Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies(FEM)

Diploma Thesis

Case Study of Network forensic readiness for financial network in the Case of Ethiopian banks

Author: Lulit Girma Woldegiorgis

Supervisor: Ing.Tomas Vokoun

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

B.Sc. Lulit Girma Woldegiorgis

Systems Engineering and Informatics
Informatics

Thesis title

Case Study of Network forensic readiness for financial network in the Case of Ethiopian banks.

Objectives of thesis

General Objective

The general objective of this research is to analyze and study how to maximize the ability to collect valid digital evidence and minimize the cost of Network forensics during an incident.

Specific Objective

Perform a cost-benefit analysis to determine if implementing network forensic readiness is valuable to the organization.
How capable the organization is to collect, preserve, protect, and analyze digital evidence.
How much Network Forensic Readiness is necessary for the organization and what it used for?
Evaluate how much the evidence from network forensic is helpful in legal matters and the court of low.

Methodology

To fulfil the objectives, there will be literature studies used and also analyse the information gathered from the organisations. Also, use the forensic readiness policy and the ISO standards for network forensic analysis as a reference is expected.

The proposed extent of the thesis

50-60

Keywords

Forensic

Recommended information sources

1. Ivtchenko, Dmitri_Sachowski, Jason – Implementing digital forensic readiness _from reactive to proactive process-Syngress (2016)
2. Ric Messier – Network Forensics-Wiley (2017)
3. Jason Sachowski – Implementing Digital Forensic Readiness_From Reactive to Proactive Process-CRC Press (2019)
4. Douglas J. Landoll – Information Security Policies, Procedures, and Standards_A Practitioner's Reference-Auerbach Publications, CRC (2016)
5. Digital Forensics Processing and Procedures-Syngress (2012)
6. NTWO56-ForensiceReadinessPolicy-V05-IssFeb15

Expected date of thesis defence

2020/21 SS – FEM

The Diploma Thesis Supervisor

Ing. Tomáš Vokoun

Supervising department

Department of Information Technologies

Electronic approval: 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 21. 10. 2020

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 17. 03. 2021

Declaration

I declare that I have worked on my diploma thesis titled "Case Study of Network Forensic Readiness for financial network in the case of Ethiopian banks" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 31.03.2021 _____

Lulit Girma Woldegiorgis

Acknowledgement

First, I would like to thank The Almighty God for the gift of life and protection. Next, I would like to express my sincere gratitude to my supervisor Ing. Tomas Vokoun, for his insight and support through this research. My appreciation also goes to the Czech Republic Government for funding my Master' studies.

I would also like to thank the experts who participated in the interview and the online questionnaire for this research. Finally, my deepest gratitude goes to my families and friends for their countless support throughout my years of study.

Case Study of Network Forensic Readiness for financial network in the case of Ethiopian banks

Abstract

Banks are a crucial portion of the economy that facilitates expenditure, but, despite their importance, they are vulnerable to failure. Ethiopian banks' reliance on technology is growing faster than previously and has far-reaching consequences like exposing them to cyber-attacks. Despite the fact that banks are working on cyber security, attacks cause damage, and the investigation of the damage exposes the banks to additional costs and time waste. This is a signal for banks that need to improve their network forensic readiness capabilities. There is an observation of good practices to fulfil the readiness processes before an incident. However, there are not much studies that address current practices in the literature part. This research follows a qualitative method to study the case in which the current practices regarding Network forensic readiness in Ethiopian banks and the first paper to address the area. The results revealed that banks do not have satisfactory pre-incident activities implementation, including incident detection and alerting tools. Most important findings regarding the improper performance of defined information system architecture and data handling, including incident management, are observed as if there are good practices on implementing modern monitoring tools and frequent revision of necessary job aids and documents. Also, work on the awareness gap and develop the skill of employees, proper digital evidence source identification, and set the capability of pre-incident data analysis are Expected from banks to maximize the ability of Network Forensic Readiness and introduced a model. This also has been supported by other related studies.

Keywords: Digital Forensic, Network forensic, Network forensic readiness, potential digital evidence, International Organisation for standards, Intrusion detection system, Data investigation

Případová studie síťové forenzní připravenosti na finanční síť v případě etiopských bank

Abstraktní

Banky jsou rozhodující částí ekonomiky, která usnadňuje výdaje, ale přes svůj význam jsou náchylné k neúspěchu. Závislost etiopských bank na technologii roste rychleji než dříve a má dalekosáhlé důsledky, jako je vystavení kybernetickým útokům. Navzdory skutečnosti, že banky pracují na kybernetické bezpečnosti, útoky způsobují škody a vyšetřování škod vystavuje banky dalším nákladům a plýtvání časem. Jedná se o signál pro banky, které potřebují zlepšit své schopnosti forenzní připravenosti v síti. Pozorujeme osvědčené postupy k plnění postupů připravenosti před nehodou. Není toho však mocstudie, které se zabývají současnými postupy v literární části. Tento výzkum sleduje kvalitativní metodu ke studiu případu, ve kterém jsou současné postupy týkající se forenzní připravenosti sítě v etiopských bankách a první práce zaměřená na tuto oblast. Výsledky odhalily, že banky nemají uspokojivou implementaci činností před incidenty, včetně nástrojů pro detekci incidentů a varování. Nejdůležitější zjištění týkající se nesprávného výkonu definované architektury informačního systému a zacházení s daty, včetně správy incidentů, jsou pozorována, jako by existovaly dobré postupy pro implementaci moderních monitorovacích nástrojů a časté revize nezbytných pracovních pomůcek a dokumentů. Očekává se také od bank, že budou maximalizovat schopnost Network Forensic Readiness, pracovat na rozdílech v povědomí a rozvíjet dovednosti zaměstnanců, správnou identifikaci zdroje digitálních důkazů a nastavit schopnost analýzy údajů před nehodou.a představil model. Thi s byl také podporován dalšími souvisejícími studiemi.

Klíčová slova: Digitální forenzní, Síť forenzní, Síťová forenzní připravenost, potenciální digitální důkazy, Mezinárodní organizace pro normy, Systém detekce narušení, Průzkum údajů

Table of content

List of figures

List of tables

List of abbreviations

DF	Digital Forensic
DFR	Digital Forensic Readiness
NFR	Network Forensic Readiness
PDE	Potential Digital Evidence
ISO/IEC	International organisation for standardization/International Electro technical commission.
IDS	Intrusion Detection System
SIEM	Security Information and Event Management Software
IMS	Incident Management Systems
INSA	Information Network Security Agency
NISS	National Intelligence and Security Service
Ethio-CERT	Ethiopian Cyber Emergency Readiness and Response Team.

1. Introduction

Digital Forensic (DF) is essentially collecting digital evidence after an incident following the proper way of data preservation and analysis. The DF process is not only for the analysing step. Still, it stretches to the presentation process, too, since the DF investigator needs to present the output to the court of law as evidence. So we can see that it is a post-incident activity. Still, another step is useful for organizations to minimize the cost of investment on the investigation, which is called Digital forensic readiness (DFR).

The DFR is a pre-incident preparation to tackle an incident and keep the attackers' trace as a log file that helps to find out the evidence. Organizational Potential digital evidence (PDE) recognition, preparing pre-incident operation, implementing the pre-incident activity, and assessing the implemented mechanism to achieve the DFR are essential processes in fulfilling the readiness. Basically, DFR is introduced to maximize an organization's capability after an incident has happened, to conduct DF and reduce the cost of an investigation.

We cannot perceive Cyber security and DFR separately. In this research, we are primarily interested in the Network Forensic Readiness (NFR). It is all about increasing the network's quality by sniffing every traffic and capturing evidence from packets in the network; this helps the investigator identify the attacks from an internal or external source of an organization. Since cyber security is also about ensuring cyberspace from attacks, we cannot see these two concepts separately because one is an input for the other.

An organization needs a coordinated cyber security plan for adequate cyber security, so NFR should be included in those organizations' plans to achieve the confidentiality, availability, and integrity of a cyber-systems and secure the criminal's time in front of the law. In addition to that, the NFR monitoring tools can be considered as an asset for organizations to detect and respond to attacks on time.

The banking industry can be called a major challenge in cyber security, and a lot of attacks these days are targeting the business. This research is conducted on Ethiopian banks to evaluate how capable they are of the DF process and how to maximize their ability of collecting digital evidence while minimize the investigation cost after an incident if the PDE source is identified.

This research is carried out on Ethiopian Banks NFR, a case study using a qualitative method in which the advanced usage of NFR for the financial network specifies Ethiopian banks. As the idea is deep and needs further investigation, an interview with four professionals has been done. The interview questions were adapted from the ISO/IEC 27043 standard. The targeted online survey interviewees were with the information technology professionals who work on those banks' IT security areas and two- person from one bank has been used, the first one is the lead of the department and the second person is the incident management team's leader to achieve a good output and study the current practices and suggest the feed backs to maximize the ability to collect valid digital evidence and minimize the cost of NF during an incident in those banks.

The overall study addresses the case study of Ethiopian banks on readiness before any incident has been occurred and cover what kind of practices are observed and what should be done to achieve the NFR of those banks.

2. Objective and Methodology

2.1 Objective(s)

General Objective

General objective of this research is to analysis and study how to maximize the ability to collect valid digital evidence and minimize the cost of Network forensics during an incident.

Specific Objective

- Perform a cost-benefit analysis to determine if implementing network forensic readiness is valuable to the organization.
- How capable the organization is to collect, preserve, protect and analyse digital evidence.
- How much Network Forensic Readiness is necessary for the organization and what it used for?
- Evaluate how much the evidences from network forensic are helpful in legal matter and court of low.

2.2 Methodology

To fulfil the objectives, there will be literature studies used and also analyse the information gathered from the organisations. Also, use the forensic readiness policies and ISO standards for national forensic analysis as a reference is expected.

Research Approach

A qualitative method is sustained to spout the research objectives because qualitative research is used for small samples, while the outcomes cannot be measured or quantified. It offers a complete description and analysis.

Data collection Method

From the qualitative data collection methods, online surveys and Google meet interviews were used to get richer and have a deeper insight into the subject of this research. The interview questions were adapted from the Information technology Security techniques Incident investigation principles and processes ISO/IEC 27043 standard. After conducting the interview internal reports regarding the NFR practices were required but due to Banks security reason it was not possible to access the data.

Data source

The purposive sampling approach was used to choose the source of the data. The samples were selected based on their experience and knowledge regarding the research subject. The research's targeted group was IT professionals who work on those banks' security areas at the head offices since the practices observed on the bank's main branch are applicable for the sub-branches. To achieve a good output. The participants for the research on the virtual interview were 2 Bank IT department Mangers at different banks and 2 digital forensic analysts in Ethiopia.

Data analysis

The Data was obtained and analysed using a statistical tool, and the results of the data are accurate to represent the specified output. A Frame work also done using draw.io.

3. Literature Review

This section presents document studies and knowledge concerning Digital forensic Readiness and details on network forensic Readiness by analysing the financial Network's challenges according to cyber security.

This section will also discuss and analyse the existing DFR resources, Ethiopia's digital world growth, and the country's current level of cybercrime. The influence of DF in the region, as well as the legal and policy frameworks that underpin our research, will be discussed, followed by the current state of NFR in Ethiopian banks, as determined by studies, and finally, an overview of other countries' organizational forensic readiness practices and related works will be discussed.

