even during the attack itself.

The challenge facing a digital investigation in a military based scenario is speed. The investigation needs to happen in near real time whilst not sacrificing the quality, integrity and accuracy of the evidence collected.

2.2 Digital Forensics Research Workshop

The Digital Forensics Research Workshop held in 2001 produced the following investigative model as the basis for future research.

The DFRW model is divided into seven steps. Most of the steps are sequential in nature, however the process should not be cast in stone. If in the analysis phase a new potential source of evidence is found, then the Preservation, Collection, Examination and Analysis phases would be repeated [3].

The Investigation is initialised during the identification phase. This is precipitated by either a crime that has been reported or an incident within an organisation. In the Preservation Phase the case management procedures start, including the chain of custody. Evidence is then duplicated and preserved [3].

In the collection phase, the preserved evidence is collected using approved software, methods and hardware. For example in this phase temporary internet files are found and stored for examination in the next phase. Potential sources of evidence are then examined using filtering and pattern matching techniques. The idea is to reduce the volume of evidence and identify the relevant pieces of evidence to be used to recreate the crime scene or the incident. In the analysis phase the evidence is collated and linked together to reconstruct the crime scene [3].

In the presentation phase, the investigation is documented and either presented as expert testimony or as a report to a superior regarding an incident. Lastly, in the final phase a decision is made regarding an incident, or a verdict is made in a court of law [3].

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event or Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synchronisation	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Event or Crime Detection		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Recovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
		Data Reduction		Spacial		
		Recovery Techniques				

Figure 2: Digital Forensics Research Workshop [3].

2.3 Law enforcement process model (Department of Justice)

The US DOJ released a guide for first responders to crime scenes on the appropriate steps to take when encountering digital evidence.

The guide makes the following assumptions before elaborating on the steps to be taken. It assumes that the officers have the necessary legal authority to search the scene, then that the crime scene has been secured and documented and that the officers are using the appropriate crime scene protective equipment. For example, gloves to avoid undue contamination [4].

The guide deals with the following four phases:

The collection phase involves the search for, identification, collection and documentation of various types of digital evidence at the crime scene. This not only includes the PC itself, but any optical or magnetic media, networking equipment or other miscellaneous PC equipment.

The examination phase takes place at a specialist laboratory with the necessary tools and skilled personnel. Here the individual pieces of digital evidence are found. For example: data in slack space, image files in “temp” directories and internet browser histories. Once all the evidence has been found, the evidence is then sorted to extract useful pieces of data. This is an extremely important step considering the amount of data that can exist on a computer system.

The analysis phase differs from the examination phase as it looks at the results from the examination phase to extract evidence of relevance to the case. In other words, the phase looks for evidence of relevance and probative value. It is in this phase that a timeline of the incident is created.

In the last phase of the DOJ model, a written report is generated. It contains an outline of the processed followed during the investigation and the outcomes of the analysis phase.

2.4 Digital Investigations in a Physical Investigation

Research conducted as a part of the Center for Education and Research in Information Assurance and Security at Purdue University by Brian Carrier and Eugene Spafford recommends modelling the digital investigation model on the traditional investigation model used for physical crime scene investigations [2].

The rationale behind this approach is that the investigative model used in a real world crime scene has been refined through the experiences learnt from a vast amount of physical crime scene investigations. The model can be used by law enforcement and corporate incident response teams.

The gist of the model is to regard the computer as a secondary crime scene, a digital crime scene. The computer is typically one piece of physical evidence; however it can contain many different sources of evidence within it. Each of the sources of evidence can be further analysed to identify ownership, location and timing [2].

There are seventeen phases within the model, broken up into five groups. The groups are as follows: A Readiness Phase followed by the Deployment Phase after which the Physical Crime Scene Investigation Phase starts. It is at this point that if there is any digital equipment collected or identified at the physical crime scene that the Digital Crime Scene Investigation Phase starts. After the Physical Crime Scene Investigation and the Digital Crime Scene Investigation Phase comes to close, both phases lead into a Review Phase.

