International Journal of Academic in Engineering Trends & Multidisciplinary Advance Study
Volume 3, Issue 4, 05–15.
http://www.ijaetmas.org/

Review on Digital Forensic Framework and Its Applicability in Organization

Adamu Abdullahi Garba*[1], Ibrahim Bukar Dauda[2], Ya'u Nuhu[3]
[1,2]*Department of Computer Science, Yobe State University Damaturu, Nigeria,BSc, MSc*
[3]*Department of Computer Science, the Federal Polytechnic Damaturu, Nigeria, BSc*

ABSTRACT:*The advance of the internet has made many business organizations conduct their operation automatically, this new way of doing business has also opened potentially harmful unforeseen information security incidents of both illegal and civil nature, with the potential to cause harm to the organization's business. Therefore, if an organization does not prepare itself for such incidents, it's likely that important relevant digital evidence will be damage. An organization not being able to respond effectively to an incident could affect the business. Forensic readiness is the capacity of an organization to exploit its prospective to use digital evidence whilst minimizing the cost of investigation subsequently, to prepare organizations for incident responses, the implementation of digital forensic readiness policies and procedures is important. In this research paper, the aims are to determine the concept of Digital forensic readiness (DRF) and how its strength and limitation would guide the organization to adopt the suitable framework for their organization. The review of the recent framework was achieved and its applicability was explained as well.*
Keywords:*Digital Forensics, Framework, Forensic Policy, Models*

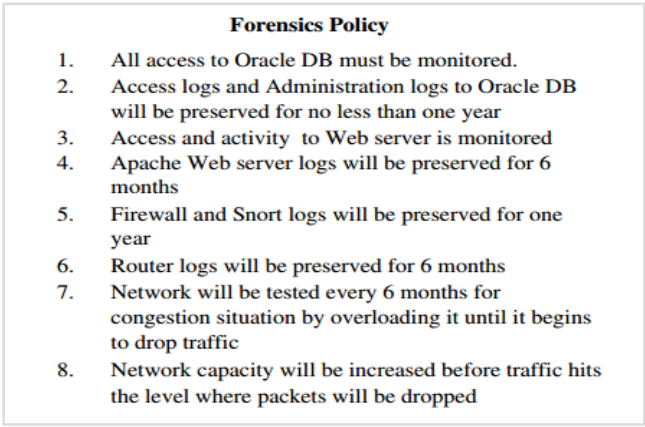
INTRODUCTION

There are many definitions given to digital forensic from various researchers and books, According to the Oxford dictionary, forensic can be defined as linking to the usage of systematic approaches to the investigation of crime and of or relating to courts of law. The practice of science and expertise to examine and institute facts in an illegal or civil court of law can be referring to as forensic (Farlex, 2014).Digital forensics (DF) is the systematic proposition of the procedures involved in the recapture, safeguarding, and investigation of digital evidence, including audio, imaging, and communication devices (TC-11, 2006). DF is the division of computer science that emphasizes evolving evidence related to the digital world for use in civil or criminal court proceedings (Reith, 2002). DF evidence can also be found in digital documents, emails, digital photographs, software programs, or other digital archives and network metadata, which may be the question in a legal circumstance to win a case (Marangos, 2012).Most organizations oversee the basic requirement of digitalforensic, lack of concrete evidence to verify the authenticity of fraudulent transaction that will link to the invader(Adamu and Aliyu, 2019) .Digital forensic is the accomplishment of a suitable level of competence by an organization for it to accumulate, preserve, shield, and analyze any digital evidence so that the evidence can be excellently used in any courts of law, in corrective matters. In another context, some authors have recognized three modules in digital forensic: Proactive, Active, and Reactive DF. These modules are linked to one another. Proactive means before an incident alert, actively refer to real-time happening and reactive refers to afterward an incident (Grobler*et al.*, 2012). Proactive DF is for the preparation of organizations for investigations; Active DF refers to consideration, the procurement, and exploration of live evidence; and Reactive DF is the real 'post-action forensic investigation. Nowadays many organizations only invest in reactive DF rather than all the components. Even with the advancement of alertness and educational research on proactive forensic, its description and enactment are still not reliable in the digital forensic domain (Frincke*et al.*, 2006).

