International Conference on Computational and Social Sciences
http://iccss.vfast.org/@ 2015 ICCSS-15
August 25-27, 2015

pp. 551--560

A HOLISTIC–BASED DIGITAL FORENSIC READINESS FRAMEWORK FOR ZENITH BANK, NIGERIA

ADAMU ABDULLAHI GARBA[1], AND MAHEYZAH MD SIRAJ[2]
[1] Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai Malaysia.
adamugaidam@yahoo.com
[2] Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai Malaysia
maheyzah@utm.my

ABSTRACT. *The advancement of internet has made many business organizations conduct their operation automatically, in effect its open a possibly dangerous unforeseen information security incidents of both illegal and civil nature. Therefore, if any organization does't arrange themselves for such instances, it's likely that vital significant digital evidence will be damage. In other word an organization should has a digital forensic readiness framework (DFR). DFR is the capacity of anyassociation to exploit its prospective to use digital evidence whilst minimizing the cost of investigation. Subsequently, in order to prepare organizations for incident responds, the application of digital forensic readiness policies and procedures is important. Contemporary lack of forensic skills is one of the factors that make organizations reluctant to implement digital forensics. This project propose a holistic-based framework of DFR and investigate how it can be applied to Zenith Bank Plc. This paper surveys existing frameworks to identify the best-suited practical components for Zenith Bank's operational unit*

***Keywords**:* Digital Forensic; Holistic Readiness Framework Zenith Bank Evidence

1. Introduction. Industries have being growing tremendously in the 21st century, with each improvement in information technology field comes a new threat. The growth of threats of fraud and security lead to various challenges for the law enforcement and organization to tackle all over the globe. This incident has led many companies and organization to start investing on security measures that will protect their organization from any threats. It includes the development of

effective strategies to manage any incoming incidents.These plan help in detection of a risk and describe, recover from it by continuing with the normal trade as promising. Small amount of consideration is given to the identification and safeguarding of digital forensic (DF) evidence for possible prosecution [1]. DF is a subdivision in information security incident management. The subdivision offers the basis to ensure that each organization should consider the obligation to gather permissible information in order to define the actual main cause of an event and effectively indict criminals [2]. Most organizations overlook the basic requirement of digital forensic, lack of concrete evidence to verify the authenticity of fraudulent transaction that will link to the attacker. Therefore, it has become necessary for all functioning organization to prepare for the digital forensic examination so that full investigation can be carried out. Organization must implement DF at their operational unit to ensure that all incidents can be investigated fully. Many organization undervalue the highly need for digital forensic evidence [1]. When evidence is vital to verify deceitful transaction, is often not enough linkage the foe to the crime. It is important for each organization to be preparing for DF investigation and guarantee that the whole organizational functioning environment is primed for any investigation. The acknowledged literatures on DF readiness concentrate generally on evidence identification, management, and storing and training requirement [3].

DF is the process for an association to exploit its possible in order to use the electronic evidence when necessary, it helps to improve security approach and minimize cost of investigation. This project aims at proposing the appropriate components of digital forensic readiness for operational unit.

2. **Related Works**. The main objective of this section is to analysis the related literature in the area of digital forensic readiness. DF is the systematic proposition of the procedures involved in the recapture, safeguarding and investigation of digital evidence, including audio, imaging and communication devices. DF is the part of science that emphases on evolving evidence of computers in court [4]. Digital forensic evidence can also be found in digital documents, emails, digital photographs, software programs, or other digital archives and network metadata, which may be at question in a legal circumstance in order to win a case [5]. In another context some authors have recognized three modules in digital forensic: Proactive, Active and Reactive. These modules are link to one another [6]. Proactive means preparing the organizations for investigations; Active refer to consideration, the procurement and exploration of live evidence; and Reactive as the real 'post-action' forensic investigation. Many researchers believed that computer forensic advancement is surrounded by three-stages of evolution, which are: Ad hoc, structured and enterprise phase:

   i) **Ad hoc**: This phase can be described as when there is lack of structured, clear goal and adequate tool, processes and procedures to be used in conducting investigation, some

literature calls it pre-forensic period. In this phase no any acceptable use policy and procedures are implemented.