Figure 3 depicts the 5 main phases of the model. The Physical and Digital phases feed into each other in terms of locating potential sources of evidence.

The Readiness Phase is broken down into an Operations Readiness and an Infrastructure Readiness Phases. The Operations Phase ensures that the necessary training, support as well as the necessary equipment has been provided for when an incident occurs. The Infrastructure Readiness

Phase ensures that the necessary data is available and secure for the investigation [2]. This phase applies to organisations that maintain an environment that may be attacked.

The deployment phase provides a means for the incident to be detected, confirmed and reported. During the detection and notification phase an incident is detected and the appropriate response procedures are followed. During the confirmation and authorisation phase if the model is being used by law enforcement, a search warrant(s) may be required. For corporate incidents, a search warrant is not necessary so long so the necessary privacy policies are in place [2].

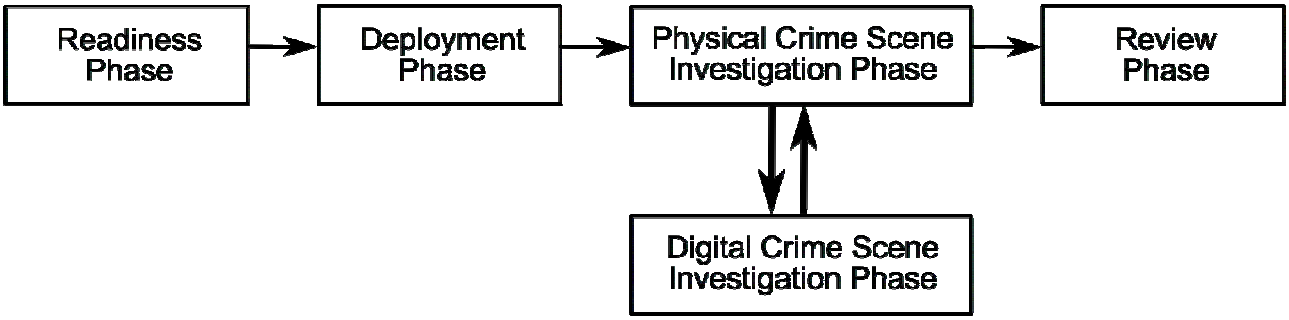

Figure 3: Physical and Digital Investigation Model. [2].

Figure 4 details the sub phases of the Physical Investigation Phase. It also shows how a Digital Investigation is started. Figure 5 details the sub phases of the Digital Investigation Phases and how it leads back into the Physical Investigation phase and the recreation of the physical crime.

During the physical crime scene investigation, physical evidence is collected and analysed with the aim to reconstruct the events that took place. In the event of a law enforcement case, a law enforcement officer will be in charge of the crime scene. Inside an organisation, the senior member of the incident response will be in charge of the crime scene.

When a digital incident occurs within the organisation is physical and / or digital boundaries, the physical crime scene can be regarded as the room in which the server or desktop computer is located in. In the preservation sub phase the actions taken to preserve the crime are the same whether it was a digital or physical incident. In terms of a physical crime, the following activities would take place: the exits would be secured, wounded treated, suspects detained and witnesses identified. In terms of a digital incident, the physical location of the affected machines should be secured; access to the machine/server room/building should be established as well as identifying potential witness's, if any. This phase preserves the actual crime scene so that evidence can later be identified and collected. Preservation of evidence does not occur in this phase.