This research paper aim is to review the current digital forensic readiness framework/model and explain its components, strength, and limitation. This would guide new organizations that are looking for which framework to adopt and be implemented in their organization

DIGITAL FORENSIC POLICY

The policy is a strategy that explicitly specifies what is allowed and what is disallowed with regards to security (Taylor *et al.*, 2007). The organization must ensure that written policies contain a clear statement that almost addresses all major forensic considerations, it includes communicating law enforcement, observation, and also performing assessments of forensic strategies and procedures.Correct policies at a high level allow only authorized persons to monitor the system and network and perform investigations for an only legitimate reasons. According to Taylor *et al.*, (2007) Digital forensic focuses on capturing evidence in a way the forensic veracity of the seized data is well-kept for legitimate reasons. Organizations may also have another different policy for the incident handler and other forensic roles: this policy would provide a more comprehensive rule for applicable behavior, however, all policies should be updated frequently, especially for an organization that spans many jurisdictions, because of changes of law enforcement and regulations. The digital forensic policy should always be consistent with the other policies within the same organization. Figure 1 shows an example of forensic policies for a corporate organization.



Forensics Policy

1. All access to Oracle DB must be monitored.
2. Access logs and Administration logs to Oracle DB will be preserved for no less than one year
3. Access and activity to Web server is monitored
4. Apache Web server logs will be preserved for 6 months
5. Firewall and Snort logs will be preserved for one year
6. Router logs will be preserved for 6 months
7. Network will be tested every 6 months for congestion situation by overloading it until it begins to drop traffic
8. Network capacity will be increased before traffic hits the level where packets will be dropped

Figure 1: Forensic Policies for a Corporate IT System (Barbara *et al.*, 2007)

DIGITAL FORENSIC POLICY BY NIST

NIST (2006) provided a guideline to be considered when implementing forensic policy in any organization, in the Guide "To Incorporating Forensic Techniques into Incident Response paper". This policy stated that for an incident to be handled effectively and efficiently, forensic consideration must be fused into the information system life cycle, such concerns include:

- Carrying out routine backups of the system and preserving previous backups for a long duration.
- Supporting auditing on workplaces, servers, and system peripheries
- Dispatching audit records to a more protected centralized log server
- Designing mission life-threatening system application to implement auditing
- Maintaining records of network and system configuration.
- Establishing policies that will support data retention and performing historical reviews of system and network activities and destroying data that is no longer needed.

These considerations are just extensions of the existing provision in the organization's policies and procedures so that they are specified within the relevant individual documents instead of a centralized forensic policy.

STATEMENTOFTHE PROBLEM

The Computer Crime and Security Surveys confirm that cybercrime is real and also remains to be a significant problem, andcause financial damage, less percentage of loss reported by law enforcement was 16% in 1996 and 25% in 2006. Furthermore, in 2006 total losses reported were $52,494,290 for 313 respondents and the average annual loss more than doubled from $168, 00 in 2006 to $350,424 in 2007. This survey shows that cybercrime cases always increase as the years go by. Today, as we all know a small proportion of commercial incidents were told to the law enforcement authorities. This happens because of many reasons, which include negative publicity, believed law enforcement could not help, challengers would use to their advantage, the civil remedy sought, unaware of law enforcement interest, etc.Other reasons include fear of reputational damage, loss of customers, and also fear of exposing organizational security vulnerabilities, lack of confidence in the ability of law enforcement agencies, fear of encouraging other fraudsters, and ignorance.The Consumer Sentinel Network (CSN) holds almost over 9 million complaints dating from 2009 across the calendar year 2013; also over 13 million do-not-call complaints from the same year. Only between January and December 2013, it has almost received customer complaints of over 2 million with 55% fraud complaints, 14% identity theft, and 13% other types of complaints. Based on the reports identity theft was number one with 14% complaints, and then followed by Debt collection with 13%, Banks and Lenders with 7%, Imposter Scam and Telephone and Mobile Service with 6% (FTC, 2014) as shown in Figure 2 below

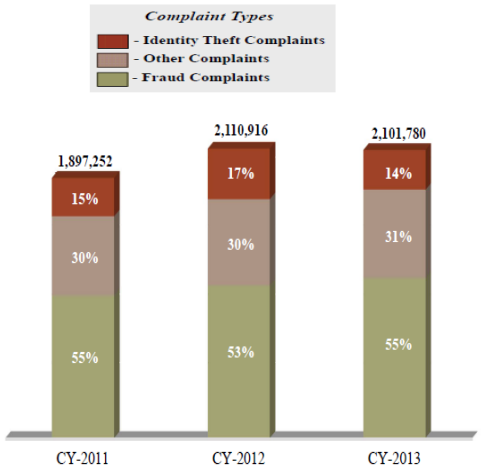


Figure 2: Complaint Type (FTC, 2014)

