DIGITAL FORENSICS: A MULTI-DIMENSIONAL DISCIPLINE

CP Grobler, Prof B Louwrens

University of Johannesburg, Department of Business IT

Nedbank, SA

talania@uj.ac.za

011 406 3551

buksl@nedbank.co.za

011 294 2260

ABSTRACT

Computers and the Internet are becoming a fundamental way to communicate worldwide. Information security has become an essential part of our daily lives. Organizations have accepted that the protection of information and information assets is a fundamental business requirement and are implementing an increasing number of security counter measures against potential threats.

However, when a security incident has taken place, many organizations do not have proper guidelines to conduct a forensic investigation and often fail to bring the investigation to a productive conclusion (Sinangin D, 2002). Many organizations do not regard forensic investigations as a priority item. The key role of computer forensics is the protection, adducing and presentation of evidence, in that order. In all abuse cases, protection of the evidence is both critical and central to the organization's ability to investigate and take action against the abuser (Sheldon A, 2004).

This paper will define Digital Forensics (DF) and propose DF as a multi-dimensional discipline and identify Corporate Governance, Policy, People, Legal and Ethical and Technology as dimensions of DF within the context of process and tools.

KEY WORDS

Digital Forensics, Multi-dimensional discipline, Governance, Policy, Legal, Ethics, DF readiness

1 INTRODUCTION

Information is a sought-after commodity by competitors and criminals to either increase their competitive advantage in the marketplace or enable criminals to plan attacks on critical targets. Information is fuel for the cyber war. Computer crime is a very lucrative activity that continues to grow in prevalence and frequency (Casey, 2000; CERT/CC, 2003; Kruse and Heiser, 2002; Richardson, 2003).

Similarly, the introduction of computers as a criminal tool has enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. In particular, the surge of technical competency by the general population, coupled with anonymity, seems to encourage crimes using computer systems since there is a small chance of being prosecuted, let alone being caught (Reith, 2002). These "cyber-crimes" are not always new crimes, but rather traditional crimes translated into a cyber world by exploiting computing power and accessibility of information.

The increase of criminal activity places a strain on law enforcement and governments. Courts no longer require only document-based evidence but also digital/electronic-based evidence. Criminal investigations require solid, well documented, acceptable procedures and evidence. Normal forensic investigations are no longer suitable or applicable and digital forensic investigations needs to be undertaken.

Various forensic investigation methodologies exist, but most of them concentrate on the investigation process. There is a need for an integrated management model for pro-active and re-active Digital Forensics (DF) in an organization.

2 LAYOUT OF THIS PAPER

The paper consists of three main parts. The first part defines DF and discusses the relationship between digital forensics, computer forensics and other forensic disciplines.

The second part of the paper proposes DF as a multi-dimensional discipline where the various dimensions are inter-related and should not exist in isolation.

In the last part of the chapter the authors map out the various dimensions to a DF control framework.

3 WHAT IS DIGITAL FORENSICS?

From the earliest days, men have been interested in the cause of an event. Whenever an incident occurred, men wanted to know what happened or what went wrong. The process of investigating what went wrong, with the gathering of sufficient evidence to prove the cause of the event can be seen as a forensic investigation.

Forensics is the use of science and technology to investigate and establish facts in criminal and civil courts of law (American Heritage Dictionary of the English language, 2000). The goal of any forensic investigation will be to prosecute the criminal or offender successfully, determine the root cause of an event and determine who was responsible. The way the investigator conducts the investigation is crucial as the evidence must be able to stand up to legal scrutiny. Not all reported incidents will be taken to court, but all cases should be handled as if they will be taken to court. (Kruse and Heiser, 2002)

The environment in which digital crimes are committed has changed drastically with the emergence of digital devices e.g. digital fax, the internet and wireless devices. It is no longer sufficient to only investigate the hard drive of the victim's PC (computer forensics), as there may sufficient evidence gathered for successful prosecution. Cyber-trained defense attorneys require the chain of evidence to must link the attacker to the victim. (Stephenson, 2003). DF is more

comprehensive than computer forensics. With the emergence of new technologies e.g. wireless communications and the internet, computer forensics has become a subset of DF. Various overlaps with other forensic disciplines exist. All evidence must be gathered and investigated during an investigation. Figure 1 is a diagrammatic representation of how digital forensics, computer forensics, physical and other forensic investigations can overlap. The DF investigation must include all aspects, physical evidence for example physical credit cards, printouts, cameras etc. as well as digital evidence. Results from pathological, ballistic and other investigations must be included in an investigation.

