Digital Forensics Policies for Forensics Readiness in Organizations

Stanley Githinji

smgithinji@usiu.ac.ke , stanleygithinji@outlook.com

United States International University-Africa

Abstract

As the technological trends in Digital Forensics keep changing, new challenges are also constantly mushrooming in the domain which needs to be resolved. This research focused on identifying forensic policies which can provide the organizations with the authority to conduct investigations and collect and examine digital evidence within the organization. The research adopted a primary research method that was fundamentally tailored towards gathering context-specific data that can solve a particular problem. These research findings indicated that the proposed list of digital forensics policies had high importance level, hence the need for organizations to develop digital forensic policies and readiness plan that can effectively assist organizations and investigators in dealing with forensic investigations.

Keywords: *Forensic Readiness Plan, Investigation Process, Security Policy, Forensic Policy*

1.0 Introduction

The increase in the number of successful cyber-attacks is threatening organizations and personal security worldwide (Harichandran, Breitinger, and Baggili, 2016). As a result, digital forensics has been employed to combat any attack or cybercrime and to improve and acquire legal evidence found in digital media. Digital forensics can be identified as the application of science to identify, acquire, examine and analyze data while maintaining data integrity and the chain of custody of the information (Alenezi, Atlam and Wills, 2019). The recent era has witnessed a cloud computing revolution; this revolution not only has led many to view the concept as a new IT paradigm but also has given cloud computing a reputation as one of the most rapidly growing and industry changing technologies since the conception of computing itself (Hamid & Amin, 2014).

1.2 Motivation

The US National Institute of Standards and Technology (NIST) has identified forensics challenges. Among these concerns are the issues of how to conduct a thorough digital investigation in cloud environments and how to prepare to gather data ahead of time prior to the occurrence of an incident; indeed, this kind of preparation would save money, effort and time (NIST,2020). In today's complex international security environment, investigations more often require highly specialized and technical expertise. To better address these challenges, one of the policing capabilities that INTERPOL focuses on is digital forensics, a rapidly changing discipline which requires robust policies and procedures (Interpol, 2019).

There is need for well-defined policies, especially as they relate to digital forensic readiness which can provide the organization with the authority to conduct investigations and collect and examine digital evidence within the organization, and can demonstrate that the organization is fair-minded and objective in its actions, and follows due process in all forensic matters (Barske, Stander & Jordan, 2020).

1.3 Research objectives:

1. To identify forensic policies which can provide the organizations.
2. To develop digital forensic policies that intends to contribute to forensic readiness in organizations.

2.0 Literature REVIEW

This section provides literature background on the following areas: Digital Forensics, National Institute of Standards and Technology (NIST) Cybersecurity framework, International Organization for Standardization (ISO) digital forensics, digital forensic readiness, security policy and finally on digital forensic policy.

2.1 Digital Forensics

Digital forensics is a field that is still evolving. Digital forensics is the application of science to identify, acquire, examine and analyze data while maintaining data integrity and the chain of custody of the information (Alenezi, et al, 2019).

Digital Forensic is a field that is new and emerging with the introduction of new technologies readily accessible, available, affordable, and heavily dependent on individuals and businesses. As technology grows, new criminal techniques and activities known as cybercrimes emerge, posing challenges to law enforcers (Tonye, 2018).

Cooperate Digital Forensic Investigation (CDFI) process model is used is to avoid failed investigations and to improve CDFI procedures. The model consist of four-phases i.e. identification & preparation, acquisition, analysis, and presentation of digital forensic report.

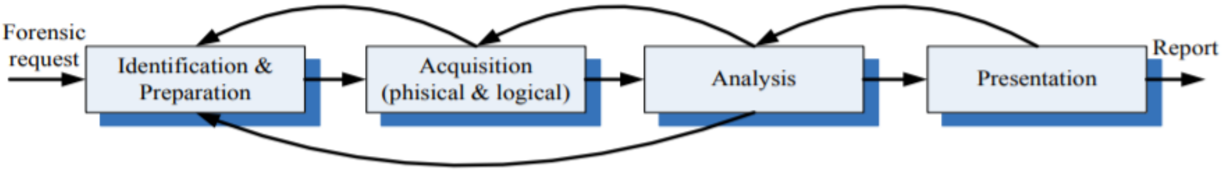

Forensic request
Identification & Preparation
Acquisition (phisical & logical)
Analysis
Presentation
Report

Figure 1: CDFI investigation process model using four phases (Grubor, Heleta, Ristić and Barać, 2016)

2.2 NIST Cybersecurity Framework

The five core functions of the Cybersecurity Framework are defined identify, protect, detect, respond and recover. The activities in the identify function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident" (NIST, 2018).