Based on the complaint type: identity theft, fraud, and others across 3years starting from 2011 to 2013 show fraud has 55% in 2011 and decrease by 2% in 2012 and then rise to 55% again in 2013, while other complaints in 2011and 2012 keep the same 30% and then increase by 1% in 2013. Identity theft also increases exponentially from 15% in 2011, 17% in 2012, and then decreases to 14% in 2013. From above Figure 3, it shows that fraud has the highest percentage compared to the remaining two complaints and the least among them is identity theft based on the complaints made by the customers.

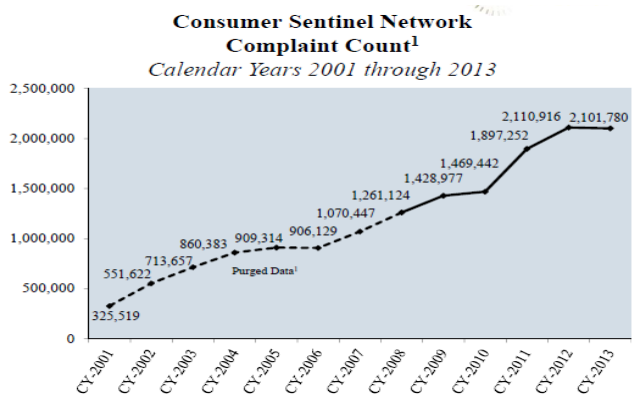


Figure 3: Customer Compliant Based on Calendar (FTC, 2014)

The above Figure 3 shows along complaints made since 2001 to 2013 by customers, it also shows the numbers of complaints for each year, which rise drastically. It's started from 325,519 compliance in 2001 to almost 2,101,780 in 2013, but from 2001 to 2008 the data were purged while for the rest of the year isn't purged at all. From this section, we can conclude that as the years goes by complaints always increase.Moreover, According to the Federal trade commission (FTC, 2014), the overall findings of the problems released by CSN are from the complaints types both frauds and other has been increasing while identity theft the last recorded was less than the previous one i.e. 2013 and 2012. Finally, the total compliance is 2,101,780. This survey shows that adequate measures were not taken properly to overcome customers compliances which in time will result in customer loss of trust from the companies or organization. Digital Forensic ReadinessForensic Readiness is the reaching of a suitable level of competence by an organization to assemble, preserve, safeguard and analyze digital information so that it can be effectively used in any authorized matters. Rowlingson (2004) defines forensic readiness as the capacity of an organization to exploit its prospective to use digital evidence whilst minimizing the cost of the investigation. Digital forensic is a division of science surrounding the retrieval and investigation of data found in digital devices often in connection to, but also not partial to computer crime (Micheal *et al.*, 2006).In forensic readiness discipline, incident preparedness has become an important goal of an organization and consists of those actions that can be either technical or non-technical, that exploit an organizations' ability to use digital information. Forensic readiness is event anticipation for incident response, it supports the business requirement to use digital information.

DIGITAL FORENSIC READINESS POLICY

The development incorporation and implementation of pro-active forensic ethics, comprising the creation of an organization policy be will ponder as a preventive side of security. As explained before forensic readiness focuses on the collection of admissible digital evidence by reducing the cost of investigation and also minimize time to track attackers so that the evidence can be used in the court of law for hearings. Many authors like Rowlingson (2004) stated that not only forensic readiness from a practical point of view but also provide some specific weight to procedures and processes stressing the need for organizational readiness. He further goes on to recommend a ten-step framework in implementing forensic readiness: the application of these steps forms the foundation of forensic readiness policy and it also includes: risks valuation, documentation of target and evidence, legal capabilities, archives, and observing policies, staff awareness, and regal reviews.According to Taylor *et al.,* (2007) they indicated the lack of suitable theory for creating Forensic readiness precondition (FRP) and propose a method for creating such policy based on computer security policy requirements. Their processes are data and event-based, specifying the data and event that will worsen to a full formal investigation. The FRP preconditions are risk assessment, digital assists and data identification, "forensic-ready" data identification, and forensic readiness policy management. The objective specified by Tan (2001) and Rowlingson (2004) consists of price reduction and digital evidence usage expansion. Henceforth, the preparation and defense of such policy will be based on mechanisms that satisfy both of those objectives. By a combination of passed ideas and inclusion of mathematical validation of digital evidence, they proposed several modules that the preparation of forensic readiness policy should consider. Digital evidence documentation