DF can be defined as the efficient use of analytical and investigative techniques for the preservation, identification, extraction, documentation, analysis and interpretation of computer media which is digitally stored or encoded for evidentiary and/ or root cause analysis and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. (Kruse & Heiser, 2004; Digital Forensic Research workshop, 2001; Reith, 2002; Rawlingson, 2004).

DF can be conducted in a pro-active as well as a re-active manner. Re-active forensic investigations will occur after an incident has taken place. Most of the current investigations are re-active. Typically an investigation will focus upon the legal and law enforcement aspects of an incident or it will be used to determine the root-cause that permitted the incident (Stephenson, 2003).

Pro-active DF will enable an organisation to become DF ready. DF readiness can be defined as the ability of an organization to maximise its potential to use digital evidence whilst minimising the costs of an investigation (Rawlingson, 2004).

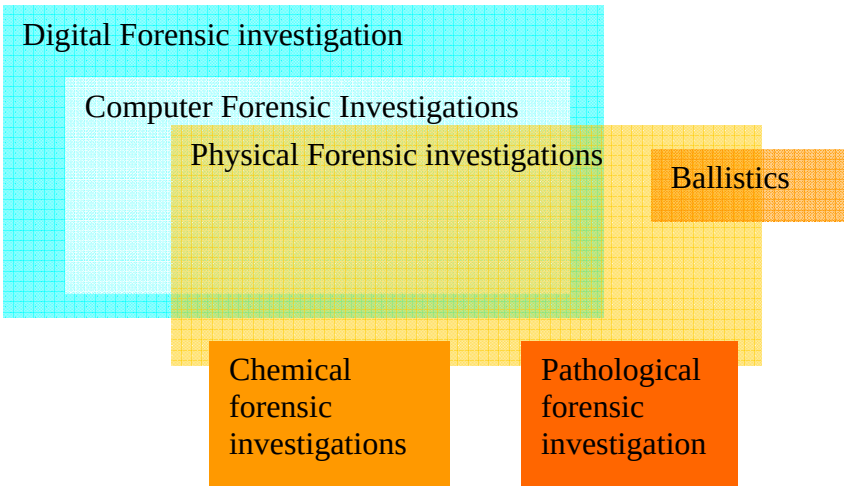

Figure 1 Relationship of digital and physical forensic investigations

Various methodologies exist to conduct DF investigations. Beebe and Clarke (2004) propose a framework or model that encapsulates all phases and activities of other prevailing models to date (Palmer, 2001; Reith et al, 2002; Carrier and Spafford, 2003). This is a multi-tier, hierarchical framework to guide digital investigations, but this model also only concentrates on the investigation but does not cater for other digital devices e.g. personal data devices (PDA's), digital cameras, telephones and removable storage devices (Beebe and Clarke, 2004). The model, however, supplies the investigator with clear objectives and steps to achieve the objectives to conduct the investigation. The model does not consider the legal implications, requirements for DF readiness in

the organization, training of staff or the impact that DF can have on the corporate governance of the organisation.

There is a need in industry for a an integrated Digital Forensic Management Model (DFMM) that will guide management to create DF in the Corporate Governance of the organization, promote DF readiness, guide investigations, consider and enforce the legal requirements and guidance on the correct technology / tools to use.

This model must be scientifically sound and legally accepted. This model must also ensure that the chain of evidence is maintained and that all evidence will be admissible in court. According to a survey done - (Electronic Security Breaches Survey, 2002; Singangin, 2003) - only 10% of UK businesses have appropriate forensic computing guidelines.

In the next part of the paper the authors will propose that DF is a multi-dimensional discipline. The concept of DF as a multi-dimensional discipline will be used in future research to define and verify an integrated DFMM.

4 DIGITAL FORENSICS IS A MULTI-DIMENSIONAL DISCIPLINE

Information Security (IS) is a multi-dimensional Discipline. Von Solms (2001a) has identified various dimensions for Information Security: People, Policy, Risk Management, Legal, Ethical, Insurance, Technology, Strategic Governance and Operational Governance etc. In a subsequent study an assessment model for Information Security in an organisation was developed by referring to the following dimensions of IS: Corporate Governance, People, Policy, Legal, Compliance and Technology Dimensions of Information Security (Grobler CP & Von Solms B, 2004).