2.3 International Organization for Standardization (ISO)

International Organization for Standardization (ISO) is engaged in the development and publication of standards for almost all areas of human activity. This concerns standards for products, services and best practices. The family of standards ISO 27000 focuses on information security including digital forensic investigation (Veber, Klíma, 2014), which also includes standard ISO/IEC 27037: 2012 (ISO, 2012).

ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions (ISO, 2012).

The international standard (ISO, 2012) mainly deals with the initial process of collecting and storing potential digital evidence and disregards subsequent work with the evidence, such as its analysis, presentation and disposal. The persons who handle digital evidence should be able to identify and manage risks that can arise when working with this kind of evidence, in order to prevent its debasement and rendering it useless. DEFR (Digital Evidence First Responder) should follow certain general principles to maintain the integrity and reliability of digital evidence.

2.4 Digital Forensic Readiness (DFR)

Forensic readiness has been defined as: ‘the capability of an organization to use digital evidence in a forensic investigation’. For businesses, especially medium or small enterprises, gaining this capability can seem time consuming and expensive: it may involve a number of processes, it may require new hardware and software and people with specialized skill sets may need to be hired in order to implement any plan (Collie, 2018).

A DFR plan according to Benny (2014) is a policy document that sets out exactly what to do when digital evidence is required, either as part of the legal action, regulatory response, internal investigations or disciplinary procedures. However, Cobb (2013) states that DFP sounds like a daunting challenge to most organizations. Many areas, for example, the emergence of cloud computing have not been thoroughly considered in terms of its forensic readiness, hence posing a challenge to many organizations. The objective of a DFR plan is to maximize the amount of evidence data that is readily available and to minimize the time and costs needed to secure the required evidence.

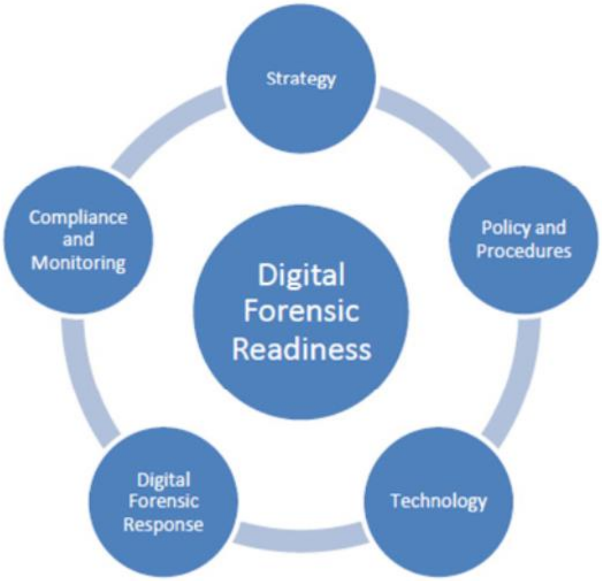

Strategy
Policy and Procedures
Technology
Digital Forensic Response
Compliance and Monitoring
Digital Forensic Readiness

Figure 2: Components of Digital Forensic Readiness (Barske, Stander & Jordan, 2020).

Figure 2 above depicts components of Digital Forensic Readiness. The decision to implement a digital forensic readiness program must be a strategic decision. Every organization need some form of policies and procedures in place to guide members of the organization with regards their actions and activities. It is crucial that an organization that implements a digital forensic readiness program acquire the necessary software and hardware to acquire and preserve digital evidence, and if needed, conduct a completed digital forensic examination. Digital forensic readiness should address the response by the organization to an event that actually requires digital forensic investigation. Once a digital forensic readiness program is in place, it must be monitored, and complied with or else risk the failure of the entire digital forensic readiness program (Barske, Stander & Jordan, 2020).