3.1 Overview of Digital Forensic

At this time, the world faces many cybercrimes and other digital crimes, so our initial thoughts go directly to solving this problem. The professionals need to collect digital evidence; this process includes identifying the problem, preserving the situation, and analysing and presenting the digital proof; this is commonly known as digital forensics (ISACA, 2017).

According to ISO/IEC 27043:2015(E), it is necessary to investigate digital evidence whenever an incident occurs and applies to any digital device. Digital investigation process classes are applicable to conduct DF at a higher level (ISO/IEC, 2015).

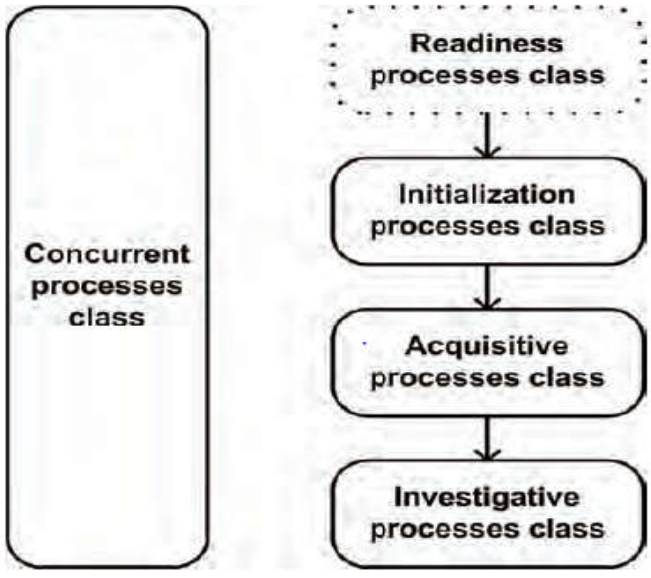

Figure 3. 1 Classes of digital investigation processes (ISO/IEC, 2015)

The readiness process class deals with the pre-incident investigation process, and the author will explain the readiness process class in the next chapter. In contrast, the initialization process class deals with a digital investigation like incident detection, planning, first response, and preparation. Acquisitive processes are all about the physical exploration of the case where digital evidence identification, acquisition, transportation, and storage taking the place of the investigative procedures follow, including evidence examination, analysis, interpretation, reporting, presentation, and finally closing the case. The concurrent processes are about the documentation, the chain of custody, and other interactions with the investigations (ISO/IEC, 2015).

Even though Computer forensic relates to retrieving missing data from computers, DF, also known as Computer forensic, was introduced to the world in the 1970s (Pui Chow & Shenoi, 2010). Digital forensics has become a well-known and widely used science practically applied to recover lost data from digital devices due accidentally, purposely, or because of some incident that happed in organizations and using the data for investigation (Watson & Jones, 2013).

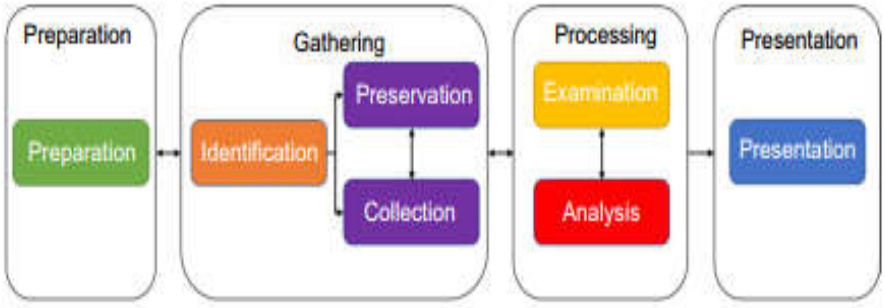

Figure 3. 2 High level of DF process model (Jason & Ivtchenko, 2016)

Digital Evidence is similar to any other shreds of evidence in many ways. To be admitted in a court of law, DF had to be accessed lawfully, relevant, complete, reliable, authentic, accurate, and believable. Digital evidence potentially differs from other evidence as it can be easily changed during an investigation, Duplicated quickly with copies, and change the structure of data due transfer (Watson & Jones, 2013, pp. 5-9). It is crucial to check whether the whole process follows the proper ways, and it is essential to seek advice if there is uncertainty in the specific jurisdiction.

From all the DF process's preparation stapes, the primary and basic one leads to where to begin and the direction to go. All the time in the process of investigation sustains the chain of custody. It is vital to record every step of the investigation, tools used, and the procedure to follow. Sadly many failures are caused in the court of law because of improper understanding of digital forensic investigation.

In the collection phase, searching of data and the grabbing must be compatible with the law. It is essential to exercise caution on the techniques used with the packing of data, investigation tools, and the evidence's transportation. The second phase is preserving the data. There must not be any change to the evidence; rather, evidence should be as similar as the original one, but if there is any change, it must be documented accordingly for audit. The preserved data will be analysed to get the appropriate information and recreate the chain of events in the analysis phase. In the presentation phase, it is crucial to present the evidence that considers the audience since the presentation should include every detail of the communication between the forensic analyst and the investigator (Watson & Jones, 2013, pp. 8-10).

DF's primary objective was to investigate a crime carryout by computers; the specialty has stretch and includes various devices that handle digitally stored data like mobile devices, networks, and virtual storage as the cloud. To carry out digital inquiry, the data should follow authenticity and integrity; in addition to that, an individual should know how computers, mobile devices, and Networks work to investigate this digital device (Sachowski, 2019).

Different DF processes used from those Computer forensic, Mobile forensics, Network forensics, and cloud forensics are widely known (Evans, 2020).

Computer Forensics

Computer evidence is used more prevalently in civil and criminal cases. From all investigations, Computer forensics is the first and foundation of all forensic types. Nowadays, it primarily deals with hard drive evidence, proving a case, and memories if there is any leftover from the attacker.

"*The examination of digital data from a computer's storage medium, either the traditional hard drive or the Solid State Drive*." (Reiber, 2019)

Compute's may be used on their own to hack a network which means without a computer the crimes like DDOS cannot be possible, and Computers usually store evidence of civil crimes like murder or drug dealing (Free Training, 2017).

The search warrant limits a forensic investigator at the beginning of the investigation. Without a warranty, the collected evidence has no value. Even with the warrant, the searching should be specific. The acquiring of evidence is handled using forensic software's which takes a bit by bit copy of the suspects' media drive. The evidence-driven should not be in a lettered form to avoid evidence corruption, and we shouldn't touch the actual evidence unless critical situations happened. To check whether the drives are identical, we can use methods like Hash algorithm (Watson & Jones, 2013).

Preserving the evidence on computer forensics is avoiding the corruption of the original device, which is the computer drive and transport, store, and handle the device from the crime sine to the court properly then analyse the evidence from the actual source using forensic tools (Watson & Jones, 2013).

Mobile Forensics

Mobile forensics is all about gathering and analysis of digital data from mobile devices. The number of mobile devices in the world is currently more than the population, so mobile device forensics has become the most rapidly advancing discipline that digital forensics has ever seen or will see because of the actual device's rapidly changing environment. Mobile device data today is almost equivalent to yesterday's DNA results, which shows how the pieces of evidence from mobile devices are critical.

Due to mobile devices' investigation, the seizure must follow a search warrant's using legal way; if not, the legality of the data obtained will be in question, and the collected information can't proceed. In contrast, in the data collection, the person conducting the process has to take immense care of the electronic fingerprints to make them stay as they were collected and not lose data on the volatile memories.

Analysis of the data will proceed after the collection, and it takes much more time than the other forensic steps. On the analysis, the responsible person should document every information to present in a written report (Reiber, 2019).

"*The successful examination of digital evidence from a mobile device requires an intimate understanding of the data, and not the medium that produced it. To be a truly good forensic practitioner, the examiner must understand the specimen."* (Reiber, 2019)

Network Forensics

Increasing the number of IT users have a higher impact on Network traffics and incidents. Monitoring and analysis of Network traffic for information and digital evidence gathering or intrusion detection become a core and basic idea at this time. Organizations are giving attention to Network and data security due to many attacks on many companies frequently.

Network forensics relates to network attacks and consents to digital evidence in the network traffic after the suspected event and addresses the complete occurrence of seizures and their consequences in the Network (Khan, Gani, Abdul Wahad, Shiraz, & Ahmad , 2016). NF is constantly being investigated, but it appears that many details have yet to be clarified, and it is still a young science with many unanswered questions.

Coming to the network world, attacks damage networks and systems. Denial of service, vulnerability exploits, insider threats, external threats, the hybrid of the internal and external, evasion and application attacks are from the frequently listed attack technics in recent years, so having an incident management team is a smart idea even if the organization is small, but attacks are not usually hard to spot on if the responsible person is aware of the area to look for (Messier, 2017, pp. 114-141). The NF helps find the attack source, as the devices and stop the virus or malware to enhance network performance and then manage network flow.

persepting the networks investigation as a physical environment identify the physical and logical topologies, identify outside network connections such as partner organizations, understand whether an outside server room supports the Network or they have a cloud service provider outside the country, acquire the current network diagram, identify log generating devices, Identify the critical systems run as imitating OS on a dedicated server or as virtual machines and check the proxy servers also firewalls which might have logs stored are the primary step that a NF investigator should follow on an investigation (Anson, Bunting, Johnson, & Pearson, 2012, pp. 6-23).

Like other legal investigations, NF needs to present proof plus correct evidence in front of the court, and the evidence maintained in its original manner. It is necessary to produce similar evidence at the end as initially, but this is a little bit challenging when we come to network forensics. Hence, the chain of custody documentation is essential. Mostly in NF investigative Scenario and investigative method is unique, so the investigator should find their way of analysis and determine their approach.

Different types of network forensic technics used to make our investigation easier. Every single packet and event recorded to facilitate every search spread into the Network (Khan, Gani, Abdul Wahad, Shiraz, & Ahmad , 2016).

Cloud Forensics

Since virtualization is so cost-effective, it has become the most important way to run computer systems and infrastructure. Many companies are struggling as a result of the prevailing business climate transitioning to the cloud. However, information security is the primary concern for every business.

"Cloud is an emerging technology moreover cloud-based storage is a relatively new concept that enables users to not just upload data to the network but also to access to available resources and share data with anyone at any point of time." (Dhumal & Rokade, 2020)

The basic characteristics of cloud computing are on demand self-service which is free from human interaction on the service provided, client's access on several platforms, the rapid elasticity of the plat form, cloud systems automatically measure services and resources provided to several consumers at a time (Herman, et al., 2020).

Investigating a cloud platform is a difficult task to complete since data stored on clouds can be accessed from any system, computer, or location, leaving few traces behind. The arrangement joining the causality and the service giver governs data collection and access to log files.

The collection and review of digital evidence from cloud storage systems is referred to as cloud forensics. Antimalware lists virtual machine introspection as a way to detect attacks on virtual machines where the intrusion detection mechanism is located outside the host for better attack resistance. Digital prevention is used in cloud forensics to explain the history of the digital entity, and then logs are used to check the behaviour on the cloud. Taking snapshots of events is another common method of obtaining digital proof (Dhumal & Rokade, 2020).

3.2 Digital Forensic Readiness

The concept of forensic readiness was first introduced in 2001 by John Tan. In the forensic readiness program, Tan underlined that organizations' primary objectives are to maximize the ability to collect credible digital evidence and minimize the cost of forensics during an event or incident (Sachowski, 2019, p. 80).