The authors considered the dimensions of Information Security as a baseline when defining dimensions for DF. From the literature studied, the following dimensions were identified for digital forensics: Corporate Governance – strategic and operational, Policy, Legal and Ethical, People and Technology. The authors want to propose DF as a multi-dimensional discipline.

Although the authors identified different dimensions, we propose that the dimensions are interrelated and should not exist in isolation for a total DF solution. In the next part of the paper the authors provide a short discussion and outline of the various dimensions.

4.1 Corporate Governance dimension

The Corporate Governance dimension will handle the management aspects of DF in an organization. Management is responsible for the security posture of an organization. Various reports on Corporate Governance e.g. King II and Sarbarnes- Oxley have clearly outlined the fact. According to Thomas Hoffman (2004) – ‘Most companies working on Sarbanes-Oxley projects are focused on documenting their internal controls to meet the compliance deadlines that start taking effect late this year. But the law's requirements are generating interest in using computer forensics tools to help identify potential cases of financial fraud’.

Management can only manage security incidents if for example the root cause of the event is determined and appropriate action to rectify it can be taken – this may involve forensic investigations.

According to Von Solms and Louwrens (2005a), IT Governance is a subset of Corporate Governance and Information Security Governance a subset of IT Governance. DF overlaps with Information Security Governance, IT governance and Corporate Governance (Von Solms & Louwrens, 2005a). Forensic readiness will help to demonstrate due diligence and good corporate governance of an organization’s assets (Rawlingson, 2004). It is therefore important that a forensic

investigation must be performed in a way that it adds value and improves the security posture of an organization.

The Corporate Governance dimension includes strategic governance and operational governance. Typically strategic governance will be from a strategic perspective, while operational governance will provide management directives on an operational level. It is vital that management should become involved and buy into the DFMM of the organization. DF investigations can be very expensive and management must realize the need for investigations, as well as dealing with the results from an investigation.

The operational governance dimension should guide the management on how to manage digital forensic investigations by providing a DFMM. This DFMM must include reactive DF as well as pro-active DF management.

Organizations tend to handle security incidents internally and patch up holes in their security posture. This statement is supported by the CSI/ FBI 2004 survey that 70% of the respondents are patching up the holes of the breach and only 20% of respondent have reported the incidents to law enforcement agencies (Gordon, 2004).

Pro-active DF management must ensure that all business processes are structured in such a way that essential data and evidence will be retained to ensure successful DF investigations, should an incident occur. Proper pro-active DF management should minimise interruption to the business processes while conducting an investigation. It is essential that the organization become DF ready. Re-active DF management should clearly define the management or process of an investigation, once an incident has occurred.

4.2 Policy dimension

Every organization needs policies to guide employees on activities. A general forensic investigation policy is required to provide a framework for DF policies in the organisation. Examples of other policies are how to handle evidence, how to seize evidence and how to conduct covert or overt investigations. Policies are normally supported by procedures and guidelines. Procedures also need to be set up so that the investigations will be able to stand up to legal scrutiny in court. These procedures must also be scientifically sound and proven to maintain the integrity of the evidence and process.

Yasinsac and Manzano (in Rawlingson, 2004) note that enterprise policies can enhance computer and network forensics. They propose six categories of policies to facilitate Digital Forensic Investigations (DFI):

- Retaining Information;
- Planning the Response;
- Training;
- Accelerating the Investigation;
- Preventing Anonymous Activities;
- Protecting the Evidence. (Louwrens et al., 2006)

Well-defined policies give digital investigations and forensic examiners the authority to conduct investigations in the organization. Policies will demonstrate that an organization intends to be fair-minded and objective about how it treats employees and that it will follow due process for all investigations (Nelson B, Phillips A, Enfinger F, Steuart C, 2005, p 15).

4.3 Legal and Ethical dimension

The Legal and Ethical dimension of DF is very important in organizations. In Cyberspace there is no universal or common 'Cyber law'. Various judiciary systems exist in different countries. The forensic investigator must be familiar with local legal and international laws, treaty requirements and industry specific legal requirements when preparing to present a case that will be able to stand up to legal scrutiny in court. The impact of for example the Electronic Communications Act, Electronic Communication and Transaction Act (ECT), Interception of Information Act will be investigated and included in this dimension in the South African context. An example is the specific legal requirements for electronic and digital evidence in the ECT Act.