2.5 Security Policy

A security policy is a statement that clearly specifies what is allowed and what is disallowed with regards to security. At the lowest level security policies partition the states of a system into a set of authorized or secure states and unauthorized or insecure states. Initiatives to improve cybersecurity policies and address digital security threats should involve appropriate collaboration among governments, the private sector, civil society, academia, and the technical community. Initiatives to improve cybersecurity policy frameworks that address digital security threats should involve appropriate collaboration among governments, the private sector, civil society, academia, and the technical community (Global Partners Digital, 2018).

2.6 Digital Forensic Policy

This policy sets out how to gather and preserve electronic data for the purposes of any criminal or disciplinary investigation that may arise. National Institute of Justice (2020), developed a manual that give law enforcement agencies a resource that will serve as a starting point for the development of policies and procedures for the collection, handling, and processing of digital evidence.

Well-defined policies, especially as they relate to digital forensic readiness, can provide the organization with the authority to conduct investigations and collect and examine digital evidence within the organization, and can demonstrate that the organization is fair-minded and objective in its actions, and follows due process in all forensic matters (Barske, Stander & Jordan, 2020).

2.7 Policy Process-Formation Process

According to Global Partners Digital, 2018, framework for multi-stakeholder policy making provides the four stages of policy development: Policy process formation, this stage establishes the protocols that will guide the policy process, including rules of engagement and mechanisms for agreeing the outputs. The next stage is policy drafting, the number of steps within this stage will depend both on the issue and on national policymaking norms or frameworks and could include. The policy drafting process is not a linear process, and some or all stages may be repeated several times.

Policy agreement, this is the third stage of the process in which the parties in the policymaking process come to agreement typically through consensus on the policy in question. If agreed, the policy is then forwarded on to those parties who are in a position to stage four which is policy adoption. If the policy is not agreed upon, then it would, subject to protocols agreed in the first stage, be further worked on by the stakeholders (GPD, 2018).

3. 0 Research Methodology

The researcher adopted a primary research method that was fundamentally tailored towards gathering context-specific data that can solve a particular problem. Primary research is defined as a methodology used by researchers to collect data directly, rather than depending on data collected from previously done research. It allows the researcher to gather first-hand information which can be considered to be more valid and authentic in a research environment (Creswell & Clark, 2017).

3.1 Questionnaire construction

An online questionnaires provided a cost-effective way of gathering information given the nature of the study. It provided anonymity where sensitive questions were asked and therefore promoted the chance of more honest answers. To ensure reliability, the questions were designed to measure particular traits. The researcher ensured questionnaires were not biased and ambiguous and data collected was guided by research objective and specific issues being investigated. To enhance the quality of data obtained, the questionnaire comprised of scaled questions and open-ended questions.

3.2 Sampling and Target population

Purposive sampling technique is the deliberate choice of an informant due to the qualities the informant possesses where the researcher decides what needs to be known and sets out to find people who can and are willing to provide the information by virtue of knowledge or experience. The respondents comprised of IT Managers, Cybersecurity professionals, Digital. According to Forster and Grancht (2013), it is the duty of the researcher to ensure that there is a cross section representative of the stakeholders involved.

Europa (2014) explains that, the criteria for selecting participants should be based on professional experience, independence and ability to work in a group. The advantage of having experts is that the credibility of conclusion is high, significance reduction in time allocated and cost effectiveness but they also have a tendency of going beyond their field of competence. Selected participants were employees in both private and public institutions according to table 1.

Table 1: Target participants

Participants	Number
IT Managers	10
Cybersecurity Professionals	7
Digital Forensic Professionals	10
ICT Officers	8

IS Lecturers	5
Total	40

4.0 Data Analysis and Results

Raw data collected was subjected to coding before it was analyzed. The research utilized descriptive statistical data analysis using Excel 2019. The statistical information presented is derived from forty (40) questionnaires distributed to respondents. Thirty-eight (34) questionnaires were completed and returned, giving a response rate of ninety-five percent (85%). Figure 3 below summarizes the descriptive statistics for the respondents. The respondents were IT managers (9), cybersecurity professionals (5), Digital Forensics Professionals (7), ICT officers (10) and Information Security Lecturers (3).