The main goal of digital forensic readiness is to minimize the effort required for an investigation to sustain the reliability of digital evidence collected and reduce the effort includes maintaining the time and cost of incident response (Pui Chow & Shenoi, 2010, p. 110). The time spent by the intruders is much smaller compared to time spent to clean up the mess after them, so Organizations need to develop the ability to respond rapidly using forensic readiness to save time and money. Having digital forensic capabilities, organizations can easily find out what happened, how and by whom.

''Forensic readiness assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature'' (ISO/IEC, 2015).

Organizational goals for implementing DFR processes (ISO/IEC, 2015):

- Increase the potential use of digital evidence;
- Reduce forensic costs imposed directly on the organization's system or in relation to the system's services;
- Reduce interaction with organisations and avoid disruption of business processes;
- Maintain or increase the existing level of information protection of systems throughout the organization.

DF strategy is designed differently from one company to another depending on its forensic objectives (Elyas, Ahmad, Maynard, & Lonie, 2015). Other than forensic strategy, organizations should consider the cost and benefit of digital forensic readiness before implementation. Cost analysis of forensic readiness includes technical, administrative, and practical information security costs, whereas benefit analysis addresses the organization's overall benefit using forensic readiness (Sachowski, 2019, pp. 82-85).

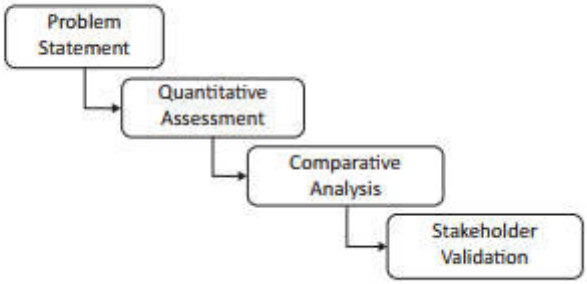

Figure 3. 3 Cost-benefit analysis window (Sachowski, 2019, p. 302)

The problem statement includes the core idea and documentation of why the cost-benefit analysis is needed then generates all feasible solutions on the cost-benefit analysis workflow. After the problem statement is registered, organizations need to invest their time in identifying all keys at the Quantitative Assessment level and pointing out their tangible and intangible costs to clarify project benefits (Sachowski, 2019, pp. 301-304).

The comparative assessment is done on the present values of the cost and benefit, so current values should be calculated and used as a criterion for identifying which alternative provides the best return in investment. Reducing the expected value is essential for organizations to concentrate on the existing matters and consider the possible cost. Calculating the gap between the baseline scenario and the proposed scenario helps to know how ideal is the benefits gap to finalize and communicate with the stakeholders whether the positive or negative impact is the outcome (Sachowski, 2019, pp. 305-312).

Evidence preservation and time to execute the evidence are affected by logging, ways that the logging performed, intrusion detection system (IDS), evidence handling, and forensic acquisition (Tan, 2001). Time synchronization impacts when we log from different devices because without synchronized time, the reporting will have wrong results.

The central logging server should time stamp all records with a consistent time frame for the evidence to be convincing using the NTP GPS receiver (Tan, 2001). According to experts' perspective in focus group desiccation, a new model was introduced, which can be used by organizations to estimate their forensic readiness. Those specialists underlined the organization's size plus limited resources cannot be a cause for not being forensically ready.

The frame work suggests top managers and governance leadership commitment toward forensics, staff awareness and commitment toward forensics, organizational structure that take forensics in to considerations, enforcement of forensic policy and training, accountability of

staffs towards their forensics responsibilities, active monitoring and continuous assessment of system activities (Elyas, Ahmad, Maynard, & Lonie, 2015).

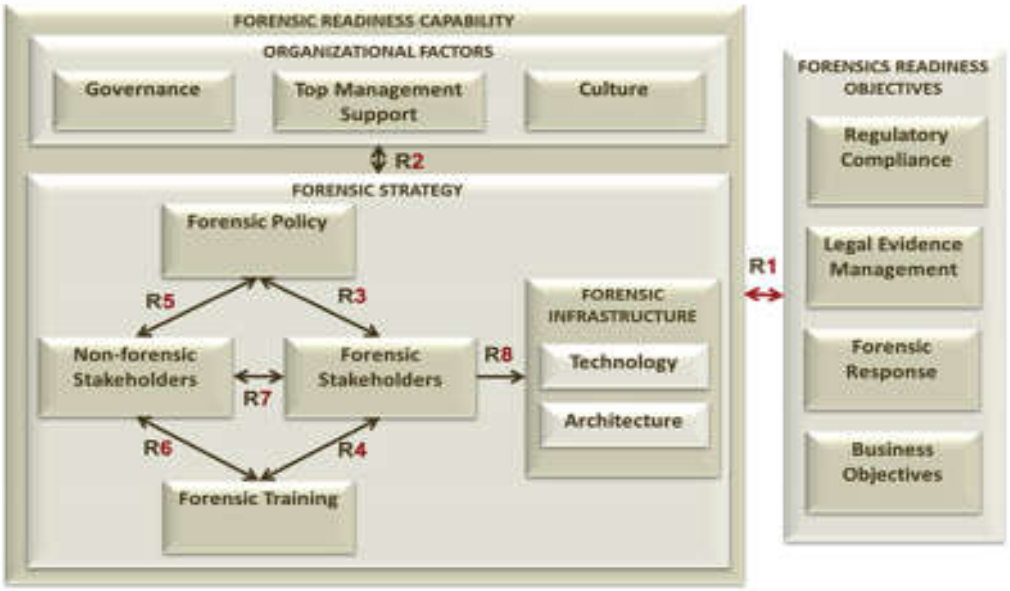

Figure 3. 4 The DFR frame work (Elyas, Ahmad, Maynard, & Lonie, 2015, p. 78)

The framework shows how properly an organization manages digital evidence and forensically responds to an incident using its forensic readiness. Forensic stakeholders are those who are accountable for giving training, policy making, and other critical forensic performances, whereas non-forensic stakeholders require to develop awareness to behave in a way that helps them to respond to an incident; hence anyone in the organization can be the first responders and should comply with the policy.

If an organization deploys DFR it will be considered a natural progression with matured information security posture, and it will offer a second line of defence to information security measures and support organizations when other security measures have failed (Danielsson & Tjøstheim, 2004). To implement DFR there are processes that we followed to build the digital investigation process easier.

3.2.1 Digital forensic Readiness processes

The process is a severe action that is taken to achieve a particular goal. When we come to DFR processes, this includes the procedures taken to facilitate the quality of a piece of digital evidence and maximize the environment's potential to provide valid digital evidence. As we can see from the figure, three DFR process groups are the planning, implementation, and assessment process groups (ISO/IEC, 2015).

1. Planning process Group

This process group defined as making up one's mind about what to do when to do it, how to do it, and who will do the activity. The DFR planning process group begins from defining the scenario and then continues with identifying the evidence sources, then planning pre-incident collection, storage, and handling of data plus the pre-incident analysis and defining the system architecture (ISO/IEC, 2015). Once the system architecture is customized to meet DFR requirements, the implementation process will continue.

1.1 *Scenario definition process*

In the scenario definition process, all the probability of the digital evidence occurrence should define; furthermore, the outline is used as an output. The risk assessment is fundamental for every scenario because it leads us to identify the possible vulnerabilities and threats that might expose information assets. Following the defined process, organizations can do the cost-benefit analysis and manage the risk level as things will be simple to reduce risks.

1.2 *Identification of PDE sources process*

Identification of PDE source can be taken place here, and output might not be available in situations like when clarification of access logs is missed as a data source for digital investigation, so this process helps explore controls that will make identified sources accessible.

1.3 *Planning pre-incident gathering, storage, and handling of data representing the PDE process*

In this process, the identification of pre-incident gathering based on the risk assessment, storage, and handling can be taken place. These processes are essential in front of the law and help us to make the evidence acceptable, so it is advisable to take the previous experience on incident detection and other related factors that might impact the efficiency of the process.

1.4 *Planning pre-incident analysis of data representing PDE process*

Procedures for the pre-incident analysis of data representing PDE are defined here. This process is focused on detecting an incident; hence activities in this process should include how an incident is identified and the behaviours that compose an incident.

1.5 *Planning incident detection process*

In this process, we need to define the actions that we carry out when an incident is detected. Defined activities to be performed when an incident is detected are considered as the output of this process.

1.6 *Defining system architecture process*

In this process, the design of an information system or an information system's organizational structure is defined considering all DFR processes' output results. Input to this process is the result and aim of previous DFR processes.

2. Implementation process Group

The definition of implementation is the action that follows the preliminary thinking of a specified plan for the visible part to happen. This process group states the implementation of the planning process groups. All the planned processes should implement accordingly, and the organization or the service provider will take the role to take responsibility.

2.1 *Implementing system architecture*

In this process, the defined system architecture on the defining system architecture process will be implemented. One will have implemented system architecture as output.

2.2 *Implementing pre-incident gathering, storage, and handling of data representing PDE process*

In this process, the planned pre-incident gathering, storage, and handling of data representing PDE will be implemented.

2.3 *Implementing pre-incident analysis of data representing potential digital evidence process*

The implementation will take place as described in the planning pre-incident analysis of data representing PDE. This process will provide a feed for incident detection.

2.4 *Implementing incident detection process*

In this process, the defined actions on the planning incident detection process will be implemented, and we can consider this process as an overlap between the readiness process and the investigation taken place since investigation can't start until an incident detected.

3. Assessment process Group

The assessment process group is concerned about gathering information from the planning process group and the implementation process group and discussing the diversified sources to develop DFR for the organization or the service provider and implement the needed improvements stated on the assessment.

2.5 *Assessment of implementation process*

In this process, the results from the implementation process group are assessed then compare the results to achieve DFR. The results of the assessment of implementing DFR for the information system are the output. In this process, all the architectures, procedures, and controls should be reviewed and revised considering the legal environment. The principles for digital forensics should be visible to increase the admissibility of digital evidence in the court of law.