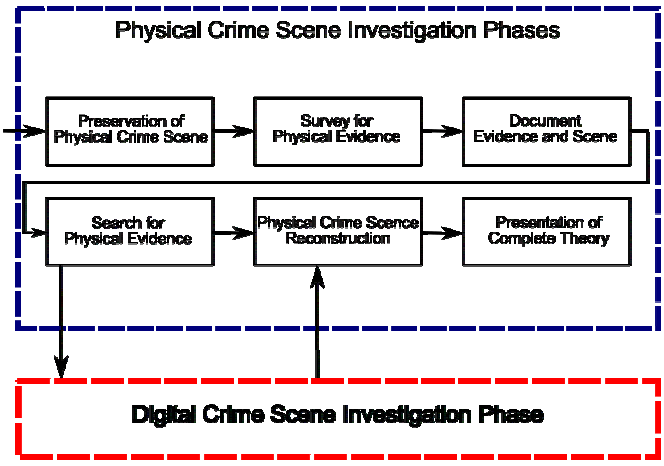

Figure 4: Physical Crime Scene Phases [2]

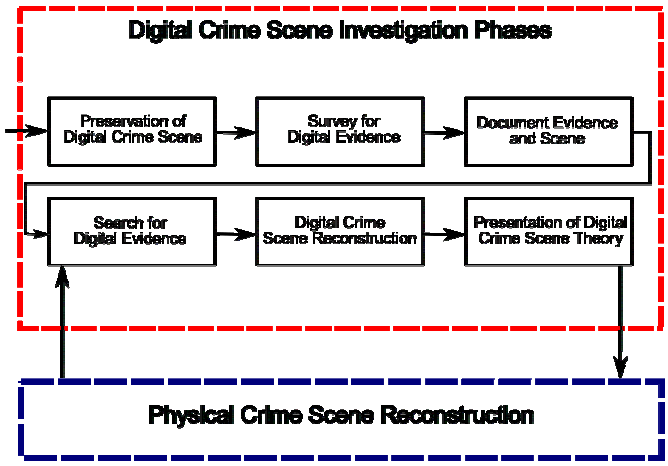

Figure 5: Digital Crime Scene Phases [2]

In the survey sub phase, the crime scene is examined. Obvious and fragile pieces of evidence are identified and an initial theory of the crime is developed. In terms of a murder investigation, possible murder weapons would be identified as well as the suspect who entered the house where the murder took place. In a digital incident, examples of physical evidence that are identified could include the computer(s), location of the computer(s), network connections, CDROMs or DVDs, disks and PDA's. Any digital equipment that is attached to a network should be considered fragile as commands could be executed remotely [2].

The documentation sub phase captures as much information as possible so that the crime scene is preserved. It is important to take note of all connections leading into any digital equipment, size and number of hard drives and the amount of memory.

The Search and Collection Phase is an in-depth search of the crime scene for additional evidence to be collected. In a physical crime scene this could include dusting for fingerprints, or DNA analysis. In a digital incident, this could entail retrieving firewall logs, Virtual Private Network (VPN) logs, and server update logs. This phase is where the digital crime scene investigation starts.

Evidence collected from the Digital Crime Scene Investigation Phase is piped into the reconstruction sub phase. The reconstruction sub phase organises the results from the physical and digital evidence to develop a theory for the incident. In the case of a digital incident, the results from the digital crime scene investigation are correlated with the physical evidence to link a person to the digital events.

The Digital Crime Scene Investigation Phase begins when physical evidence of a digital nature is collected. This can include any digital media, network traffic captures and a complete server or desktop system. In this model, each digital device is regarded as a separate crime scene. The results are then presented to the physical crime scene reconstruction sub phase.

The preservation sub phase involves preserving the digital evidence that could change or of a volatile nature. This could entail isolating the system from the network, capturing page files and memory before turning the computer off, identifying suspicious processes that are running and securing log files [2].

The survey sub phase of the Digital Crime Scene occurs in a secure environment using a clone of the affected system. If it is necessary to conduct the survey phase on a live system, a forensic copy should still be taken for record keeping purposes. This phase, like its physical counterpart identifies the obvious pieces of evidence.

All the evidence found during the Digital Crime Scene investigation is properly documented in the documentation sub phase. Measures should be taken to verify the integrity of the evidence; this typically involves creating hashes of the evidence. Part of the documentation that is collected is the chain of custody forms that are vital when the case is elevated to a court of law.