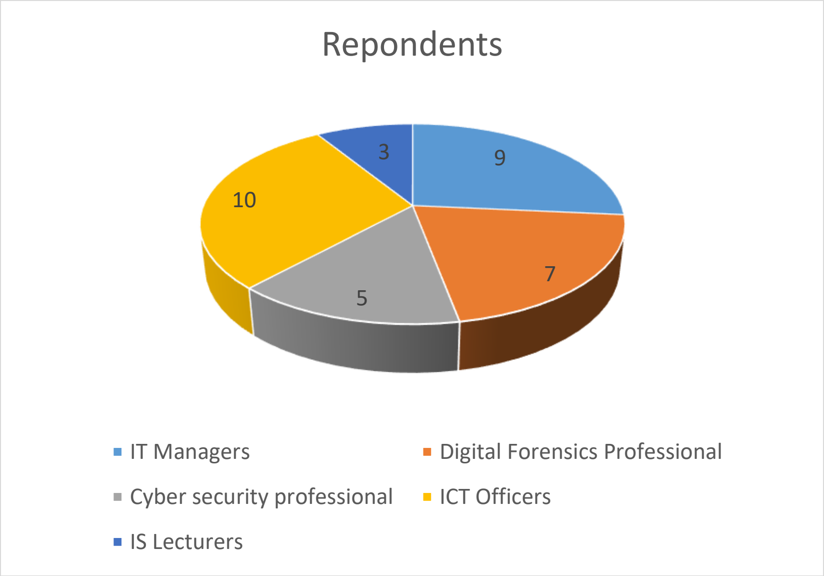


Figure 3: Survey Respondents

What is the percentages of organizations that had a robust Information security policy?

Figure 4 below show the percentage of organizations that had a robust information security policy. 82.4 % had a robust information security policy and only 17.6 % did not to have an information security policy. The results show that majority of organizations are aware that IT security policies are pivotal in the success of any organization.

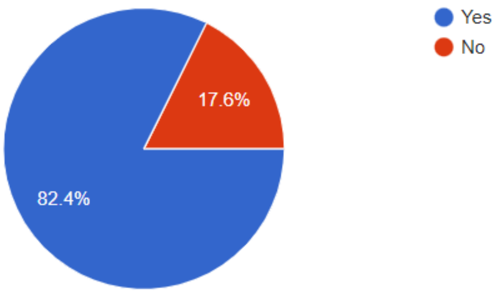


Figure 4: Robust Information security policy.

Figure 5 below shows that, 67.6 % of that organization didn’t have a digital forensic policy in place. NIST, 2020 and Cobb, 2013, noted developing digital forensic plan and policies sounds like a daunting challenge to most the organizations.

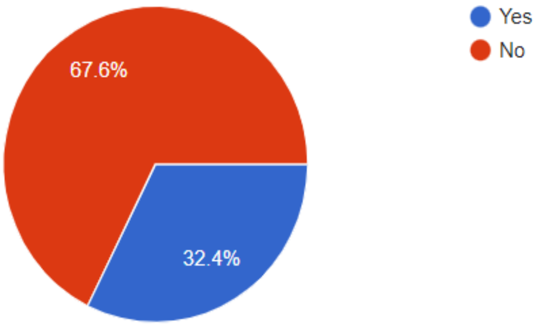
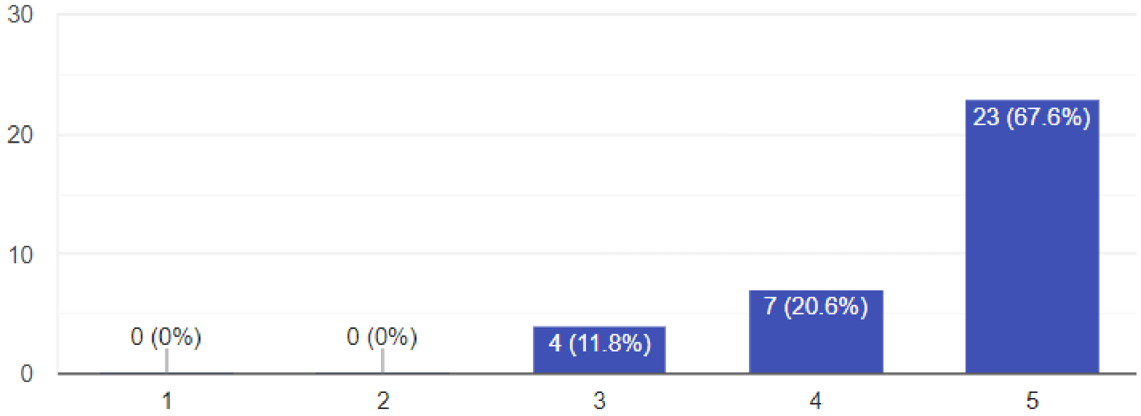