Classifying digital evidence exposure and correlating it with threats based on risk assessment
Digital evidence access control and preservation of chain of custody (Ray, 2007).
Calculation of the link between cost and benefit each factor of digital evidence by using statistical representation
Evidence management plan development (Grobler *et al.*, 2010)
Digital forensic investigation model choice – the technique to be obeyed after an event occurs (Pollitt, 2007)
Technical structure standard (Mandia*et al.,* 2003)
Staff training providers on policy's content
Taylor *et al.*, (2007) Stated that the methods below will help in forensic readiness request in uncovering forensic policy:
Classify digital assets that have values
Implement risk evaluation of likely loss and threats to the identified assets
Eradicate the assets that do not guarantee the effort of hearings
defined associated data required for those assets along with gathering and preservation needs
Compose the forensic policies in terms of digital assets, forensic events, data collection, and archiving.
Sufficient forensic policy enforcement is in place.

Even with the emerging development of pro-active forensic standards across my private organization sector, the Payment Card Industry (PCI) is the only one formally being implemented; therefore, all organizations fulfilling with the PCI and Data Security Standard (DSS) standard must have proactive methods in place (Antonis*et al.*, 2011). I believed in the coming future, it will be a precondition for any organization to have a digital forensic readiness policy because from indication it shows some organizations have started to implement it, then it will be eventually become a competition.

OBJECTIVES OF THE STUDY

General Objective

The study will be guided by a specific objectives.
To Review on Digital Forensic Framework and Its Applicability in Organization

LITERATURE REVIEW

In this section, the research paper has provided the recent digital forensic framework/models and has explained in detail their components found in the literature.

Digital Forensic Readiness Framework for South Africa SME's

According to Stander *et al.*, (2010) they resented a visual representation that managers should monitor to assist the execution of digital forensic readiness to their organization. This framework consists of five major components, which include: strategy, policy, and procedures, technology, digital forensic response, compliance, and monitoring as shown in Figure 4.

Figure 4: Components of Digital Forensic Readiness Framework (Stander *et al.*, 2010)

Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems

According to Valijarevec and Venter (2011), the stated that system should have the following components: scenario, source, pre-incident collection, pre-incident analysis, incident detection, post-incident collection, post-incident analysis, architecture defining, implementation, and assessment as shown in Figure 5.

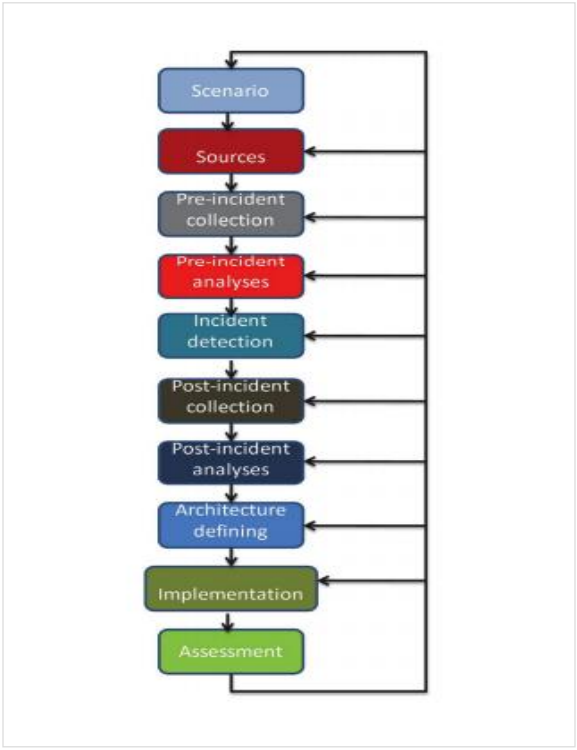


Figure 5 Digital Forensic Readiness Model for PKI Systems (Valijarevec and Venter, 2011)

A Conceptual Model for Digital Forensic Readiness

According to Antonio and Labuschagne (2012), they stated that the most basic components of digital forensic readiness should consist of the following elements: people, process, policy, and technology, in this DFR the elements has sub-activities that can be classified into proactive and reactive as shown in Figure 6.