The ethical aspect of DF is becoming more and more important. Although the Legal and Ethical aspects of DF have been placed together in the same dimension, it is essential to note that not all legal operations or actions are ethical. It is essential that the DF investigator does not misuse the trust that the employees place in him / her. DF investigator utilises tools that, if handled inappropriately, can cause a lot of damage in an organization. There should be very clear guidelines on ethical behaviour and possibly a code of conduct for DF Investigators to guide professional behaviour (Nelson B, Phillips A, Enfinger F, Steuart C, 2005, p 20).

4.4 People dimension

People are the most important part of any organisation and normally the weakest link in the security chain of the organization. When an incident occurs it is most likely that people will contaminate the evidence while figuring out what has happened. Training is therefore essential. According to Rawlingson (2004) there is a huge need for forensic awareness training. This dimension will look at training and awareness programs in an organization.

The profile and composition of a DF team is also very important. One person normally does not have all the required skills to conduct an investigation. Stephenson (2003) has suggested that the team should consist of a team leader, network specialist, code specialist, business process specialist and a quality manager.

The team leader is a person who specializes in the investigative process, forensics, data analysis and investigation management. Currently the team leader reports to various units in organizations, e.g. CEO, Chief Risk Officer and Financial Manager. The team leader should not report to the Chief Security Officer as segregation of duties needs to take place.

The network specialists are typically people who specialize in TCP/IP for Microsoft and other operating systems by having thorough knowledge of firewalls and intrusion detection software.

Code specialists analyse rogue code involved in the incident specialise in an operating system and its behaviour. The business process specialist is typically a person who specialises in a standard e.g. ISO17799 and /or industry regulations e.g. banking industry. They should uncover process failures and calculate the cost of the incident to the organization.

Finally, the quality manager must ensure that the chain of evidence and custody is managed and maintained. All records of the investigation need to be secured.

Organizations seldom have people with all the above-mentioned skills available, therefore the industry trend is to outsource all investigations to an outside party (Stephenson, 2003).

4.5 Technology dimension

No DF investigation can be conducted without a DF toolkit. Various specialised software and / or physical hardware tools will make up the DF toolkit as different tools are used for different

purposes. The way the tools are utilised as well as the acceptance of a specific tool by the legal authorities are vital for any forensic investigation.

Although courts have found that an inanimate object, e.g. a software package cannot be considered to be an expert, the results generated by an acceptable software package are acceptable. The person who will use the software packages will have to be an expert. The forensic and legal community has accepted certain industry standard tools e.g. EnCase (Meyers M, Rogers M, 2004).

4.6 Putting it all together.

All 5 dimensions must exist for a total solution. The dimensions cannot exist independently but are related to the other dimensions for example: the Corporate Governance dimension will interact with all the other dimensions for example: Management will provide direction on the *Policies* and procedures that will be required by the organization, T*raining* and recruitment of quality staff and general forensic awareness training programs in the organization as well as typical L*egal and ethical* requirements. The *tools / Technology* that will be utilised by the investigator will be managed on an operational level.

It is essential to use all possible resources to gather evidence. The forensic investigator will consider the following resources: hardware / physical equipment, people, networks, systems (applications and system software), information (digital and physical) and also the physical environment within each dimension.

The main source of evidence for an investigation will be the information stored on the physical hardware, and information obtainable from operating system logs. Every dimension can contain or interact with different resources.

All the above-mentioned resources must be considered in each dimension when conducting a DF investigation or creation of DF readiness. In the Legal dimension for example, software licensing, acceptance of digital evidence in court, seizure of evidence (physical / hardware and digital), human behaviour must be incorporated. Not all the resources may exist, but all resources must be considered during an investigation. Further research is required to provide more detail regarding the resources in each dimension.

The investigator will use processes and tools to deal with DF in the organization. The various dimensions will employ one or both for a successful DF investigation or the creation of DF readiness. The governance dimension will, for example, be implemented by using processes as well as tools to document the entire investigation. The people, legal and ethical dimensions may utilize only processes and the technology dimension would be processes as well as tools.

The forensic investigation manager should consider all dimensions of DF to implement DF awareness, readiness as well as conducting a DF investigation in an organization

In the next part of the paper the authors will map out the dimensions to the Digital Forensics framework as proposed by Louwrens et al. (2006) to provide more detail to the dimensions.