ii) **Structure phase**: this phase can be characterized by the development of more complex solution for computer forensic, this include recognize and acceptable procedures, tested tools that were developed to tackle computer related problems.

iii) **Enterprise phase**: this phase can be states to as the present state of the computer forensic and is the advance of all the phases. In this current time Computer Forensic (CF) is widely considers as actual science, which involve real-time collection of evidence, using effective tools and processes. CF is widely accepted by the international communities. CF also allows proactive collection and detection and can be accomplished in a way that is consistent with the process approved by the law [7]

Many researchers shows that forensic investigation has two approaches: Dead and Live forensic: Dead forensic is the traditional ways of collecting and preserving evidence collected in a computer in offline and creating duplicate of the storage media in a bit-stream[8]. Live forensic is the investigation that is performed with the first few hours of an investigation which provide information used during the suspect interview phase. Live analysis techniques uses software to investigate the time frame which is on the system [9]. While dead analysis do not use software that existed on the system throughout the investigation of the time frame [10].

Computer Crime and Security surveys confirm that cybercrime is real and also remains to be a significant problem, and cause financial damage, less percentage of loss reported by law enforcement is 16% in 1996 and 25% in 2006. Furthermore, in 2006 total losses reported was $52,494,290 for 313 respondents and 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 goes by.

Table 1 The common components from the existing frameworks studied

Features	Authors	Stander et al., (2010)	Antonio, and Labuschagne, (2012)	Taylor, et al., (2007)	Valijarevec, and Venter, (2011)	Dimotikalis et al.,(2013)	Ivan Chiuns, (2013)	Whyte and Chiuns,(2012)	Jeroen de Wilt, (2013)
1	Strategy	✓	x	✓	x	x	✓	✓	✓
2	Policy	✓	✓	✓	x		✓	✓	x
3	Technology	✓	✓	x	x	x	x	x	✓
4	Response	✓	x	x	x	✓	x	x	x
5	Compliance	✓	x	x	x	x	✓	✓	x
6	People	x	✓	x	x	x	x	x	✓
7	Process	x	✓	x	x	x	x	x	✓
9	Goal of the system	x	x	✓	x	x	x	x	x
10	Procedures	✓	x	✓	x	x	x	x	x
11	Mechanism	x	x	✓	x	x	x	x	x
12	Security	x	x	✓	x	x	x	x	x
13	Scenario	x	x	x	✓	x	x	x	x
14	Source	x	x	x	✓	x	x	x	x
15	Pre-incident collection	x	x	x	✓	x	x	x	x
16	Pre-incident analysis	x	x	x	✓	x	x	x	x
17	Incident detection	x	x	x	✓	x	x	x	x
18	Post-incidentcollection	x	x	x	✓	x	x	x	x
19	Post-incident analysis	x	x	x	✓	x	x	x	x
20	Architecture defining	x	x	x	✓	x	x	x	x
21	Implementation	x	x	x	✓	x	x	x	x
23	Stakeholders	x	x	x	x	x	x	x	✓
24	Tactical	x	x	x	x	x	x	x	✓
25	Operation	x	x	x	x	x	x	x	✓
26	Methodology	x	x	x	x	x	x	✓	x
27	Systems and events	x	x	x	x	x	✓	✓	x
28	Compliance	✓	x	x	x	x	✓	✓	x
29	Training	x	x	x	x	✓	✓	✓	x
30	Report	x	x	x	x	x	✓	✓	x
31	Legal	x	x	x	x	✓	✓	✓	x
32	Judiciary	x	x	x	x	x	x	x	x
33	Governance	x	x	x	x	x	✓	x	x

34	Digital evidence management	x	x	x	x	✓	x	x	x
35	Incident respond process	x	x	x	x	✓	x	x	x
36	Legal review	x	x	x	x	✓	x	x	x
37	Risk assessment	x	x	x	✓	✓	x	x	x
38	Monitoring	✓	x	x	x	x	✓	✓	x
39	Awareness	x	x	✓	x	x	x	x	x

The table 2 above shows the authors and also the components they used in their DFR framework. Thirty nine components were found in this existing framework from eight different authors. The rows show the components while the columns show the authors that proposes those components.