3.2 *Implementation of assessment results process*

This process is all about the assurance of assessment of implementation process, and it is not mandatory; hence no changes are needed that we can observe from implementation process assessment. The improvement might also be required on the planning or implementation process groups based on the evaluation, so the decision on changes is mandatory**.**

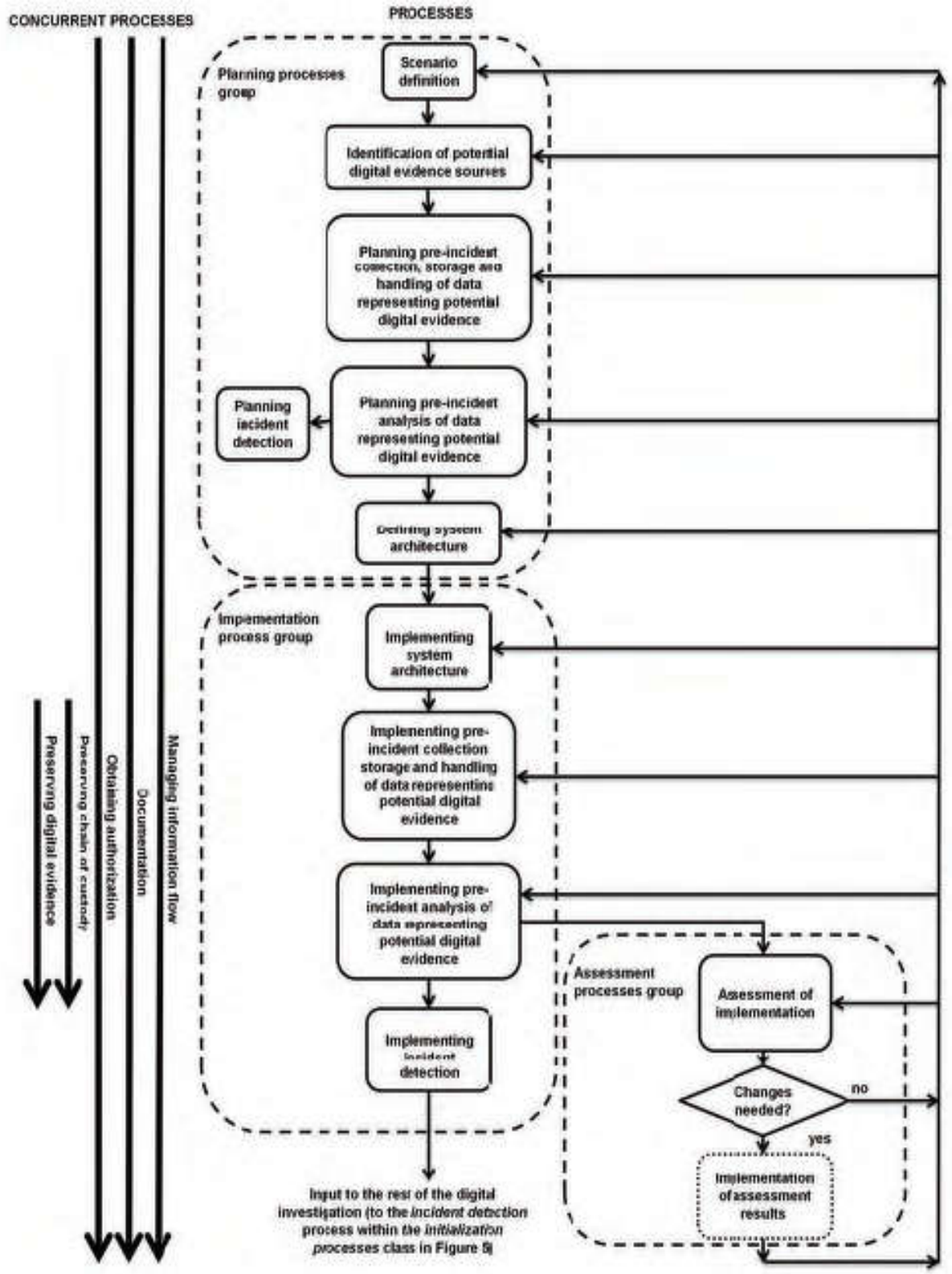

Figure 3. 5 DFR processes (ISO/IEC, 2015)

3.2.2 Network Forensic Readiness

There are many challenges faced at this time on network forensic investigation; from those challenges, lack of funding or lack of finance, lack of qualified professionals, and juridical struggles can be listed from main issues. To combat new cybercrime methods, customizable aspects of data security both for wired and wireless networks is indeed a task which is continually finding tough to accomplish.

Networks face vulnerabilities like a natural disaster, physical security vulnerability, inferior network design and targeted vulnerability like malicious software's attack, and some protocol and application vulnerabilities. Designing the proper policy and procedures is essential to protect the Network from any problem, making the Network vulnerable to attack.

Post-mortem forensics (forensics executed after an incident) is not viable. Hence, a more provident approach is needed to identify and possibly obtain evidence from a system network. The integration of Network forensic readiness into an organization can potentially provide a higher probability of decrypting attacks on the system network and provide critical evidence about the attack.

"Potential sources for incident data are the victim system, the attacking system, Logs and physical securities at attacking systems" (Tan, 2001).

The NFR main goal is preparing organizations to Network to catch some evidence if an incident occurs. We can quickly answer questions like who did it, the gain and loss of the attack, in which part of the organization device, assess the incident's timing and life span, and provide the best solutions quickly. The answer for NF caught from the network wires and the physical connection, from the virtual sources like the wireless Network, from the switches looking at the Mack addresses, from the security appliances like firewall logs plus IDS/IPS logs, from network infrastructure services like DHCP and DNS logs, from the routers routing table, from overall system logs, proxy and authentication server logs (Tan, 2001). The criminal will leave some evidence behind on one of the above devices or infrastructures, so identifying the primary digital footprints easily is the core idea; hence, data traces will be applicable easily if the service provider is ready for network forensic investigation.

These days' malware-based cybercrimes are increasing, and they are factors for the problems happening on the Network. Trojan, spyware, worms, adware, botnets, rootkits, and more recently, ransomware exist commonly known as those viruses. Through time malware have changed their adoptive techniques as Polymorphism which means changing the structure without changing its shape, Metamorphism which is rewriting the malware in a way that it is difficult to identify and Obfuscation the act of malware impersonating a file archive (Breitinger & Baggili, 2018, p. 93). Those malwares can easily make the Network available for informal traffic flow.

Inside different packets of the network forged information is used by malicious attacks, in IP address, in port numbers and TCP flags. Some of the attacks as IP spoofing are based on spoofed IP address which enable the intruder a trusted one so it is easy to make communication to the victim node. The intruder can also insert source IP address and destination IP address of the casualty and lead the casualty to self-connection loop attempts using land attack (Khan, Gani, Abdul Wahad, Shiraz, & Ahmad , 2016).

Kaspersky Security Bulletin 2020 Statistics shows that from November 2019 to October 2020, there were 26,700 ransomware modifications, and those 21 were new families (Statistics, 2020). We can observe that how those attacks are the fastest and wide-spreading. DFR framework for ransomware investigation was introduced based on the ISO/IEC 27043 standard, and the process of the model begins from identifying digital evidence from the Network and then extract the proof from the Network like windows registry as if it points out the location of the malware and RAM because ransomware leaves traces (Breitinger & Baggili, 2018).

The database management system is also needed; hence it is used lately for investigators as the extracted file's origin. It goes to the phase that logs all activity, ensuring chain of custody (Breitinger & Baggili, 2018).

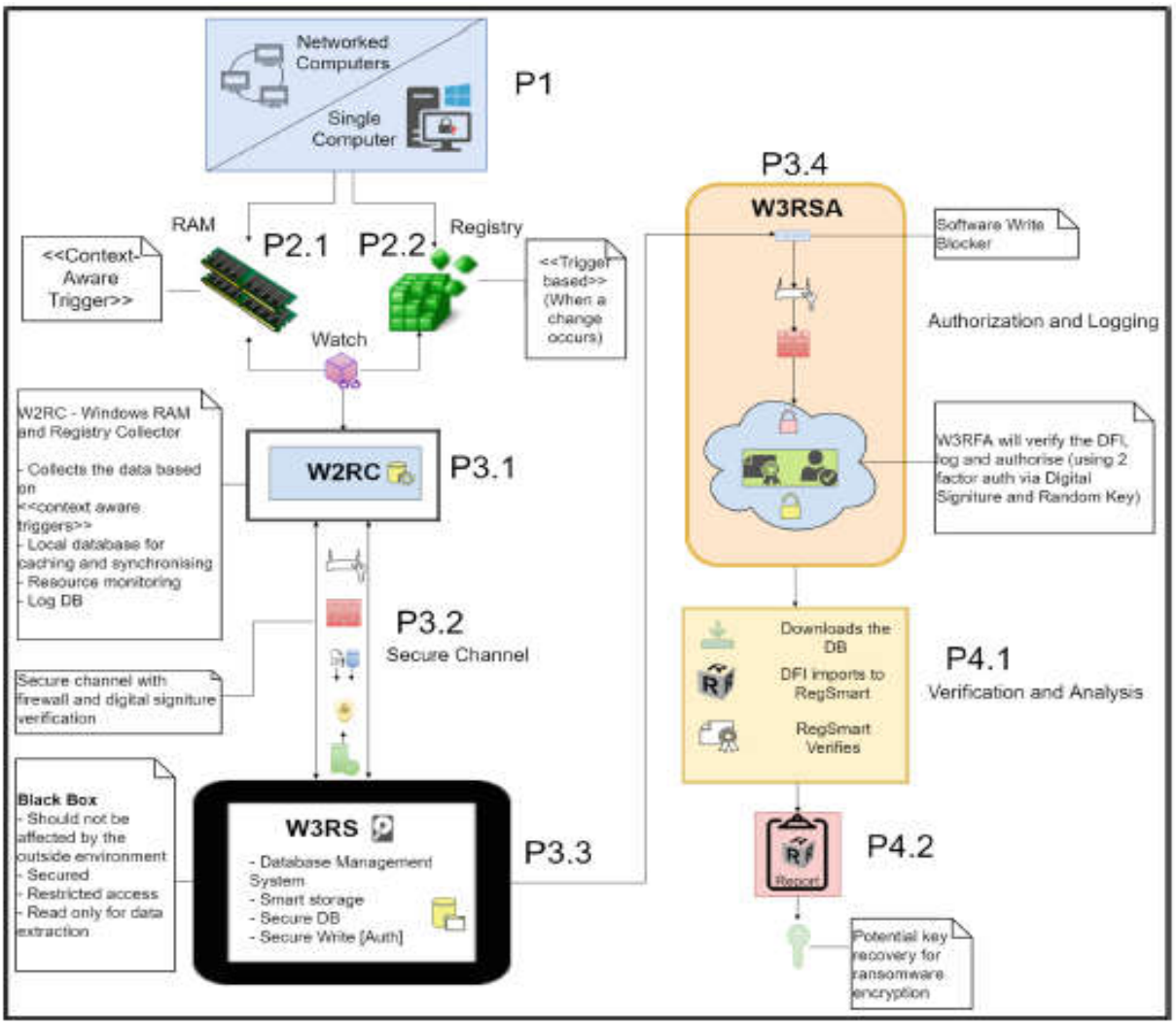

Figure 3. 6 DFR framework for ransomware investigation (Breitinger & Baggili, 2018)

In addition to Malwares there are a lot of attacks frequently happening on the network and wireless local area networks are the main target of the attacker's hens the number of users for the previous years have been spread throughout the world vastly.

3.3 Most popular tools used for DFR

There is no tool decided entirely to manage DFR. Therefore the author tries to cover related tools. The addressed tools are not agreed upon for forensic readiness but used for related work. The security event management software, intrusion detection systems, and incident management systems are sprightly pertaining to the management of DFR (Masvosvere, 2019).

Intrusion detection system (IDS)

The intrusion detection system (IDS) enables the administrators to monitor the events by alerting when a possible incident is approaching (Frincke & Popovsky1, 2007). They learned known intrusion scenarios or unusual behaviours or signatures so quickly identify new issues and provide them to the professionals on the place. IDS needs humans to handle some matters, but it is limited to authorized professional users; if not, the evidence might corrupt.

Security Information and Event Management software (SIEM)

SIEM is a system that collects log files, security alerts, and events in one place so security teams can analyse data easily. SIEM can be seen as a log management system specialized for security. All information from other security systems like endpoint security, firewalls, and IDS will collect here; hence it is a central system. Centralized log data is much easier to secure, backup, and easier to acquire for analysis (Tan, 2001).

Reddy listed Common functions performed by SIEM's (k & H.S, 2012).

- Log strengthening. Gathering all logs from the origin to the server.
- Threat correlation. To identify attackers or threats, artificial intelligence is applied to sort multiple logs and log entries to identify attackers or threats.
- Incident Management. What happens when an incident occurs is defined at workflow. Incident management includes notification during an incident, incident ticket creation, automated responses, and remediation logging.
- Reporting. Reports generation to underline the operational efficiency and effectiveness of SIEM's.