5 DIMENSIONS MAPPED TO DF CONTROL FRAMEWORK

Louwrens et al (2006) has proposed a Digital Forensics Reference Framework. The framework propose 5 High-level Digital Forensics Control Objectives (HDFCO):

- Digital Forensic Readiness
- Evidence Preservation
- Forensic Acquisition
- Forensic Analysis

- Evidence Presentation

These 5 Digital Forensic Control Groupings were then refined into 22 Digital Forensics Control Objectives (DF-COs) and these 22 DF-COs were again refined into 66 Digital Forensics Detailed Control Objectives (DF-DCOs).

The authors mapped the DF-CO and DF-DCO's to the proposed dimensions. The mapping may not be complete and further research will be conducted. The purpose of the mapping is to provide a reference framework for each dimension.

5.1 Digital Forensic Readiness (DFR) – Group 1

(4 DF-COs with 21 DF-DCOs)

		Dimension					
DF Control Objective	**Description**	**Policy**	**People**	**Technical**	**Governance**	**Legal Ethical**	
DFR1	**Planning Information Retention Requirements**	**X**		**X**	**X**	**X**	
DFR1.1	Define the business scenarios that require digital evidence;				X		
DFR1.2	Identify available sources and different types of potential evidence;			X			
DFR1.3	Determine the evidence collection requirement;			X		X	
DFR1.4	Establish a policy for secure storage and handling of potential evidence;	X				X	
DFR1.5	Establish a capability for securely gathering legally admissible evidence to meet the requirement;					X	
DFR1.6	Time synchronization of all relevant devices and systems;			X			
DFR1.7	Systematic gathering of potential evidence;	X		X			
DFR1.8	Preventing Anonymous Activities.	X		X			
DFR2	**Planning the Response**	**X**	**X**	**X**	**X**		
DFR2.1	Ensure monitoring is targeted to detect and deter major incidents;	X			X		
DFR2.2	Implement Intrusion Detection Systems (IDS);	X		X	X		
DFR2.3	Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;				X		
DFR2.4	Establish a Computer Emergency Response Team (CERT);		X		X		
DFR2.5	Establish capabilities and response times for external Digital Forensic Investigation (DFI) professionals.		X		X		
DFR3	**Digital Forensic Training**		**X**				
DFR3.1	Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;		X				
DFR3.2	Develop an in-house DFI capability, if required;		X				
DFR3.3	Enhance capability for evidence retrieval.		X				
DFR4	**Accelerating the Digital Forensic Investigation**	**X**		**X**	**X**	**X**	
DFR4.1	Document and validate a DFI protocol against best-practice;	X			X		
DFR4.2	Acquire appropriate DF tools and systems;			X			
DFR4.3	Ensure legal review to facilitate action in response to the incident;					X	
DFR4.4	Clear definition of responsibilities and authority for the CERT and DFI teams;				X		
DFR4.5	Define circumstances when to engage professional DFI services should the need arise.				X		

5.2 Evidence Preservation (EPV) – Group II

(4 DF-COs with 13 DF-DCOs)

		Dimension					
DF Control Objective	**Description**	**Policy**	**People**	**Technical**	**Governance**	**Legal Ethical**	
EPV1	**Incident Response**	**X**			**X**		
EPV1.1	Initiate Incident Response plan	X			X		
EPV1.2	Activate the CERT	X			X		
EPV2	**Secure Evidence**	**X**		**X**		**X**	
EPV2.1	Secure the physical environment of the crime scene	X				X	
EPV2.2	Secure all relevant Logs and Data	X		X			
EPV2.3	Secure Volatile evidence, including Laptops	X		X			
EPV2.4	Secure Hardware	X		X			
EPV2.5	Label and seal all exhibits	X				X	
EPV2.6	Preserve chain of evidence	X				X	
EPV3	**Transport Evidence**	**X**				**X**	
EPV3.1	Securely transport evidence	X				X	
EPV3.2	Preserve chain of custody in transport	X				X	
EPV4	**Store evidence**	**X**				**X**	
EPV4.1	Store evidence in safe custody room	X				X	
EPV4.2	Control access to evidence	X				X	
EPV4.3	Preserve chain of custody in storage	X				X	

5.3 Forensic Acquisition (FACQ) – Group III

(5 DF-COs with 8 DF-DCOs)