2.1 Issues To Consider. The issues to be considered from Table 2 are:

- All the components are generic and can be applied to any digital forensic readiness.
- Most of the frameworks have similar components like policy and people while only few components are uniquely to some frameworks like incident respond process.
- Also frameworks merge some components to be one like in policy and compliance [11].
- There are no holistic frameworks that will suite many organizations.
- Each researcher designs their framework based on their own scopes.

Therefore, a generic DFR is proposed which covers eight components:

- Strategy
- Policy and procedures
- People
- System and event
- Legal requirement
- Monitor and report
- Forensic preparation.

4. Proposed Components Actvities. There is presently no holistic based digital forensic readiness framework. Therefore, no application of holistic based forensic readiness framework to the best of the author's knowledge. The author is recommending a framework which consists of eight components as basic components in DFR and is explained in more details in this section. These components were chosen by the author based on the analysis conducted using table 1 above and also the scope of this research (Zenith Bank). As mention earlier, these components make a basic holistic based digital forensic readiness framework. Other researchers can adopt and enhance based on their own scope. The activities of each component will be discussed in details in the following section:

A) Strategy. This component ensures that the organization has a DFR strategy aligned to the organization needs. There must be a tactical order from executive to instrument and maintain DFR [12]. Successful implementation of this component will allow the alignment of business risk unit incident- monitoring unit [11]. To form an organization strategy, adequate resources and support must be ensured and the following activities should be performed:

- A DFR strategy aligned to the organization
- Identifying what lawmaking and procedures enacts on the organization to preserve records
- Detecting which situations cloud possibly requires digital evidence
- Ascertaining the evidence source and diverse forms of digital evidence within the organization
- Confirm adequate cash to the set up of digital forensic readiness program.

B) Policy and Procedure. Organization need some form of policy and procedure within the workplace to guide the staffs' regarding their activities. These policy and procedure can only be successful when top management didn't simply ignore the policies. Failure to comply with policy and procedure will result to bad result to the organization. [13]. Proper policy and procedure can provide the organization with authority to conduct investigations and collect evidence that are admissible in court [14]. The following policy should be implemented in the organization:

- Policies and procedures about the acceptance of evidence system within the organization
- Policies that stated all systems and resources within are sole property if the organization and activities will be monitored
- Policies that describe how the source system will be supervised
- preserved and the duration of storing the evidence
- Policies that indicate when will internal investigation will begin

C) People. An organization must have forensic processes to implement the DFR completely at their workplace. People are the backbone of all investigation. People are so important because they contribute toward the presentation and detection of security incident [15]. The below activities should be performed:

- Identifying the individuals and procedures that will have to be followed in reacting to attack.
- Identifying an other providers and enter into a service planning, which will confirm that t hey can respond anytime there are needed
- Selecting Forensic response Team in the organization

D) Forensic Preparation. This component ensures that Digital forensic staff training strategy is well developed; also DFR awareness campaigns are design so that all the organisation staffs' are aware of the forensic strategy and polices. Also its helps to reduce disturbance to the business from any exploration [16]. Activities to be performed include:

- Awareness campaigns
- Training strategy
- Certifications and accreditation programs

E) System and Events. The main aim of having this component is to detect all the source system (hardware, software, technologies, people, policies and procedures) that strength contain possible information, which may be incorporated in DFR strategy. Some rare examples of system and tools that might contain possible evidence are; logs, firewall, network devices, surveillance devices and computer [17]. Therefore, organization must have necessary resources to gather evidence in a forensically sound manner. Activities to be performed include:

- A list of System and infrastructure requirement(proactive and reactive tools)
- The identification and classification of source system
- Record all system activities and logs (computers and other connected device to the network)
- Identify storage for potential evidence and network requirement

F) Monitor and Report. This component ensures that organisation digital forensic incident report which compile with requirements and have an incident escalation policy. Also it can be used to monitor sources that house potential evidence to detect threat. Activities to be performed include:

- Identify correct Tools to monitor incident
- Incident escalation policy
- Report generation
- Audit report

G) Risk Assessment. Risk assessment is very important to be considering in any organisation. Risk assessment should be performed combined with the preparation of the rest of the forensic readiness policy which will cover the security issues. All processes and designs defined when applying DFR have to go through legitimate review during evaluation phase in order to ensure acceptability of potential evidence in court [18]. Activities to be performed include:

- Threats identification

- Threat categorization:
- Exposure assessment:
- Conduct the risk mitigation strategy
- Risk classification

H) Ligal Requirenment. This component ensures that judiciary, monitoring, and other commandments inside the organisation's realm of process are measured and combined in inclusive DFR strategy. Other aspect like legal requests, judicial requirements, other lawful requirements and business requirements that will affect the investigation of any incident must be covered. Activities to be executed include:

- Legal requirement
- Judicial requirement
- Other lawful requirement
- Business requirement

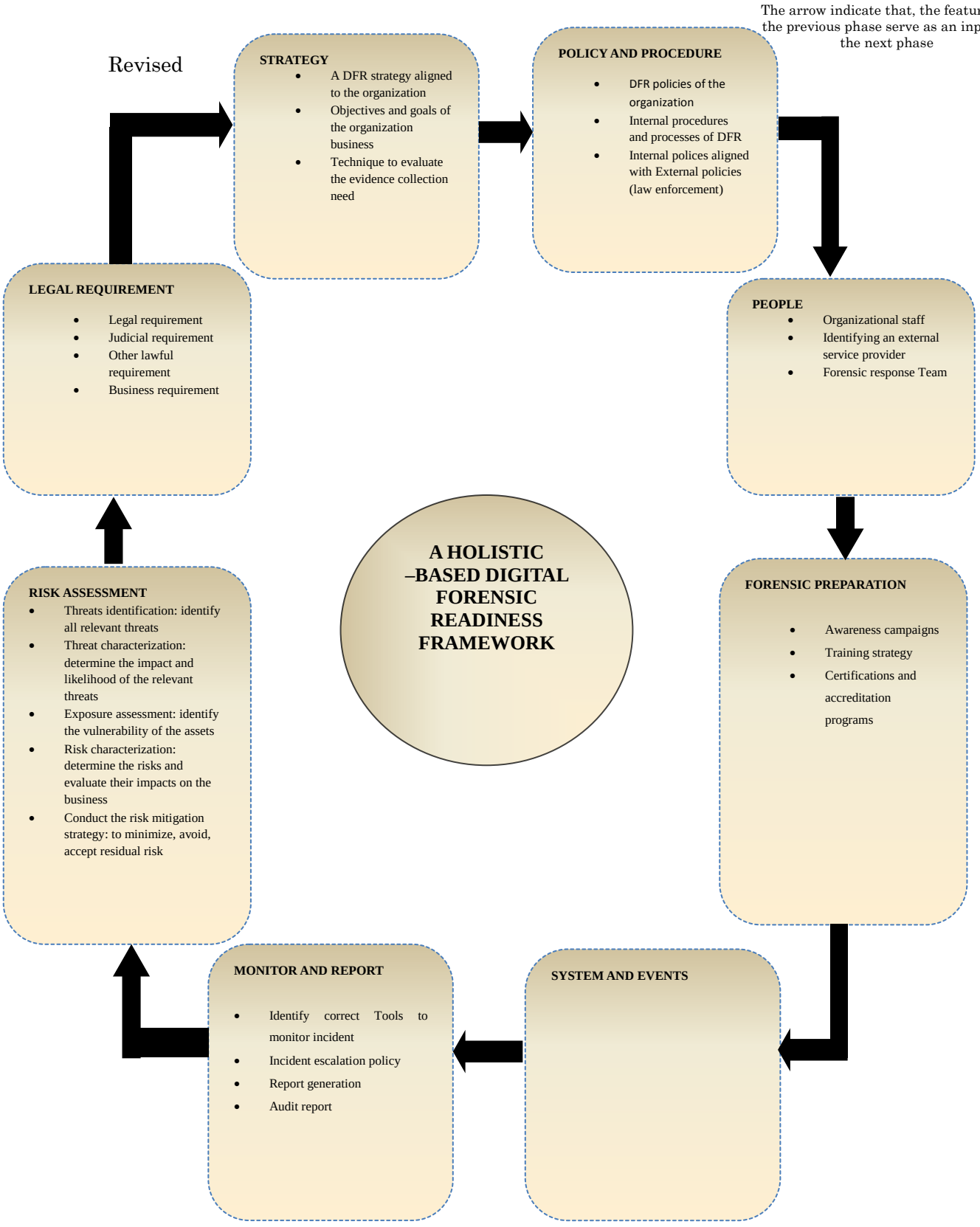

Figure 1 Proposed Holistic–Based Digital Forensic Readiness Components

5. Conclusion. In conclusion, the author proposed holistic–based digital forensic readiness components for Zenith Bank Plc. This framework will serve as guidance to other researchers to explore more in this area. This framework is can be adopted for wide range of organizations dealing will electronic information as an asset, so that it will help to minimize the impact of attacks to the organizations and avoid any unwanted situation that may occur in the organization.

REFERENCES

[1] Sommer, P., *Directors and corporate advisors' guide to digital investigations and evidence.* 2005.

[2] Veiga, A.D. and J.H. Eloff, *An information security governance framework.* Information Systems Management, 2007. **24**(4): p. 361-372.

[3] Rowlingson, R., *A ten step process for forensic readiness.* International Journal of Digital Evidence, 2004. **2**(3): p. 1-28.

[4] Reith, M., C. Carr, and G. Gunsch, *An examination of digital forensic models.* International Journal of Digital Evidence, 2002. **1**(3): p. 1-12.