During the search and collection sub phase of the Digital Crime Scene, a more thorough examination and analysis of the digital evidence identified in the Physical Crime Scene and in the Survey Phase of the Digital Crime Scene is conducted. This is the most time consuming part of the investigation.

The reconstruction sub phase will identify how the digital evidence came to exist, and what the existence means. The evidence is also assessed based on the amount of trust that can be placed on it. For example: Local log files may have been tampered with if an attacker managed to gain root on a Linux / BSD web server. However the remote syslog files stand less chance of being tampered with.

Finally, the evidence found during the digital crime scene investigation is presented to the physical crime scene investigation team during the presentation phase. In the physical crime scene's

presentation phase, the evidence collected from the physical and digital investigations is presented in court, or to the management of the organisation.

The last stage of this model (Figure 2) is conducted after the evidence has been presented in a court of law or to management. It is the Review Phase and its goal is to identify possible areas of improvement.

2.5 Discussion

The military cyber forensics model emphasises the importance of being able to identify the incident, counter the incident and defend against it and counter attack. It is important for the military investigating officers to be able to keep services and system online whilst capturing, analysing and preserving evidence. The Digital Forensics Research Workshop model forms the basis for most digital forensic models. The major phases are sequential in nature with many of the sub phases being reused in many of the phases to reinforce the process of an investigation. No provision is made for service restoration in the model. In the United States Department of Justice the investigative model is straight forward. Secure the crime scene, collect sources of evidence, examine those sources of evidence, analyse the evidence and then a reporting on the findings is presented. The potential sources of evidence are taken to a specialist lab for analysis.

The last investigative model (Digital Investigations in a Physical Investigation) reviewed builds on the experience that law enforcement has gained through real world investigations. The model builds on the premise that a digital investigation occurs within a law enforcement context, although the model is extendable to business, and that the digital crime is located within a physical crime scene and the two crime scenes interact with each other. This model is particularly useful to the incident investigator as it does not operate solely in the digital realm and that there are potential sources of evidence in the real world.

These models show a distinct pattern of seize evidence, analyse, prosecute and then return equipment. The only exception is that of the military who have to be able to analyse the evidence in real time and restore services. Prosecution is a secondary objective. A business has two primary objectives with regards to a digital investigation. They need to minimise impact on services and therefore revenue loss, and also to be in a position to prosecute the offender in a criminal and civil court of law.

3 REQUIREMENTS FOR THE NEW MODEL

From the above digital forensic models and objectives the following requirements of the new model can be extracted.

- Satisfy the potential conflicting objectives of reducing revenue loss and conducting a legally sound investigation.
- Be able to conduct a legally sound investigation.
- Be able to adjust the rigor of the model based on the incident type.
- Must be holistic in terms of digital investigations, incident response and organisational goals.

The model will attempted to craft a working solution taking the above requirements into account.

4 ORGANISATIONAL INVESTIGATIVE MODEL

The models reviewed above cater for one of two goals, namely prosecution or service restoration. These two goals can be mutually exclusive in nature, as in order to prosecute, evidence needs to retrieved, analysed and interpreted and this is a prolonged process. In contrast to service restoration, no preservation of evidence occurs, instead the problem is fixed and service restored.

In an organisation both of these goals may exist in different circumstances. For example if an employee is suspected of committing fraud and if the employee has been suspended, then the PC can be seized, given that the appropriate mechanisms are in place, and then investigated for evidence with a relatively extended time frame. On the other hand, if the employee has not been suspended, but an investigation has been authorised, then the potential evidence needs to be secured and the desktop returned so that the employee can carry on working without suspicion.

Given the amount of time required to conduct a proper investigation, it would not be feasible to carry the investigation out overnight. It would, however be feasible to image the desktop over night and conduct the investigation on a copy of that image.

The above process is similarly suited to the circumstance of a server that runs revenue earning systems being compromised. There are two equally important goals that need to met: evidence needs to be preserved and a safe service restored. Downtime is minimized whilst the affected machine(s) is imaged for evidence preservation. Once the evidence has been preserved, the investigative team can start their investigation to determine the extent of the intrusion whilst the incident response team identifies how the machine was compromised in order to determine the appropriate course of action.