Incident management systems

Incident is any event occurred on the IT service of an organization which causes unplanned interruption to the quality of the service. Therefore IMS is basic to minimize the impact and restore the service to normal state. The IMS is the easiest way to identify weather the organization is impacted.

The incident management system facilitates incident detection, classification, analysis, and recovery by controlling the workflow in the incident management process (k & H.S, 2012). The software contains incident records, escalation rules, and information about end-users, customers, and configuration items. The incident management systems deal with IT incidents, and it is the organization's interest to choose IT-based or IS-based approaches (k & H.S, 2012).

3.4 Ethiopia and the Internet

Our world's total population is steadily growing, and Ethiopia is the second populated country in Africa. According to digital around the world's report, the total population of Ethiopia in 2020 becomes 113.5 million, and from those 46.75 million have mobile phone connections; this shows the number of mobile users has been increased by 18% from the previous year, with 21.14 million internet users and 6.20 million active social media users (S.KEMP, 2020).

Even if the number of internet users is small according to the population, internet coverage in the country is hastily growing. A high effort is applying to increase the internet connectivity coverage and speed of access; thus, the amount of people who use the internet has grown by 2.6% from Jan 2019 to Jan 2020 (S.KEMP, 2020).

Nowadays the internet coverage is increasing, and more people are connecting from year to year. ICT infrastructures and telecom infrastructures are in place in most of the country's geographic area. Since there is a huge potential user, huge investments made, and Ethiopia will become the ICT hub of Africa through time.

The following diagram shows the increasing number of internet subscribers to Ethio telecom from 2011- 2019. This can be an indicator of internet penetration rate growth in the country since Ethio telecom is the only internet provider.

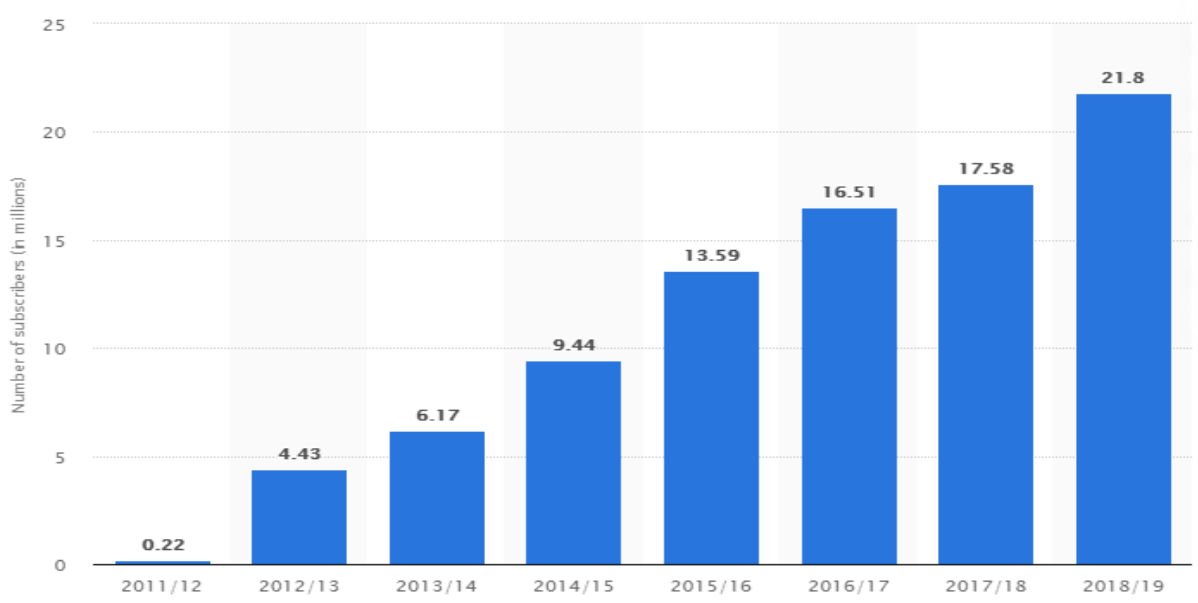

Figure 3. 7 Ethio telecom internet subscription rate (S.O'Dea, 2020)

As the country is working to improve the quality of international internet bandwidth now, there is a huge improvement. Reports are showing it is much better than many other African countries. The government is trying to promote ICT services, so it has adopted an E-Government strategy in 2010. As the infrastructure vastly expands, computer networks become the nervous system, and every bank and financial sector embarrassed the ICT (Hailu, 2015).

Growth and Transformation Plan I (GTP I), from the years 2010/11-2014/15 was first introduced by the Ethiopian government for the first time in 2010 (Commission, 2016). In those five years, the priority was the quality and development of infrastructure. As a result, the number of telecom services customers increased from 7.7 million in 2009/10 to 39.8 million by 2014/15 (Commission, 2016). Mobile users increased from 6.7 million in 2009/10 to 38.8 million by 2014/15. Telecom services are available on rural areas within 5km radius increased to 97% by 2014/15 from 62.1% in 2009/10 (Commission, 2016). The other significant achievement is the introduction of 3.75G and 4G internet networks with service capacity of 60 million customers (Commission, 2016). Within the period of Growth and Transformation Plan II (GTP II) which is from 2015/16-2019/20 the government of Ethiopia strategic direction was to enhance ICT infrastructure and human development, development of Industries and privet sectors and develop government administration in ICT (Commission, 2016).

From the resent achievements of the technology in Ethiopia artificial intelligence and robotics center of excellence and cyber intelligence centres can be mentioned. Hence government and highest educational organizations are working on it.

The development of internet penetration and the increasing number of users in Ethiopia is beneficial but has consequences without the majority's awareness and knowledge. Since IT is new for most users, the exposer of the platform for cyber-crimes is high. In addition to lack of understanding on internet users, the way that Ethiopia's government handles most IT sectors including telecom provider, and high-security organizations make a gap on defending the attacks carelessly and irresponsibly since there is no competition in the market.

3.5 Ethiopia and Cyber-crime

Poor cyber security governance, inadequate legal framework, and lack of awareness are Ethiopia's challenges, making organizations exposed to attacks. The minister of peace in the country mentioned that organizations and every citizen are highly vulnerable to cyber-attacks globally, and the government is prepared to provide all required inputs and technical assistance in the fight against cyber-attacks (Woldemichael , 2020).

According to Kaspersky analysis Ethiopia is listed from countries where users face a higher risk of local inflations where data includes malicious programs on computers or removable media such as phone memory cards, flash drives, external hard drives, plus cameras. The level of infected personal Computer in Ethiopia is 55.08 % from November 2018-October 2019, and during this time, Ethiopia was listed as a top 10 country affected by a crypto-ransomware attack (lab, 2019).

During the past three years, cyber-attacks has been increased from 479 and 576 to 791 from year to year in Ethiopia, from those attempts, 15% of them were during the period 2018/2019 and are cyber hacking attempts (Woldemichael , 2020).

Studies show that most of the attacks are on the country's financial sector, and they have high consequences and impact according to the country's economy. Furthermore, website and infrastructural attacks were standard, but INSA claimed they were all stopped before causing significant damage. Concerning this reality, this paper will try to address the awareness towards the readiness of network attacks and the forensic process after an incident has been carried out hens almost all cyber-attacks are targeting the Network.

In the year 2020, Egyptian hackers have tried a cyber-attack on Ethiopia's governmental websites because of the political stress between the countries on the great Ethiopian renaissance dam built on the Nile River. It is not certain that the hackers are connected with the government of Egypt, but messages on the web pages that refer declare war if the river minimizes its quantity and some images with Egypt's Pharaoh (Nlar, 2021).

Besides the attacks on Ethiopian financial, governmental, and non-governmental organizations from outsiders, research from the citizen's lab show attacks was carried out by Ethiopian government since 2016 on political opponents, and US-based journalists abroad and the attacks were also Targeting Eritrean organizations; Spywares like Cyber bit's PSS and Hacking Team's RCS Were used (Marczak, Alexander, Mckune, Deibert, & Scott, 2017).

The study by Adane stated that Ethiopia has no standardized cyber security framework, governance, and strategy at the national level while organizations are trying to have a framework of their type, but that is not effective, and some local researchers are developing cyber strategies and frameworks for banks and other organizations however those frameworks are not strictly tested, and their effectiveness is in question (Adane, 2020).

Ethiopia's government introduced a national information policy in 2011 to fight against cybercrime, a base for many cybercrime laws, E-commerce, E-signature, and telecom fraud. Cyber-attacks are not a possibility of future Ethiopia, but it is a reality that is happening. With more people logging online every day, the risk of being prey to cyber criminals keeps increasing and needs a comprehensive response.

Importance of NFR in Ethiopia

Studies show the attacks on governmental organizations in Africa are increasing, and the organizations' ability to respond to the attacks is insufficient; in addition to that, the preparation regarding the cyber investigation and cyber warfare is also small (Marczak, Alexander, Mckune, Deibert, & Scott, 2017).

According to political stress in Africa, the growing number of cyber-attacks is viewed as a simple issue; instead, countries must concentrate on strengthening their national cyber strategies and policies. Cyber-attacks as a means of warfare have recently been observed in various countries, and it will undoubtedly increase rather than decrease, necessitating the community of cyber-readiness.

Cyber experts in Ethiopia also mentioned Ethiopia needs to create a well-organized legal strategy to deal with the rising number of cyber-attacks on a national level since around 87.4 percent of the government agencies don't even have any accepted legal mechanisms in place to deal with cyber-attacks, while 11.6 percent are in the trial phase (Woldemichael , 2020).

Several indicators show how much attention should be paid to the country's Readiness process to combat cyber-attacks in the financial sectors.

3.6 Institutional setup on Cyber security and NF investigation in Ethiopia

Cyber security in Ethiopia can observe under the legal and ICT ministry organizations responsible for the country's national security and any cyber security damage on the financial institutes are seen as a national security issue. Digital forensics is seen as a subset because as the number of attacks increases, the capability to investigate digital evidence responds appropriately and professionally should increase.

Ministry of peace

Ministry of peace was established by proclamation number 1097/2011 on October 16, 2018, with the principle of prevention and resolving of conflicts. Among the specific duties given to the minister by law, oversee national intelligence and security, follow information network and financial security functions, and follow up proper execution of functions relate to federal police, are listed (Ministry of Peace).

Ministry of peace spans the highest security structure in Ethiopia. It oversees the NISS, the INSA, The federal police commission, and the economic security and information center. In short, the ministry is the highest responsible for national information security.

The National Intelligence and Security Service (NISS)

The NISS re-establish under proclamation number 804/2013, and it was accountable to the prime minister to protect and safeguard Ethiopia's national security and Lead the country's security and intelligence service (Gazzete, word press, 2013). According to the Description of Powers and Obligations of the Supervisory Media of the FDRE Proclamation No. 1097/2018, NISS is now answerable to the ministry of peace (Gazeta, Proclamation NO.1097/2018, 2018).

Among the powers given to NISS, fight cybercrimes both inside and outside the country responsibly, follow up and investigate evidence on other serious crimes which are treated to the national interest of the country and provide to other relevant organs and carry out protection for critical institutions plus investigate threats to economic security (Gazzete, word press, 2013).