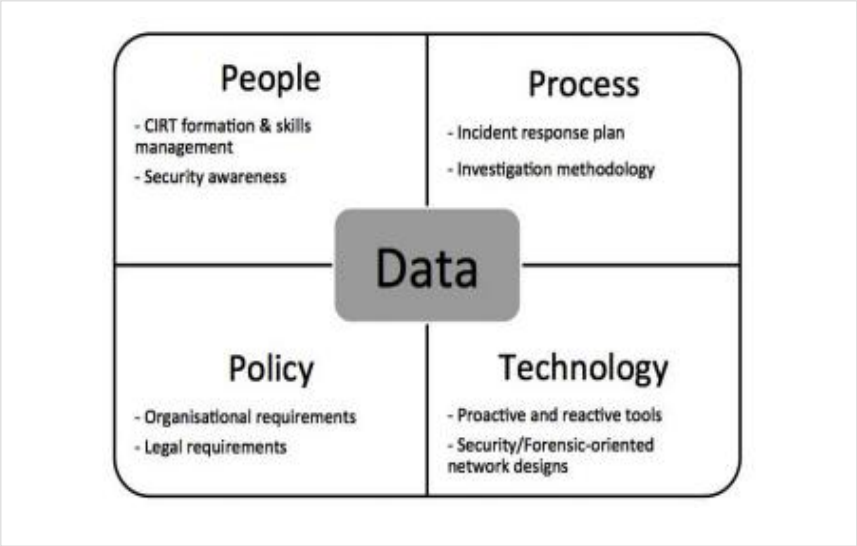


Figure 6 Digital Forensic Conceptual Model (Antonio and Labuschagne, 2012)

A Theoretical Framework for Organizational Network Forensic Readiness

According to Taylor *et al.,* (2007) they stated that the Information Assurance (IA) as a whole has network digital forensic readiness components such as security policy, practice, mechanisms, procedures, and security awareness training programs. This is expressed in stabilizing the method to sue malicious cyber invasion magnificently while decreasing the current effort used on digital forensic investigation. Figure 7 shows the components of the organizational network forensic readiness.

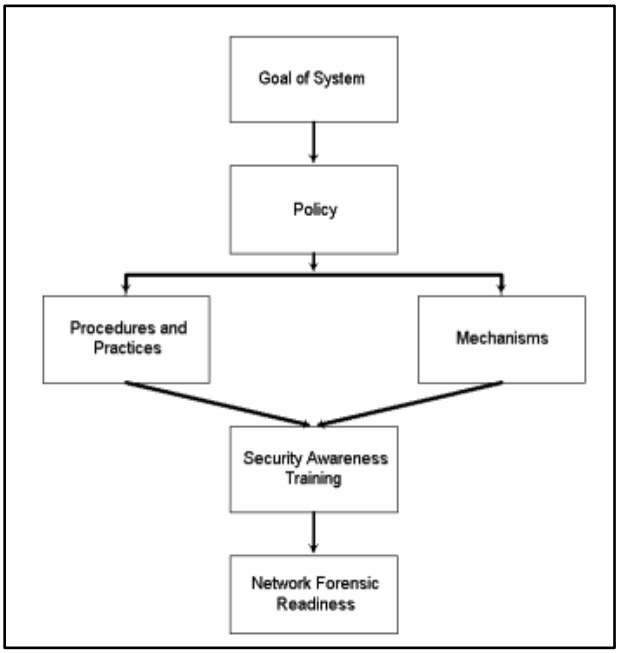


Figure 7Network Forensic Readiness Frameworks (Taylor *et al.,* 2007)

The Continues Forensic Readiness Framework

Jeroen de Wilt (2013) proposed a framework consists of four building components; these components are management, stakeholders, internal control, and plan-do-check-act. The management level consists of strategic, tactical, and operational while the internal control consists of people, processes, and technology. The plan-do-check-act cycle is plan objectives and processes necessary to deliver the expected output, while do phase is used to implement the data collected from the next phase and the check phase is used to validate the results collected and compared it with the expected results and lastly, the Act phase is used to correct any error encountered during the process. Figure 7 shows the framework and how it is organized.