The model presented in Figure 6 is an initial attempt to create an investigative model that satisfies the two conflicting goals mentioned. The focus of this paper is on the investigative side of the model and will concentrate on the following phases: Deployment, Incident Evaluation, Scene Preservation, Investigation and Service Restoration. The remainder of the phases represent future work to be carried out. However these phases will be briefly described for completeness.

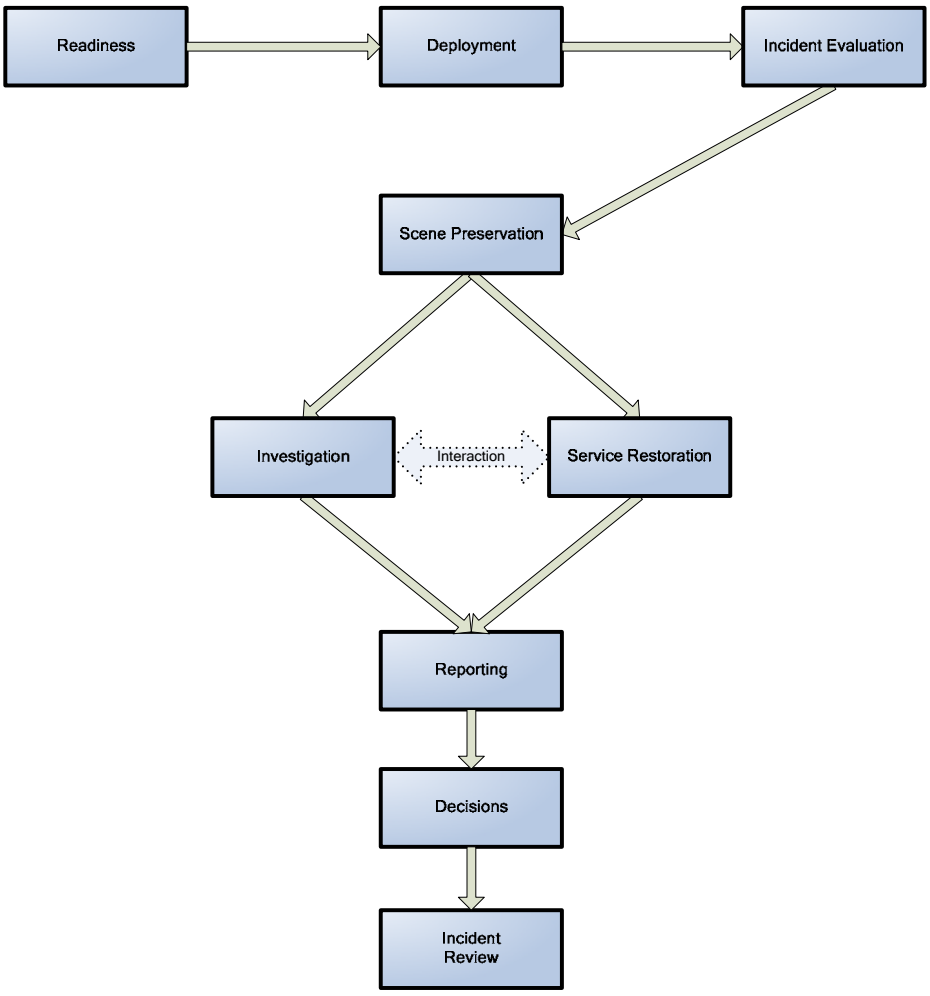

Figure 6: Proposed Organisational Investigative Model

The Readiness Phase of the model prepares the organisation itself for an investigation in terms of people related areas such as: training investigative teams, developing and refining the procedures used and establishing the necessary polices that allow for an investigation and evidence collection to occur within the organisation. This phase will also setup and maintain the technical infrastructure required. This includes the forensic lab, if any, central logging servers and time servers.