Figure 5: Availability of a digital forensic policy

How can a DFR plan enable organization to adequately prepare to handle forensic investigation?

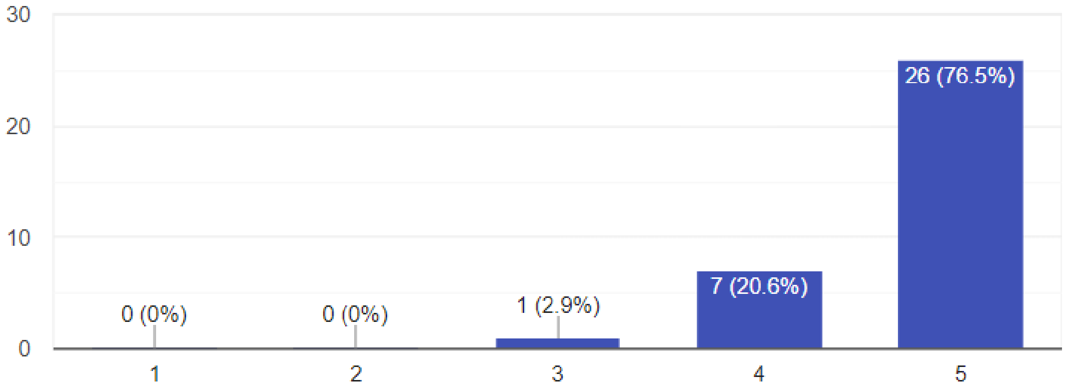
Digital Forensic Readiness (DFR) Plan prepare an organization for an event occurrence of which cannot be predicted. Table 1 below shows that 88.2 % agree that having a well-crafted DFR plan can enable organization to adequately prepare to handle forensic investigation.

Table 2: Digital Forensic Readiness Plan



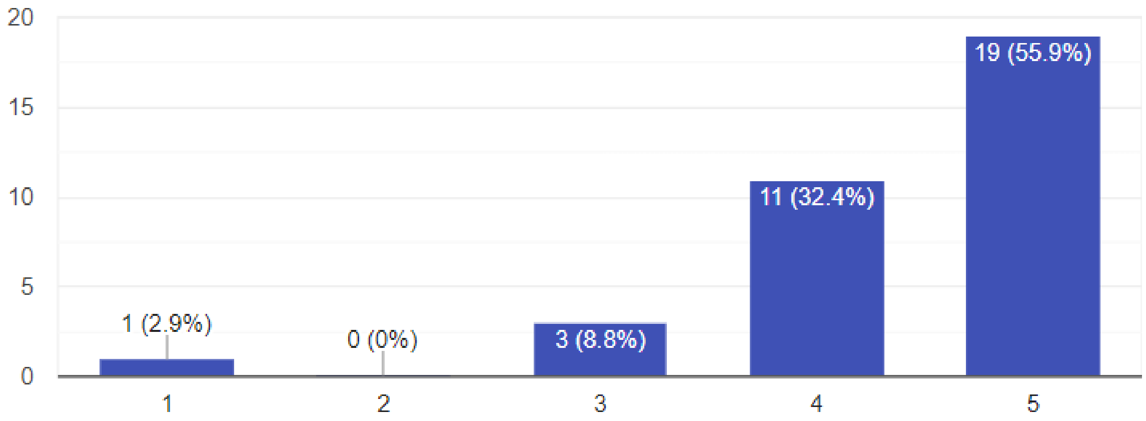
Results on table 3 below shows that decision to implement a DFR plan.97.1 % agree that a digital forensic readiness plan must be a strategic decision for the organization concerned.