[5] Marangos, N., P. Rizomiliotis, and L. Mitrou, *Time synchronization: pivotal element in cloud forensics.* Security and Communication Networks, 2014.

[6] Grobler, C., C. Louwrens, and S.H. von Solms. *A framework to guide the implementation of proactive digital forensics in organisations*. in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. 2010. IEEE.

[7] Kent, K., et al., *Guide to integrating forensic techniques into incident response.* NIST Special Publication, 2006: p. 800-86.

[8] Beebe, N., *Digital forensic research: The good, the bad and the unaddressed*, in *Advances in digital forensics V*. 2009, Springer. p. 17-36.

[9] Reyes, A., et al., *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*. 2011: Syngress.

[10] Richard III, G.G. and V. Roussev, *Next-generation digital forensics.* Communications of the ACM, 2006. **49**(2): p. 76-80.

[11] Barske, D., A. Stander, and J. Jordaan. *A Digital Forensic Readiness framework for South African SME's*. in *Information Security for South Africa (ISSA), 2010*. 2010. IEEE.

[12] Grobler, M. and I. Dlamini, *Managing digital evidence-the governance of digital forensics.* Journal of Contemporary Management, 2010. **7**: p. 1-21.

[13] Imtiaz, F., *Enterprise Computer Forensics: A defensive and offensive strategy to fight computer crime.* 2006.

[14] Grobler, C. and B. Louwrens. *Digital forensics: a multi-dimensional discipline*. in *Proceedings of the ISSA 2006 from Insight to Foresight Conference. Pretoria: University of Pretoria*. 2006.

[15] Von Solms, S., et al., *A control framework for digital forensics*, in *Advances in Digital Forensics II*. 2006, Springer. p. 343-355.

[16] Pangalos, G. and V. Katos, *Information Assurance and Forensic Readiness*, in *Next Generation Society. Technological and Legal Issues*. 2010, Springer. p. 181-188.

[17] Mouhtaropoulos, A., M. Grobler, and C.-T. Li. *Digital forensic readiness: an insight into governmental and academic initiatives*. in *Intelligence and Security Informatics Conference (EISIC), 2011 European*. 2011. IEEE.

[18] Valjarevic, A. and H.S. Venter. *Towards a digital forensic readiness framework for public key infrastructure systems*. in *Information Security South Africa (ISSA), 2011*.