In the Deployment Phase, the investigation has been started by one of several sources. For example: Management could start an "incident" by requesting that an employee's internet usage be investigated due to complaints from co-workers regarding offensive material being viewed. A technical event, such as an Intrusion Detection Sensor (IDS) Alert, can also start an incident. Once an incident has been triggered, the incident response team is dispatched to conduct an initial overview assessment of the incident to determine the scope of the incident.

In the Incident Evaluation Phase an initial assessment of the incident is carried out The goal of this phase is to gain an understanding of the incident in terms of systems, users and data affected by the incident. Once this is understood, the correct course of action can be established. It is extremely important to identify the incident type correctly as the subsequent investigation is planned accordingly. If the incident is a breech of a server due to a vulnerability in the software or operating system, the service restoration team needs to identify the point of entry and how to patch the system before restoring to a production state.

Live system analysis tools could be used to analyse the system affected by the incident instead of taking it offline and imaging it, however there are risks involved. The tools used to analyse a live system can be misled by the attacker or an application called a rootkit left behind by the attacker. The rootkit application can intercept API calls to the kernel of the operating system and hide signs of its existence [5] [6].

Live system analysis should not be discounted altogether as it can reduce the amount of time needed to investigate a minor offence and it does add great value to the evidence collected via imaging in that it places the imaged evidence into context [6].

It is at this stage that it must be decided if the organisation may want to prosecute the offender in a court of law, as it is at this stage that more formal investigative models and evidence collection and handling procedures will be implemented so that the investigation's outcomes will stand up in a court of law. On the other hand, if the investigation's results will not appear in a court of law there is no need to incur the extra overhead of a formal investigation.

For example; an investigation of an employee suspected of committing corporate espionage needs to be conducted formally as the employee could be charged in a court of law as well the offending third party. In this scenario, law enforcement would be involved and would have to verify the evidence found and its integrity. This is in contrast to an investigation of an employee sending out "chain letters" from their work email address as this matter can be safely dealt with in-house and will not require the involvement of law enforcement and the courts. If the organisation is unsure, it should err on the side of caution and conduct a legally sound investigation.

Once a decision has been made about how to proceed with the investigation, the Scene Preservation Phase begins. At first the physical area around the digital crime scene needs to be secured and searched. This is in order to ensure that any additional physical digital evidence is found. This is perhaps more relevant for "desktop" investigations but there is merit in checking the server room for physical evidence as well. For example: CDs or DVDs, stiffy disks, USB Flash sticks or a USB Cable that could have been plugged into an external USB Hard Drive. Once the physical crime scene has been secured the various sources of digital evidence can be found, secured and preserved. Log files from routers, firewalls, servers and IDS systems need to be copied, hashed and stored. Hard disks need to be imaged, hashed and either the images stored securely or disks themselves stored. Depending on the investigation's context (formal or informal) the disks should

be removed from the machine and securely stored for a formal investigation, and then new ones installed for the next phase. In an informal investigation, the disks will not be removed and stored for evidence; the hashed image of the disk should suffice.

Once all initial sources of physical and digital evidence have been sourced, the model splits into parallel phases. It is in these parallel phases in the traditional models that an organisation can potentially loose substantial revenue. Only after the investigation has been completed can the revenue earning or work flow support system be restored. The repercussions for an organisation can be severe. The splitting of the proposed model at this stage is also suited to a scenario where an employee is suspected of committing an offence and an investigation of their machine has been requested. The machine can be imaged after hours, returned to the employee's desktop without them knowing.

The reasoning behind splitting the Investigation and the Service Restoration Phase is to reduce the downtime associated with a full investigation but to still allow for a legally sound investigation to take place. The Investigation Phase will follow a more traditional investigation pattern and represents future work to be done by the author. The investigation's goal is to establish a sequence of events against a timeline with supporting evidence about the incident and to suitably document this. The Service Restoration Phase aims to return the organisation's services to normal, if not in a more secure fashion. A report will be developed at the end of this phase on the incident which details how the incident happened, events that led up to the incident and recommendations to avoid the incident occuring again.