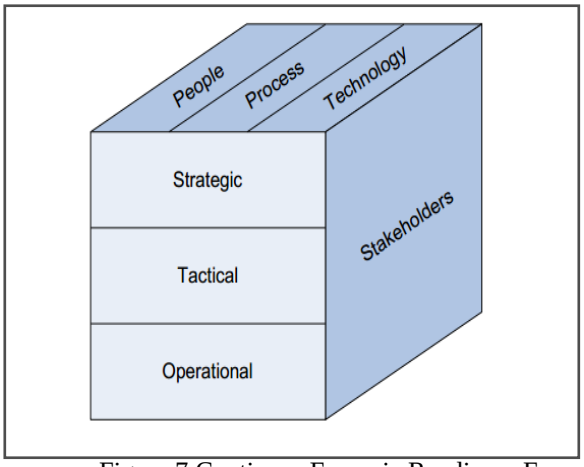


Figure 7 Continues Forensic Readiness Framework (Jeroen de Wilt, 2013)

Digital Forensic Readiness Commonalities Framework (DFRCF)

Whyte and Claims (2012) show the major domain of their framework and their relationships. From the diagram, the arrows specify steps that guide the development and execution of DFR in the organization. The framework consists of seven components which are: strategy, methodology, system and event, policy and compliance, training, monitor and report, and lastly legal involvement as shown in Figure 8.

Figure 8 Digital Forensic Readiness Commonalities Framework (Whyte and Claims, 2012)

Extended Digital Forensic Readiness Components Framework

Ivan Claims (2013) proposed an extended digital forensic readiness components framework with domains and sub-domain, per-participant input, this was proposed after careful study of the previous digital forensic readiness components framework proposed by (Whyte and Claims, 2012). This framework has eight components which strategy, legal requirement, governance, system and event, policy, compliance, training, and monitor and report as shown in Figure 9

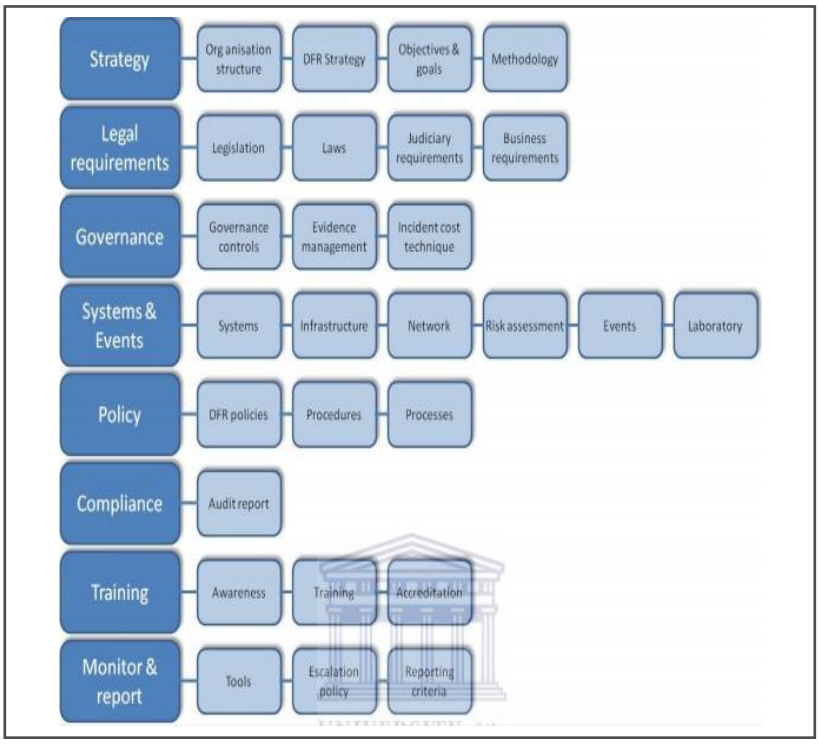


Figure 9 Extended Digital Forensic Readiness Components Framework (Ivan Claims, 2013)

Digital Forensic Readiness Framework Components

Dimotikalis *et al.*, (2013) proposed a digital forensic framework based around fix axes: these axes symbolize the initial approach to define forensic readiness framework. These components are: digital evidence management, risk assessment, incident response process, staff training, policy writing, and legal review as shown in Figure 10.