Information Network Security Agency (INSA)

INSA was established to protect the countries' information and information infrastructure from attack and prevent Ethiopia's national interest as if the plan is to build globally acceptable state-based cyber ability (INSA, 2019). INSA is the first and only organization in the country that rationally handles cyber security issues. It was accountable to the prime-minister under proclamation number 808/2013, but now the institution is responsible to the ministry of peace (Gazette, 2014).

The agency draft national policies, laws, and strategies to ensure IT-based infrastructure security to defend any cyber or electronic attacks, conduct security audits and provide security approval certificates. It also includes assistant, support, and training for police and other organs

empowered by cyber security law. INSA also controls the import and export of information technology, information sensors, and information attacking technologies also administer a national computer emergency responding center which includes the Ethiopian cyber emergency readiness and response team (Gazette, 2014).In collaboration with police, INSA conducts a digital forensic investigation and regulates cryptographic products transaction without a physical presence or physical presence upon a court warrant. Currently, the digital forensic department handles the Network, mobile, multimedia, and computer forensics with sub-departments separately.

Federal Police Commission

The federal police commission was established under Proclamation No. 720/2011 as an independent national government organ to ensure peace and security of the public and the state by ensuring the constitution's observation (Gazeta, Wordpress, 2011).

The federal police work with the ministry of justice and other collaborative organs with full authority of investigation, including crimes relating to computer network and computer system. The commission installs C.C.TV cameras at selected places to quickly investigate crimes. This directly connects to INSA multimedia forensic team as if the commission can also conduct DF investigation then provide an expert witness to the court or requesting organ. Ethiopian federal police establishment Proclamation No.702/2011 article 6 (5), (b) states explicitly that the commission can "*investigate crimes relating to information network and computer system*" (Gazeta, Wordpress, 2011).

3.7 The National Policies and proclamation in Ethiopia

The National ICT Policy and strategy of 2009

In 2009 the Ethiopian government drew a national ICT policy since the sector showed development and cybercrime is becoming a threat in the country. The 2009 national ICT policy and strategy state that Ethiopia's government has given attention to creating a safe and secure ICT environment (Ethiopia, 2009). The policy primary aim is to establish an accessible ICT infrastructure through the adoption of guidelines and principles, strengthen the private sector in the country by sharing best practices with national security agencies and similar agencies in different countries, developing the skill of the human and ensure the protection on intellectual property right in the ICT sector (Ethiopia, 2009).

This policy is also the first to address E-governance technologies and implement it according to the government service's effective delivery towards a citizen, business, and employee.

The National information security policy of 2011

Building national capabilities for identification, prevention, and reaction, deterrent, and recovery measures against threats is part of the 2011 national information security strategy; The policy also aims to reduce the cost of harm and recovery time from attacks, which interferes with the DFR mechanism and the key explanation for the policy's implementation is that Ethiopia is becoming increasingly vulnerable to external threats (Agency, 2011).

According to the policy document, information security is defined as the measures taken to protect data from attacks that compromise integrity, confidentiality, and availability while collecting, processing, preserving and communicating (Agency, 2011).

The policy structured as essential for all frameworks developed in the country, and all information security issues see with the procedure, so the creation of legal structures based on legislation helps criminalize any attack against information and information infrastructure to raise public awareness about information security and to take appropriate action against offenders; As a result, the faith built after the legal environment will be beneficial for trust in the use of information technology in the country (Agency, 2011).

Following the policy's implementation, INSA was found as the only organization protecting the national interest in cyber security, and CERT was established as a point of contact for incident information security issues (Agency, 2011).

The Computer crime proclamation

After an incident, the computer crime proclamation was used as a guideline for taking measures against citizens beyond the law and regulation of Computer and information security, based on digital forensic investigation findings.

The computer criminal proclamation No. 958/2016 was established to resolve illegal activities carried out without permission using computer systems, computer data, or networks, and it states that if an individual commits the crime, he or she shall be punished from 30,000 to 50,000 Ethiopian Birr (Representative, 2016).

Interference, unauthorized interception, and causing harm to computer data of a working computer system without permission or over authorization, then imputing, distributing, and removing data would result in a penalty, according to the proclamation (Representative, 2016).

The computer forgery and any computer-related frauds including causing economic loss by causing change, dilation, or any change, will be punished according to the proclamation on article 9 and 10(2); also, the proclamation states the police, in cooperation with the public prosecutors, should manage the investigation process, and the INSA will assist them if they require it (Representative, 2016).

3.8 E-banking: concept Ethiopia

Electronic banking (E-Banking) is described in several ways among researchers since the service involves numerous bundles. Bank customers may use devices to access services by supplying personal information. According to Sathey, electronic banking is a variety of Internet banking or online banking, telephone banking, television-based banking, cell phone banking, and offline banking or PC banking (Sathye, 1999).

More tasks are carried out virtually in the future than these days, and the impact of digital evidence will increases accordingly. When it comes to E-banking, the customers must develop confidence in the virtual environment's services, and the businesses will attract users as long as the network and data protection in the E-transaction, E-business and other virtual services are reliable; therefore, increasing the user trust and the ability to protect their interests has the most significant effect.

E-banking is showing development in Ethiopia even if the states of internet penetration in the country is causing the service problem; E-banking idea was first implemented in 2001 when the Commercial Bank of Ethiopia introduced the country's first ATM, and it was challenging (Bultum, 2014).

Gaining the customers' confidence is the first step in the banking industry, even if banks admit to having a security issue from time to time. The study by Blum revealed that a lack of confidence in the security of E-banking systems in Ethiopia, as well as a lack of trust in the use of technical facilities offered by banks can be mentioned as a barrier for the development of E-banking and the study also revealed that organizations have a lack of qualified human resource to enforce the system at the time (Bultum, 2014).

In Ethiopia, the number of customers who use E-banking services is still limited to the population. This demonstrates that in comparison to other African countries, Ethiopia's banking system deserves improvement.

E-banking can be considered a factor in attacking the organization's Network and impacting the county's business and the economy. As a result, Banks should improve their security while working on implementing electronic technology and payment methods. Banks should also work on the customers' awareness of the technologies' usage to minimize vulnerability; a study by Teka in Ethiopia states that customer's actual usage behaviour improves as they become more knowledgeable of E-banking service delivery networks (Teka , 2020).

Frauds on E-banking Current situation in Ethiopia

Ethiopian Banks are highly vulnerable to attacks these days, even if the number of E-banking users is small. Those banks' overall data security culture is not conducive to protecting information assets and minimizing cyber-attacks since handling cyber protection is not a solid basis for determination (Zewude, 2020).

To improve their business excellence, organizations should manage frauds committed by user's computers, mobiles, or other digital devices. E-banking becomes the primary attention of cyber-attacks; Kaspersky's report From November 2018-October 2019 shows that 776,728 user's computers were targeted to steal money from bank accounts worldwide in Trojan.Win32.Zbot attack takes the highest percentage (23.10%) from the banking malware family (lab, 2019).

There are not enough studies on statistics of E-banking fraud in Ethiopia, but there are some research studies that show how the situation is changing over time. According to Gebrehawariat and Lessa, there has been a significant observation of a security gap that leads to frauds since organizations' data management and discarding policies and procedures aren't well known, and existing policies for information security are not-followed (Gebrehawariat & Lessa, 2020).

The gap analysis also stated most E-banking methods are vulnerable to attacks since there was an observation of servers and other essential components without antiviruses and antivirus signatures modification problem on some necessary modules (Gebrehawariat & Lessa, 2020).

3.9 Current organizational NFR Observations in Ethiopian Banks

In Ethiopia, most studies revealed that NFR and incident management practices are not applicable at the organizational level. Availability of organizational network forensic readiness can be measured according to different Indicators. Organizational forensic readiness is not widely visible, but organizations are becoming more conscious of this process's importance. Approximately 87.4 % of governmental agencies lack an accepted framework to address cyber-attacks, while 11.6 % are in the initial stages (Zewude, 2020).

The following gaps were observed in Ethiopia on cyber security readiness (Woldemichael , 2020).

- Lack of legal frameworks
- Lack of awareness on cyber security
- Lack of well-trained human resources
- Poor cyber security governance

Organizational digital evidence source identification is the first criterion on the list for declaring an organization forensically ready, according to ISO/IEC 27043. Digital evidence source identification is essential since it is the core point to investigate an incident if the potential sources are listed. According to this subject, related ideas are rare, and it is difficult to determine whether an organization's evidence source is identified.

An observation from a study indicates that risk identification methods, control mechanisms, and documentation are not well organized, and there was a gap observed (Zewude, 2020). The system architecture includes the policy designing and documentation regarding the organizational system, including hardware and software components. Based on ISO/IEC 27043, we can evaluate Ethiopian banks to say that they are ready forensically if they implement this process. According to a study, the implementation of a policy in place to deal with an incident was missed in some banks (Yohannes, Lemma, & Solomon , 2019).

The policies and guidelines designed must consider those banks' financial dilemmas since security is different from one scenario to the other. A study by Zewude indicates cyber security policy and guideline is missed that coordinates the cyber-security activities within the financial institution, through divisions, and among employees (Zewude, 2020).

The architectural system process is vast and includes the overall design of the organization structure on IT and computer equipment; therefore, much attention is needed to handle this process sins it is used as feedback for the pre-incident gathering, storage, and handling process. According to a study, an organizational architecture gap was observed on the wireless networks, wired networks, system security practices, and other security management structure (M.Bogale,L.Lessa & S.Negash, 2019).

The pre-incident gathering, storage, and handling of data is another indicator for organizational forensic readiness on ISO/IEC 27043. Ethiopian banks introduced various services to the local market, which are completely dependent on IT, and centralized databases are applicable; this exposes the banks for attacks.

The planning and application of pre-incident gathering, storage, and handling of data in Banks can be evaluated by the methods implemented to handle the data that customers and the organization have. To make the process visible, logging software and other digital signatures that help gather data as a backup are applicable. Disaster recovery plans can be the one way to achieve this process since data lost in various ways. A Disaster recovery plan framework proposed for Ethiopian banks can be used as a reference.

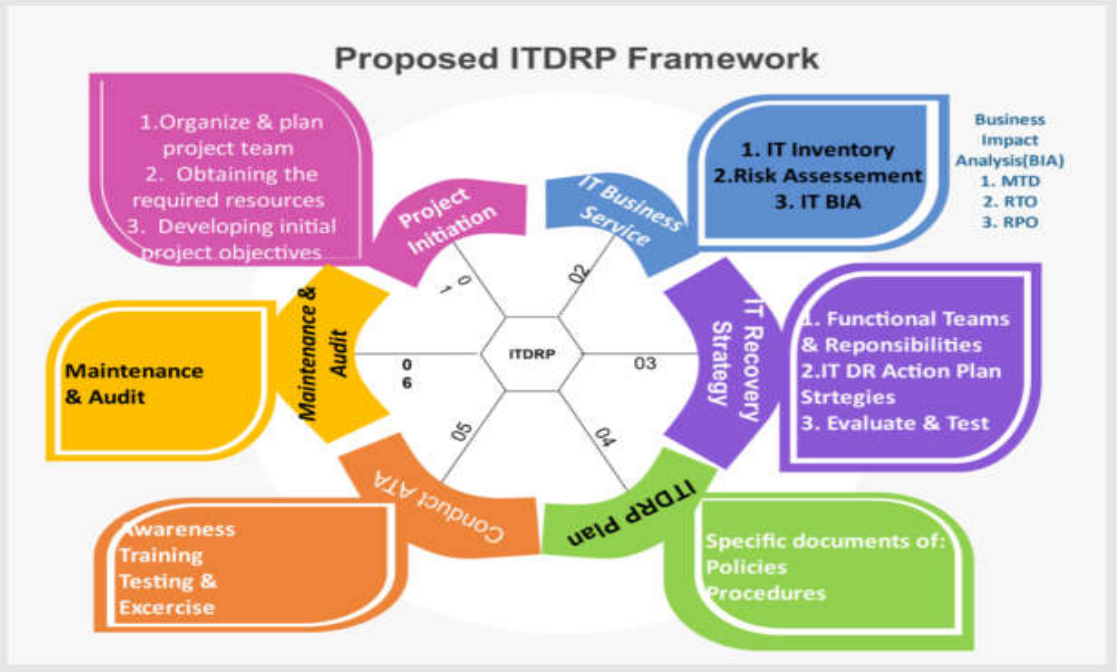

Figure 3. 8 Proposed ITDRP framework (Tariku & Lessa, 2020)

Pre incident analysis is another advisable readiness criterion according to ISO/IEC 27043 for organizations that lead them on the preparation, detecting, and defending of attacks. When we come to Networks, this readiness concept includes protecting organizational systems from attacks by analysing every packet and information using antiviruses, intrusion detection soft wares or intrusion prevention soft wares, change trucking soft wares, and antiviruses.