It is anticipated that the Service Restoration Phase will be completed well before the Investigation Phase, and as such, the report generated in the Restoration Phase will be used for immediate reporting needs. However it will form a part of the overall report that is generated in the Reporting Phase.

In the reporting phase the results, procedure and findings of the investigation are formally documented. The Service Restoration Report is included is this documentation. This report should include possible courses of action. The report is then presented to a higher authority, such as management or a human resources disciplinary board. When the report is presented a decision is made on what course of action is required. This phase is called the Decision Phase.

In this phase the incident alerter or duly appointed party determines the next course of action. This decision can be to inform the relevant law enforcement agency, an employee's supervisor or human resources.

The last phase of the model is the Review Phase. This phase is closely related to the Readiness Phase as its goal is to closely analyse the investigation and service restoration process in order to access possible areas of improvement. If any potential improvements are found, the policies and procedures are to be updated and staff retrained in the Readiness Phase.

5 FUTURE WORK

In this paper the focus has been on the investigation and deployment surrounding a digital incident. In future work the model will be refined and comprehensive policies and procedures created for the various phases of the model.

The Forensic Readiness Phase will be considerably expanded to include the formation of an incident response team, organisational policies and procedures and pre-emptive systems to be put in place. Corporate governance material will be analysed and sections that are useful to a Forensic Readiness program will be summarised and converted into a Forensic Readiness Policy.

Work will also be done to provide a legal context within which the model can operate. The relevant South African Acts, Conventions and Agreements will be analysed and evaluated and a legal framework crafted for the model.

6 CONCLUSION

Traditional investigative models are linear in nature. Most do not place an emphasis on returning the affected system to operational status as quickly as possible, but rather place the emphasis on a legally strong evidence collection process.

A similarity can be drawn between military systems and business systems, both are crucial to the existence of the entity. Without the systems operating all the time the military would not be able to mount an effective campaign, similarly without the business's systems operating the business can loose revenue.

Whilst an emphasis needs to placed on keeping critical systems operating, it is still important to remember that a law may have been broken, or an organisation's policy violated and that there are repercussions. Should a revenue earning system be hacked and taken offline, the business will want to press charges and lay claim for loss in revenue.

In order to press charges or start a civil suit, the business will need to present original evidence that still maintains its integrity, authenticity and completeness. The model presented in this paper acknowledges the importance of systems within an organisation and the importance of evidence collection.

The model presents an investigative process that allows for accurate evidence capture and analysis whilst reducing the downtime faced by an organisation during the investigative phase.

While still in early stages, the proposed model presents a conceptual map offering a series of operations sensitive to the temporal and financial nature of investigating in a commercial environment.

7 REFERENCES

[1] J. Giordano and C. Maciag, "Cyber Forensics: A Military Operations Perspective," *International Journal of Digital Evidence*, vol. 1, issue 2, Summer 2002.

[2] B. Carrier and E.H. Spafford, "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence*, vol. 2, issue 2, Fall 2003.

[3] G. Palmer, "*A Road Map for Digital Forensic Research,"* Report from the First Digital Forensic Research Workshop (DFRWS), August, 2001.

[4] "*Electronic Crime Scene Investigation: A Guide for first responders,"* National Institute for Justice, NIJ Guide #: 187736, http:///www.ncjrs.org, July 2001.

[5] B. Carrier, "Risks of Live Digital Forensic Analysis," *Communications of the ACM*, vol. 49 no. 2, pp 56-61, February 2006.

[6] F. Adelstein, "Live Forensics: Diagnosing your System without Killing it First," *Communications of the ACM*, vol. 49 no. 2, pp 63-61, February 2006.

8 ACKNOWLEDGEMENTS

This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Comverse, Verso Technologies, Tellabs and StorTech THRIP, and the National Research Foundation.