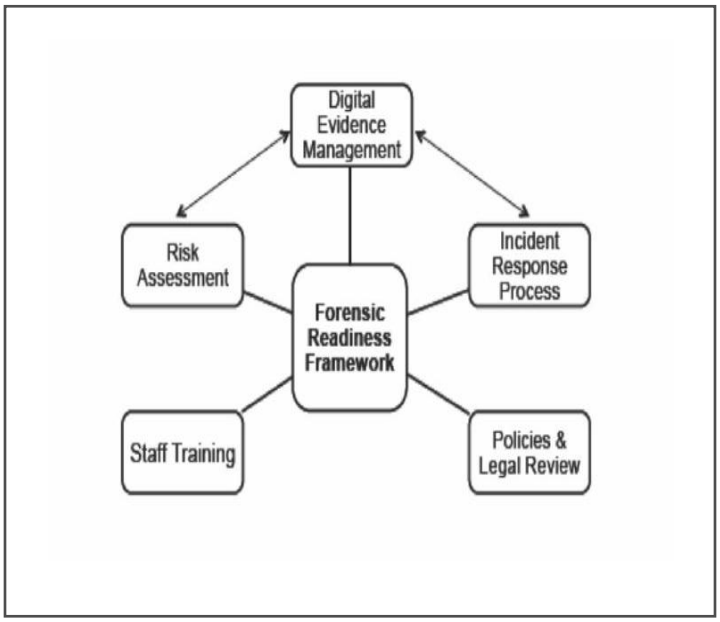


Figure10 Digital Forensic Readiness Framework Components (Dimotikalis *et al.*, 2013)

DISCUSSION

This section provided a clear discussion on the identified forensic models and have explained both their strength and limitations for easy comprehension and section, table 1 below shows the details of the models.

Table 1: Forensic Model Strength and Limitation

Framework	Strength	Limitation
Digital Forensic Readiness Framework for South Africa SME's Stander *et al.*, (2010)	Focuses on an administrative level Provide enough guidelines to collect digital evidence	Lack of judiciary concept Applicable laws Did not include people who will conduct the investigation
A Conceptual model for digital forensic readiness Antonio and Labuschagn, (2012)	Focuses on proactive activities. Enhance the credibility to respond to any incident. minimize the cost of forensic investigation	The model is conceptual. Lack of proper reactive measures
A Theoretical Framework for Organizational Network Forensic Readiness Taylor *et al.*, (2007)	Focuses on the enterprise level Inclusion of network forensic as a way of breaking the cycle of attack and defense Shows the nature of conceptual framework at the enterprise level	Lack of legal issues consideration Focuses on network perspective rather than managerial
Towards A Digital Forensic Readiness Framework For Public Key Infrastructure Systems Valijarevec and Venter, (2011)	This framework is the first to be proposed for the PKI system. The model is iterative where; one can go back to the previous phase when required. Input in all phases has a relationship to one another The framework includes both proactive and reactive responses.	Lack of legal and judiciary involvement. Retention period of pre-incident data collected.
Digital forensic readiness framework components Dimotikalis *et al.*, (2013)	The framework suggested that its components are the basic approach to DFR. All the components have a relation to one another Risk assessment can be performed more than one depending on the organization needs	This framework is not practically implemented in any organization This framework has a Reactive approach method The framework is not comprehensive enough to be widely used
Extended digital forensic readiness components framework Ivan Claims, (2013)	The framework gives a detailed process on how to execute the DFR with sub-function The framework has a monitoring and reporting function that will help to evaluate the performance of the framework	The framework doesn't specify the steps of implementation within an organization The framework lacks a risk analysis function. Lack of strategic response when an incident occurs before the investigation begins
Digital forensic readiness commonalities framework	All the components have a good relation to one another	Lack of risk assessment

Whyte and Claims, (2012)	The framework provides a methodology to be followed in implementing the framework The framework has a monitoring and reporting function that will help to evaluate the performance of the framework The framework provides a guideline for the development and execution of DFR in an organization.	More dependency on one another in the framework components. Lack of incident response approach
The continues forensic readiness framework Jeroen de Wilt, (2013)	Focuses on managerial level The emphasis on the involvement of stakeholders in the development of DFR PDCA availability in the framework	Lack of policy in the framework Lack of risk assessment components Premature Digital forensic readiness framework

LIMITATIONS OF THE STUDY

The research study has been conducted successfully, few limitations were faced including time constraints as well as the effect of Covid 19 pandemic constraints.