		Dimension					
DF Control Objective	**Description**	**Policy**	**People**	**Technical**	**Governance**	**Legal Ethical**	
FACQ1	**Ensure Integrity of evidence**	**X**		**X**		**X**	
FACQ1.1	Follow established Digital Forensic Investigation protocol	X				X	
FACQ1.2	Write-protect all evidence source media			X			
FACQ2	**Acquire evidence**	**X**		**X**			
FACQ2.1	Acquire evidence in order of volatility			X			
FACQ2.2	Acquire non-volatile evidence			X			
FACQ3	**Copy Evidence**	**X**		**X**			
FACQ3.1	Make forensic copies of all evidence			X			
FACQ4	**Authenticate evidence**	**X**		**X**			
FACQ4.1	Authenticate all evidence to be identical to original			X			
FACQ4.2	Time stamp all copies of the authenticated evidence			X			

FACQ5	Document Acquisition process	X					
FACQ5.1	Document all actions through Chain of Custody documentation	X					

5.4 Forensic Analysis (FAN) – Group IV

(6 DF-COs with 14 DF-DCOs)

		Dimension					
DF Control Objective	**Description**	**Policy**	**People**	**Technical**	**Governance**	**Legal Ethical**	
FAN1	**Plan Investigation**	**X**		**X**	**X**		
FAN1.1	Review all available information regarding the incident			X	X		
FAN1.2	Identify expertise required				X		
FAN1.3	Identify most suitable DF tools to be utilized			X	X		
FAN2	**Develop Hypothesis**						
FAN2.1	Develop hypothesis to cover most likely scenarios				?		
FAN2.2	Define criteria to prove / disprove hypothesis				?		
FAN3	**Acquire the evidence**	**X**		**X**			
FAN3.1	Acquire the evidence by means of the most suitable DF tool available			X			
FAN3.2	Analyze evidence by means of the most suitable DF tool available			X			
FAN3.3	Conform to the requirements of the "Best evidence rule"	X		X			
FAN4	**Test Hypothesis**			**X**	**X**		
FAN4.1	Reconstruct sequence of events			X	X		
FAN4.2	Compare evidence with other known facts			X	X		
FAN5	**Make finding**	**X**		**X**	**X**		
FAN5.1	Make a finding that is consistent with all the evidence			X	X		
FAN5.2	Document finding	X		X			
FAN6	**Document the case**	**X**			**X**		
FAN6.1	Document all aspects of the case	X					
FAN6.2	Enter documentation into safe custody	X			X		

5.5 Evidence Presentation (EP) – Group V

(3 DF-COs with 10 DF-DCOs)

		Dimension					
DF Control Objective	**Description**	**Policy**	**People**	**Technical**	**Governance**	**Legal Ethical**	
EP1	**Prepare case**	**X**	**X**	**X**	**X**		
EP1.1	Determine target audience (Court, Disciplinary hearing, Incident inquiry)				X		
EP1.2	Assemble all evidence required for presentation	X		X			

EP1.3	Prepare expert witnesses	X	X				
EP1.4	Prepare exhibits	X		X			
EP1.5	Prepare presentation aids like graphics, slides, hardware	X		X			
EP1.6	Preserve chain of custody	X			X		
EP2	**Present case**		**X**		**X**	**X**	
EP2.1	Present evidence in a logical, understandable way to ensure that the court can critically assess every bit of information and understand the relevance to the case at hand.				?	X	
EP2.2	If needed, make use of graphics and/or physical examples to illustrate difficult or critical concepts				?		
EP2.3	Ensure that a Digital Forensic specialist is at hand to assist in providing expert evidence.				X		
EP3	**Preserve evidence**	**X**					
EP3.1	Preserve the evidence after the case has been presented, as it may be needed again in case of appeal, or where new evidence becomes known.	X					

The authors had a difficulty to map the control objectives: FAN2 and EP2 to the current dimensions. Further research will be done to determine if another dimension e.g. Process should be included or if the above-mentioned control objectives should be included in the Corporate Governance dimension. The authors intend to use the above-mentioned mapping of the control objectives to the dimensions to define an integrated DFMM.

6 SUMMARY

The paper has defined DF as a multi-dimensional discipline. The following dimensions have been identified by the authors: Corporate Governance, Policy, People, Legal & Ethical and Technology. The dimensions are inter-related and can not exist in isolation.