Analysis performed before an incident is used as output for the incident detection process, so the proper functionality of software used at this level has a higher impact on the trust of incident detection alerts. According to a study performed in some selected Ethiopian banks, employees have been accused of improper usage of antivirus software's and poor security scanning have been observed (M.Bogale,L.Lessa & S.Negash, 2019).

To ensure the security of their activities, most commercial banks conduct risk and business impact assessments. Since the country is witnessing a rise in the number of incidents, banks must pay careful attention to risk management (Berhanu, 2017).

Incident detection listed in ISO/IEC 27043 as an indicator for DFR, and it is beneficial in tracking any change in the organizational systems. Most Ethiopian banks implement incident detection systems even if the usability and accuracy are in question. A study by Ethiopian researchers indicated a limitation in terms of accessibility and precision, but automated monitoring and incident detection systems have been implemented even if they have the problem of detecting new attacks in the observed Ethiopian banks (Yohannes, Lemma, & Solomon , 2019).

The accuracy of incident detection tools can be mentioned as a gap in banking systems since it leads to the incident response process's a wrong decision. There were gaps listed out on the practices of incident detection in Ethiopian banks which are (Yohannes, Lemma, & Solomon , 2019);

- A Lack of trained incident responders
- Lack of security awareness among employees
- Information gap among departments
- Incident detection response delay

Another way to evaluate organizations' FR is by checking organizational information security incident management practices using ISO/ IEC 27035:2016 even if the DF readiness process does not concern about decide and respond process from the cyclic processes of ISIM.

According to a study by Worku and Padayachee, end users have a significant effect on incident minimization, but incident management and communication lack observed organizations, so they suggest a framework to improve communication (Worku & Padayachee, 2020).

3.10 Suggested DFR practices for different countries' organisations

DFR becomes the goal of some other corporates other than banks since IT security is becoming the main point to attack an organization. Readiness is now a strategic priority that includes technical and non-technical activities that improve an organization's ability to use digital proof.

Here will look at DFR practices recommended for organizations located in different countries. The cases were chosen based on the scenario similarity with Ethiopian most organizations since the suggested methods for the developed organizations might be feedback when we come to Ethiopia. Main aim of this selection is to find out the ideas of organisational FR in different counties.

There was also a recommended DFR framework for Nigerian banks based on the loss of money on the county's online scam and the unresolved cybercrimes'. The framework suggested a DFR approach that aligns with the organization's priorities identifying what laws and policies impose a record-keeping obligation on the Banks. The basic improvements covered in the framework include policy implementation according to acceptance of evidence systems and time to begin an investigation, prepare a FR team in the organization and identify people that would require to respond to an assault, Daily seminars with awareness programs including certifications to keep the DFR team computable, introduce resent system components, Identify a list of organized system requirements and classify evidence source machines to easily record log files, choose the right tools to keep an eye on the situation using escalation strategy to report incident, perform a risk assessment using threat identification and classification (Garba, 2019).

Research by Karie and Karume Listed out identified problems and challenges in most organizations for DFR, and the emergence of cloud computing has been considered as a challenge for many organizations even if there are emerging frameworks related to cloud FR, from commonly observed challenges in organizations, the selected ones are lack of DFR strategy and FR policy, legal framework and law enforcement difficulty's, qualified staff, lack of DFR cost implications and guidance in implementing DFR in an organization, they observed problems to cover the cost of stored data and damages has been occurred due to absence of immediate response during an attack (Karie & Karume, 2017).

Another DFR framework was also introduced for small and medium-sized businesses in South Africa; the framework is to solve the increasing cost of DF and the observed lack of forensic skills according to the country's Act of national business (Stander, 2010).

Small to medium-size companies are characterized as non-governmental organizations with fewer than 200 employees, according to the paper; those companies may be unable to recover loss after an incident due to false evidence, or the expense of collecting evidence may be prohibitive if they don't prepare adequately since affordability of a third-party examination is less (Stander, 2010). On the framework, employee's number minimization is mentioned as an advantage for FR, limiting the access of organizational users on the financial institute and handling incidents occurred on financial consulting firms is the second factor, the type of industry, available skill in information technology, and the amount of money set for a digital forensics readiness program are from the important characteristics influencing the organizations FR (Stander, 2010).

In the case of Kenyan banks, researchers developed a cyber-resilience measuring framework for selected banks and developed a Kenyan-based tool considering the survey result; in addition to that, the findings show certain banks have a good cyber security practice and embraced cyber-resilience, security awareness is stressed out, and cyber security practices got even greater attention than expected (Mayunga, 2019).

3.11 Related works

Different digital forensic readiness frameworks have been introduced based on the international standard of incident investigation principles and processes. Those frameworks and readiness concepts help organizations look at their capacity for incident detection, response, and digital evidence identification and implementation. In this study, different NFR approaches are discussed.

The research by Zewde assessed the challenging threats of cyber security and emerging trends on Ethiopian banking and pointed out some threats that those banks are facing, the study is a major outcome that indicates there is a lack of expertise on the area and insufficient budgets have provided for IT security; furthermore, the support from top management bodies of those banks is limited, the staff of those banks has poor awareness on cyber security, there is less managing traffic from untrusted sources and the study also find out the readiness of those banks should increase since high vulnerability observed and there are even attacks from staffs (Zewude, 2020).

The research conducted by Yohannes, Lemma, and Solomon on incident response management in Ethiopian banks indicate the current practice and gaps observed in the bank aiming to identify the applicable best practices according to ISO standards and the missed parts, on the findings they clearly listed out that the bank has no separate information security incident management guide, there is a classification of incidents for better management, there are communication gaps between top managers and IT departments and challenges of hiring skilled cyber-attack analyst, but there is an observation of modern incident monitoring tools in the bank (Yohannes, Lemma, & Solomon , 2019).

Getahun, in his research called "Cyber Security Auditing Framework for Banking Sector in Ethiopia," following the collection of data from different banks and specialists, he closed his study by introducing a cyber-security auditing framework for the elected banks to be implemented even if Cyber security is quite a complex field of research; with several unexplored cases in the fields, the researcher also proposed the framework without comparing to other frameworks or the problems that banks faced around the world (Getahun, 2018).

A developed DFR model for IoT-enabled organizations Proposed beneficial top-down approach-base proactive IOT-framework aiming to resolve DFR in the planning process and implementation phase by replacing them with organizational readiness and IOT security processes, which is a valuable constrictive framework that addresses exacerbated problems due to the lack of structured approaches furthermore the framework is designed to incorporate a proactive forensic process in an enterprise by aligning the organizational process with readiness and IOT security processes, the findings suggest that if further forensic process could be incorporated into the current state of IoT, it could be beneficial (M, P Phathutshedzo ; K, R Victor ; I, R A; Venter, H S; C, Kim-Kwang R;, 2020).

A paper by Englbrecht, Meier, and Pernul have done focusing on comparing capability maturity models and evaluate how the models assist and can help with DFR integration in an organization expecting continued improvement because, in a selective region, a capability maturity model for DFR is important to assess organizations' current state concerning DFR measures and obtain assistance in achieving the desired level of getting similar abilities (Englbrecht, Meier, & Pernul1, 2019).

Proposed a model for DFR for wireless LAN based on the practice on the usage of log file in an organizational network to capture evidence after the incident; in addition to that, the author researched the relationship between mobile stations and access points to design the model, and the model aims to track log files and report Network traffics to the forensic analysis for safe communication (Siphon, Ngobeni Josian, 2016).

Based on the above literature reviews, it is clear that there are a lot of researches which have been done in different ways which are related to the research topic that the author proposed but in Ethiopia there is shortage of published papers related to cyber security and the forensic readiness since we can't see this two concepts separately and the reason behind the shortage of published peppers indicate much attention has not given for cyber security in Ethiopia.

3.12 Summary

Several methods, ideas, and processes regarding DF, cyber security, and DFR have been covered in this paper study. The concepts and descriptions on DF and the readiness processes have also been elaborated. It has also been clearly stated that the ISO/IEC 27043 standard and how the standard has put targeting incident investigation in organizations for better information security, including what the structure of an organization looks like to be called ready forensically.

The paper trays to cover organizational structure to investigate digital incidents at a national level in Ethiopia since the target is to measure how to maximize a capability of an investigation by minimizing the costs. Simultaneously, the goal directly connects to those organizations since all the country's burden regarding the sector is on them. According to cyber security, there are existing policies and proclamations to guide organizational security management and control the citizens against cyber security law in Ethiopia.

From the paper reviews and studies in Ethiopia, we observed the development of internet penetration rate and the number of users on E-banking. In another way, we also find out the current states of the country regarding cyber security and attacks targeting financial networks like banks even if we have observed there is a lack of researches which have been done on the area.

There have been various definitions for terms, and the author tries to discuss the tools that are help full for NFR in an organization. The papers cover the current observed states of banks according to the ISO/IEC 27043 based on the findings and studies of researchers' results in Ethiopia. Some observations on the organizational DFR in different countries have also been covered based on organizational readiness.

4. Practical part

This section presents the results from an online survey and interview with the corresponding professionals. The online survey was conducted on 18 different Banks in Ethiopia which are all banks currently found in the country, and 31 responses were gained. From those responses, 19 were from the private banks,2 of them are mentioned as from other sectors, and the other 10 out of 29 responses were from governmental or the public banks. The survey was done from 8/2/2021 -16/2/2021 and the online questioners were filled by information technology professionals who work in the IT security area of the banks one person is lead of the IT security team and one other person is from incident management team because to understand the practices of the NFR in the bank they are the direct contact on the area and the practices related to IT security show the current cases and practices taken and help us to suggest how they can maximize the banks capabilities according to the missed facts.

4.1 Survey

The online survey was done using Google form and has questions that enable us to understand the current reality of Network forensic readiness in Ethiopian Banks, which are the core for the financial network in the country. The survey communicates whether those banks handle evidence properly or network-related data are causing much more damage than expected.

In this section, the analysis of the online survey is present. To answer the research questions, the author seeks to provide a survey with 19 questions, and the respondents were anonymous. To go through the analysis, the IBM SPSS statistic viewer tool has been used.