CONCLUSION

In conclusion, the existing models have been widely implemented in various organizations, this indicates their acceptability in the industries, however, not all models can be implemented in any organization, and the organization needs to be familiar with the concept of the model to see the applicability in the organizational workspace. This paper has provided such details for any organization to go through before accepting or implementing any model, it serves as a guideline for selecting a forensic model

REFERENCES

Ivan Claims, (2013), Proposing a Maturity Assessment Model Based on the digital forensic readiness Commonalities Framework, University of the Western Cape

Dimotikalis Panagiotis, AntonisMouhtaropoulos and Chang-Tsun Li (2013), Applying a Digital Forensic Readiness Framework: Three Case Studies, Department of Computer Science Univesity of Warwick Coventry, UK

Valjarevic A, Venter HS, (2011),'Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems', retrieved on 17/10/2014, available at: http://icsa.cs.up.ac.za/issa/2011/Proceedings/Full/66_Paper.pdf

Antonio P, Labuschagne L, (2012), A conceptual model for digital forensic readiness, retrieved on 23/10/2014, at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320452

Stander, A, Barske, D, Jordaan, J, (2010), 'A Digital Forensic Readiness Framework for South African SME's, retrieved on 18/10/2014, at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588281

Taylor C B, Endicott-Popovsky, And Frincke D A, (2007), Specifying digital forensics: A forensics policy approach. Digital investigation, 2007. 4: p. 101-104.

Jeroen de Wit, (2013) Continuous Forensic Readiness Master Thesis, Faculty of EEMCS, University of Twente P. O. Box 217, 7500AE Enschede The Netherlands

Whyte G, and Claims, I, (2012). The state of digital forensic readiness of financial services companies in South Africa. Proceedings of the 3rd International Conference on Information Management and Evaluation (ICIME) 2012, pp. 284-299. 16-17 April 2012, Ankara, Turkey.

Federal trade commission, (2014), Consumer Sentinel network Data book, [online], retrieved on 15/9/2014, available at: http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf

NIST, (2006), Guide to Integrating Forensic Techniques into Incident NIST Response http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Barbara J, (2005). "Digital evidence accreditation in the corporate and business environment" Digital Investigation Elsevier, vol. 2, pp. 137-146

Tan J, (2001), Forensic readiness ; @stake, Inc.196 Broadway Cambridge, MA02139 USA, [online] retrieved on 15/10/2014, available at: http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

Michael K, JHP Z and Olivier MS, (2006), Framework for a Digital Forensic Investigation, Information and Computer Security Architectures Research Group (ICSA) Department of Computer Science University of Pretoria, retrieved on 21/10/2014, available at: http://icsa.cs.up.ac.za/issa/20/Proceedings/Full/101_Paper.pdf

Rowlingson, R, (2004); "A Ten Step Process for Forensic Readiness"; International Journal of Digital Evidence, Winter, 2004, Volume 2, Issue 3

Ray D, A, (2007), "Developing a proactive digital forensics system" Ph.D. Dissertation, University of Alabama, Tuscaloosa, AL, USA, 2007.

Mandia K, Procise C and Pepe M, (2003), 'Incident Response and Computer Forensics'. Emeryville: McGraw-Hill/Osborne, 2003.

Pollitt M, M, (2007), An ad hoc review of digital forensic models, in Proc. Systematic Approaches to Digital Forensic Engineering, SADFE 2007, International Workshop on, 2007.

Grobler C, P ,Louwrens C, P, and Von S, S, H, (2010a), A framework to guide the implementation of proactive digital forensics in organizations," in Proc. International Conference on Availability, Reliability and Security, 2010, pp. 677-682.

Farlex, (2014), digital forensic, retrieved on 15/10/2014, available at" http://www.thefreedictionary.com/

Reith M, Carr C, &Gunsch G, (2002), An examination of digital forensic models. Retrieved on 26/10.2014 available at:https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6 F2C1-98F94F16AF57232D.pdf

TC-11 I, (2006), Digital Forensics - Fact sheet.[online], retrieve on 10/10/2-14, Available from: http://www.tc11.uni-frankfurt.de/WG/Factsheet_WG_11-9.pdf

Morgan C, and Whitcomb,(2001), An Historical Perspective of Digital Evidence: A Forensic Scientist's, National Center for Forensic Science, International Journal of Digital Evidence Spring, 2002. Volume 1, Issue 1

Grobler C, P, Louwrens C and Solmam S V, (2012), A Framework to guide the implementation of proactive Digital forensic in organization. In workshop for digital forensic Krakow, Poland.

Frincke D, A, Taylor C B, Endicott-Popovsky, (2007) , Specifying digital forensics: A forensics policy approach. Digital investigation, 2007. 4: p. 101-104.

Adamu Abdullahi Garba and Aliyu Musa Bade. 2019. "A recommended digital forensic readiness framework for nigerian banks", InternationalJournal of Development Research, 09, (08), 28920-28928.