To conduct a successful investigation or establish a forensic readiness culture in an organization, the following resources should be considered for each dimension: Hardware, Information, Systems, People, Networks and the Physical Environment. DF will be implemented by using processes and / or utilizing tools within each dimension.

DF must become a priority in organisations as management is responsible and accountable for all activities in an organisation. There should be an integrated management model to guide management on the investigation process should a security breach occur, as well as to create digital forensic awareness in the organization.

Further research will be done to investigate a possible additional dimension for DF and to develop an integrated management model for DF.

7 REFERENCES

AMERICAN HERITAGE DICTIONARY (4th edition). (2000). New York, NY: Houghton Mifflin.

BEEBE NL, CLARK JG, (2004), *A hierarchical, objective-based framework for the digital investigation process*, Digital forensic research workshop, Baltimore, Maryland, www.dfrws.org. (24/4/2006).

CULLERY A, (2003), *Computer forensics: past present and future, Information Security Technical report,* vol 8 nr 2, p32-35, Elsevier.

DIGITAL FORENSIC RESEACH WORKSHOP, (2001), *A roadmap for Digital Forensics Research.* www.dfrws.org. (DATE)

GORDON LA, LOB M, etc. (2004). *CSI/FBI Computer Crime and security survey.*

GROBLER CP, VON SOLMS SH, (2004), A Model to assess the Information Security status of an organization with special reference to the Policy Dimension , Master's dissertation.

HOFFMAN T, (2004) *Sarbanes-Oxley Sparks Forensics Apps Interest,* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=91676, MARCH 29, 2004

KING II REPORT ON CORPORATE GOVERNANCE. (2000). Website: http://iodsa.co.za/lod%20Draft%20King%20Report.pdf, August 2003.

KRUSE II WARREN G.,JAY G HEISER. (2004). *Computer forensics incident response essentials*. Addison Wesley, Pearson Education.

LOUWRENS B, VON SOLMS SH, REECKIE C, GROBLER T, 2006, *A control framework for Digital Forensics,* proceedings IFIP W11.9.

MEYERS M, ROGERS M. (2004). *Computer forensics: The need for standardization and Certification.* International Journal of Digital Evidence, Fall 2004, Volume 3, Issue 2.

NELSON B, PHILLIPS A, ENFINGER F, STEUART C (2005), Guide to computer forensics and investigations 2nd edition, Thompson publishing.

RAWLINGSON R. (2004). *A ten step process for forensic readiness,* International Journal of Digital Evidence ,Winter 2004, Volume 2 Issue 3.

REITH M, VARR V, GUNCH G. (2002).*An examination of Digital Forensic Models*. International Journal of Digital Evidence Volume 1, Issue 3, http://www.ijde.org/docs/02 art2.pdf, (15/02/2005).

SABS ISO/IEC17799. (2001). SABS edition 11/ISO/IEC edition1, South African Standard, Code of practice for Information Security Management. South African Bureau of Standards.

SHELDON A, (2004), Forensic Auditing, *The role of computer forensics in the corporate toolbox.* http://www.itsecurity.com/papers/p11.htm (25/3/2004)

SINANGIN D, (2002), *Computer forensics investigations in a corporate environment*, Computer Fraud and Security Bulletin, 8, p.11-14, June 2002, Elsevier.

STEPHENSON P. (2003). *Conducting Incident Post Mortems*, Computer Fraud and Security, April 2003, Elsevier.

STEPHENSON P. *Applying Forensic Techniques to Information System Risk Management – First steps*. Computer Fraud and Security (17), Elsevier.

STEPHENSON P. *End to end Digital Forensics*. Computer Fraud and Security (17), Elsevier.

Von Solms SH, Louwrens CP (2005a). *Relationship between Digital Forensics, corporate Governance, Information Technology and Information Security Governance*, Information Security of South Africa Conference 2005 proceeding.

VON SOLMS SH. (2001a). *Information Security. A multi-dimensional discipline*, Computers and Security, volume 19, number 7. Elsevier.

VON SOLMS SH. (2001b). *Corporate Governance and Information Security*. Computers and Security Volume 20, number 3. Elsevier.

WHITMAN M, MATFORD H. (2003). Principles of Information Security. Thompson Publishing.

WOLFE HB, (2003), *Computer Forensics*, Computer Security, 22, p 26-28.