Table 3: Decision to Implement DFR plan



The respondents were asked whether having a well-crafted digital forensic policy can help organization to successfully manage cases and investigations involving electronic evidence. Results in table 4 below indicate that 88.3 % of the respondent were in agreement that having a digital forensic policy can help and only 2.9% of the respondent indicated that a digital forensic policy can't fully enable organization to handle forensic investigations.

Table 4: Well-crafted digital forensic policy



What is the level of importance outlined digital forensic policies?

The respondents were required to personally evaluate the importance the above proposed list of digital forensic policies that can be implemented in comprehensive digital forensic policy documentation manual.

The results in Figure 6 below indicate that proposed list of digital forensics policies had average importance level of 91.5%. A proof that the above digital forensic policies are of great importance to organizations and can be used as a starting point in development of comprehensive digital forensics manuals that can provide the organization with the authority to conduct investigations (Barske, Stander & Jordan, 2020). The above proposed policies concur with the US National Institute of Justice resource on policies for the collection, handling, and processing of digital evidence. National Institute of Justice (2020).

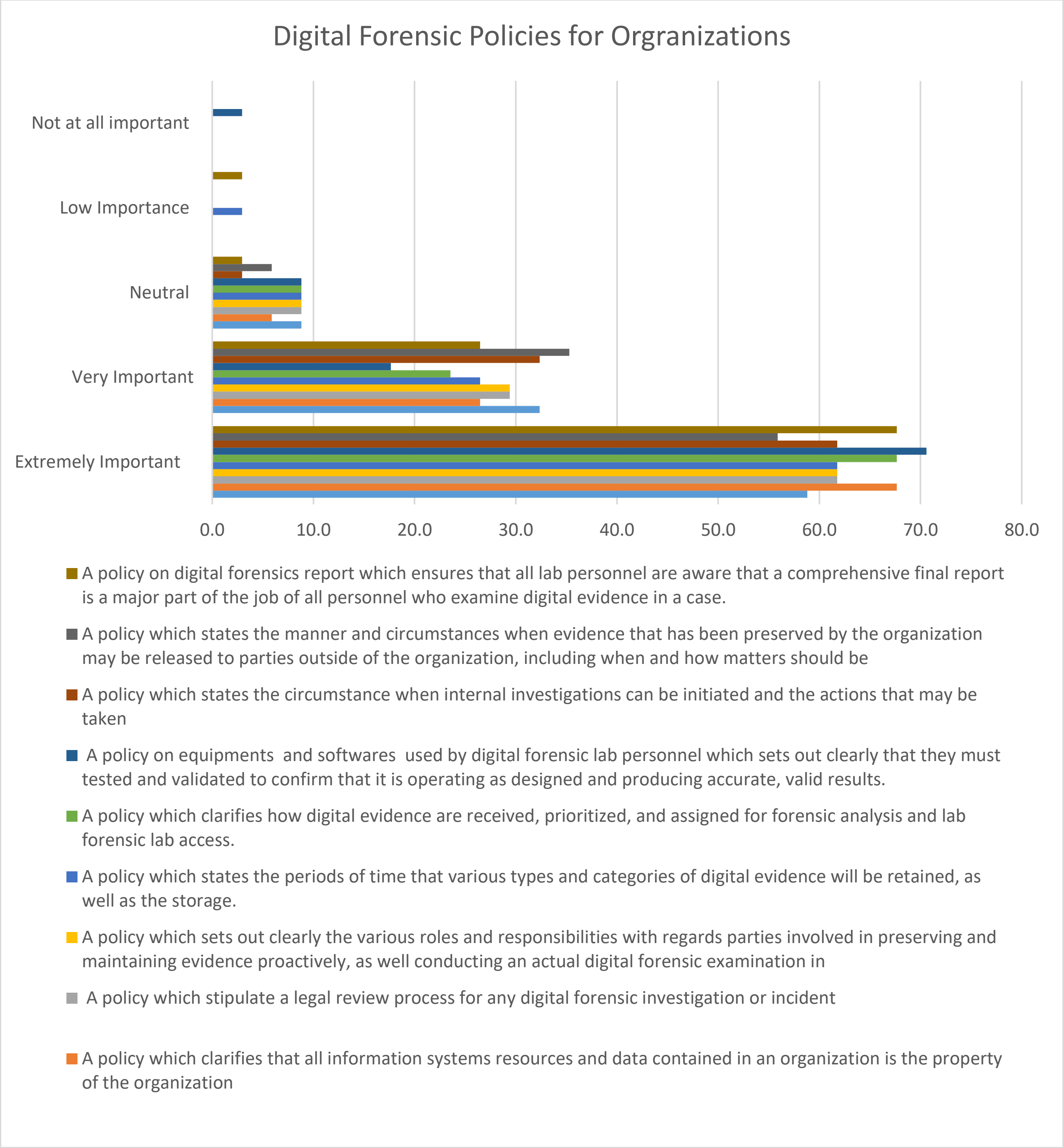


Figure 6: Digital Forensic Policies for Orgarnizations

5.0 Conclusion and Recommendations

The findings indicated that majority of organizations have information security policy but lack digital forensics policy, which is a major area of concern. Failure to have digital forensic policies can have negative consequences for the organization. The organization needs to consider proposed policies and align them to ensure they meet organization's needs. If an organization does not have the capability to forensically acquire or analyze digital evidence, it should have policy indicating how it will handle the situation when these capabilities are needed.

The decision to implement some digital forensic policies is a strategic decision and involvement of top management is critical to the design and effectiveness of any information security program. Further research opportunities lie in development of a comprehensive digital forensics procedures and quality standards for digital forensics. This standard places on the organization the responsibility for ensuring the organization has quality practices and procedures in place sufficient to provide confidence that the results of forensic examinations are of high quality.

References

Alenezi, A., Atlam, H.F. & Wills, G.B. Experts reviews of a cloud forensic readiness framework for organizations. J Cloud Comp 8, 11(2019). https://doi.org/10.1186/s13677-019-0133-z

Barske, D., Stander A., Jordan, J. (2010). A Digital Forensic Readiness Framework for South African SME's. Available at https://www.researchgate.net/publication/22417860

Bordens, K.S. & Abbott, B.B. (2014). Research design and methods: A process approach (9th Ed.) San Francisco: McGraw Hill

Benny, L., (2014). Forensic Readiness Plans. Available at: http://www2.deloitte.com/ au/ en/ pages/ risk/ articles/ forensic-readiness-plans.html

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Cobb, M. , (2013), "Digital forensic investigation procedure: Form a computer forensics policy", Available at http://www.computerweekly.com/ tip/ Digital-forensic-investigation-procedure-Form-acomputer-forensics-policy.

Europa.2009. Expert panel. Available: http://ec.europa.eu/europeaid/evaluation/methodology/examples/too_pan_res_en.pdf [Accessed 28 Oct 2021].

Forster, B. and Gracht, H., 2013. Assessing Delphi panel composition for strategic foresight — A comparison of panels based on company-internal and external participants. Elsevier.

Global Partners Digital (2018). Available at https://www.gp-digital.org/wp-content/uploads/2018/03/framework_cyberpolicy.pdf

Gojko Grubor, Milenko Heleta, Nenad Ristić, Ivan Barać (2016). Integrated Management Model Of The Corporate Digital Forensic Investigation: Tehnički vjesnik 23, 1591-1600

Harichandran, S.V., Breitinger, F., Baggili, I., &Marrington, A. (2015). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. Computers & security, 57, 1–13.

INTERPOL (2019). Global guidelines for digital forensics laboratories. Available at https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

ISO. (2012) ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, International Organization for Standardization, Geneva.

NIST (2020). NIST Cloud Computing Forensic Science Challenges. Available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

National Institute of Standards and Technology (NIST). (2018, April 16). *Framework for improving critical infrastructure cybersecurity* (version 1.1). Available at https://doi.org/10.6028/NIST.CSWP.04162018

Veber, J., Klíma, T. (2014) “Influence of Standards ISO 27000 Family on Digital Evidence Analysis”, 22st Interdisciplinary Information Management Talks (IDIMT), PodĢbrady, pp 103-114.

Whyte Stella Tonye (2018). Cyber Forensic and Data Collection Challenges in Nigeria. Global Journal of Computer Science and Technology.18, 3, 0975-4350.