The questions classify into seven parts to clarify them easily:

- Respondents background profile
- The experience of banks on cybercrimes and network attacks
- The awareness of banks information technology professionals regarding digital forensic or investigation.
- Effectiveness of digital evidence handling in the banks.
- The validity of evidence from network forensics in a legal matter.
- The capability of NFR in the banks.
- NFR costs according to challenges that are faced on the banks.

Respondents back ground profile

The first part of the survey coved the back ground information of the respondents. It includes the gender, occupation and age group. We clarify the number of respondents in percentage. From the respondents 77.4% were male and the other 22.6% were female this shows how much the participation of women's in the IT sector is small in Ethiopia. In other hand large group of the respondents were from age of 26-30 and 31-40. From the respondents largest group of them were from private company and they cover 63.3% of the survey since 33.3% of them were from government or public sector .The other 3.4% were not interested to mention the organization that they are in.

	Description	**Frequency**	**Percentage**
1.Gender	Male	24	77.4 %
	Female	7	22.6 %
	Total	31	100.0 %
2.Age	26-30	14	45.2 %
	31-40	14	45.2 %
	40+	3	9.7 %
	Total	31	100.0 %
3. Occupation	Government or public sector	10	32.3 %
	Private company	19	61.3 %
	Other	1	3.2 %
	Total	30	100.0 %

Table 4. 1 Demographic characteristics of respondents

The experience of banks on cybercrimes and network attacks

The experience of organizations on cybercrimes and network-attacks were the other part of the survey that we covered. 83.9% of the respondents has encountered a cyber breaches in there organization and 6.4% of the respondents stated there organization did not experience cyber-attack and rest of 9.7% were not aware of their organizations experience.

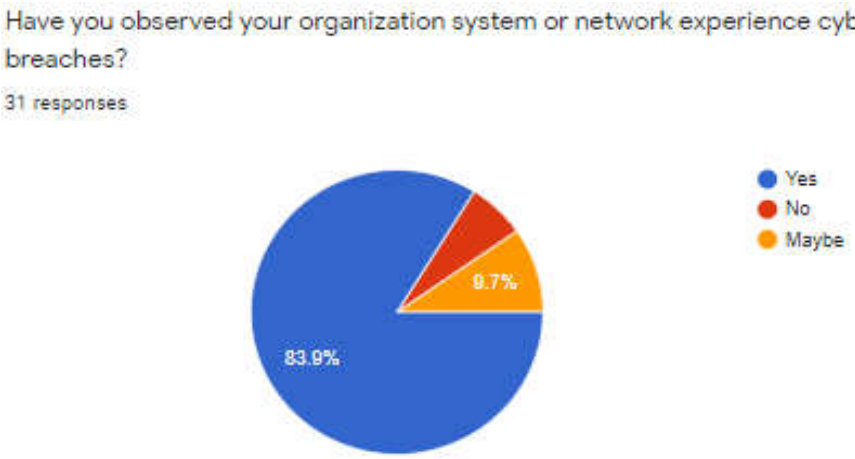

Figure 4. 1 Experience of banks on cyber breaches

Since 26 out of 31 respondents observe cyber or network attacks on their organization they were asked to encounter the experience of the attacks on their organizations system from the most common attacks observed in the country and from the listed eight forms of attacks 18 respondents observed malware based attacks which is the highest from all, 17 respondents observed DDOS ,16 respondents witnessed business email compromise, 15 of them witnessed phishing or social engineering attacks, 10 of them witnessed website defacement, 12 of the respondents observed man in the middle attacks ,8 of them witnessed SQL injection and the smallest observation of the attack is cross-site scripting (xxs) while 3 respondents observed.

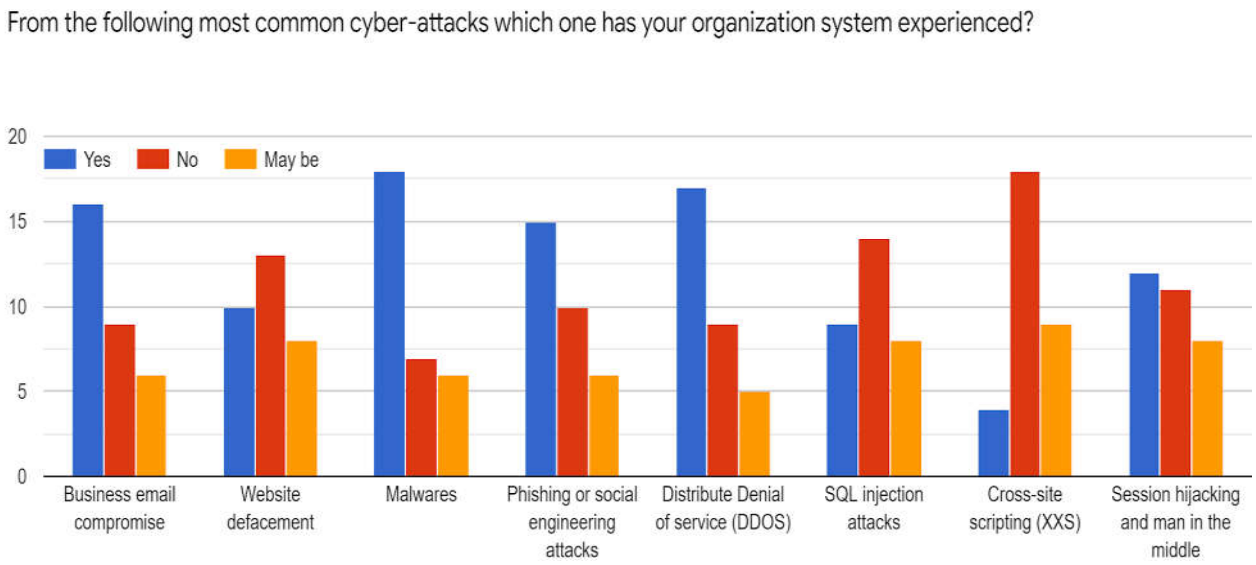

Figure 4. 2 Cyber security incidents observed in the banks

Respondents measure the experience of the attacks in there organization on the year 2020 and from the result 61.3% said the attacks are increasing , 19.4% respondents mentioned it is remaining the same, 12.9% of the respondents claim that the variation of the attacks are not known and the rest of the respondents which were 6.4% said it is decreasing.

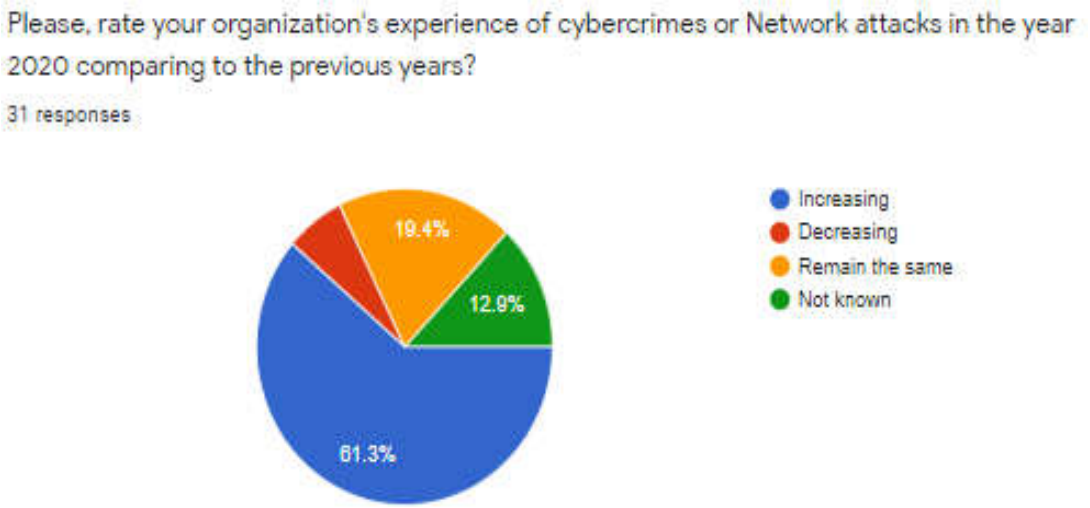

Figure 4. 3 Banks experience of attacks on the year 2020

The awareness of organization information technology professionals regarding digital forensic or investigation

The survey was also conducted to examine the awareness of IT security professionals in the banks about digital forensic or investigation and 90.3% of the respondents are familiar with the concept and rest of the 9.7% did not know what DF or investigation is.

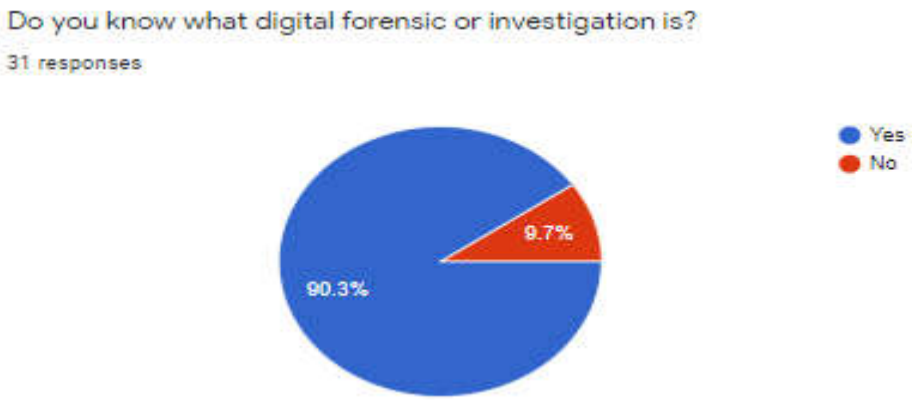

Figure 4. 4 Awareness of DF or investigation

Depending on the awareness of organization IT security professionals specific knowledge assessment has been done on the digital forensic process class and 27 respondents were aware of The investigation process class, 23 of the respondents understand the readiness process class, 21 of them are aware of the initialization process, 17 replied as they understand acquisitive process and the concurrent process class is the list process class according to the respondents awareness and 17 of them said they are not aware of it.

Statistics

		The Readiness Processes	The Initialization Processes	The Acquisitive Processes	Investigative Processes	Concurrent Processes
N	Valid	28	28	28	28	28
	Missing	3	3	3	3	3

Figure 4. 5 Missing and Valid result Statistics

Items	Yes		No	
	Freq	%	Freq	%
The Readiness processes	23	74.2	5	16.1
The Initialization processes	21	67.7	7	22.6
The Acquisition processes	17	54.8	11	35.5
The Investigative processes	27	87.1	1	3.2
The concurrent processes	11	35.5	17	54.8

Table 4. 2 Deep understanding of DF

Effectiveness of digital evidence handling in the bank

To measure the effectiveness of digital evidence handling and organizations' capability to perform those NFR practices, we provide a question to level the scale of collecting, preserving, analysing, and protecting digital evidence, and the respondents rate their observations.

From the respondents 32.3% indicated that the process is not effective at all and equal number of respondents also indicated it is satisfactory as if 19.4% of them mentioned there is

no evidence collection mechanism has been established where as 6.5% indicated there is very effective evidence collection, preservation and protection method. From this we understood the evidence collection process is totally given for the governmental structures in Ethiopia and even banks are not giving much attention for NFR.

Items	**Description**	**Frequency**	**Percentage**
1. level of collecting, preserving, and protecting of digital evidence	Very effective	2	6.5%
	Satisfactory	10	32.3%
	Not effective at all	10	32.3 %
	No evidence collection mechanism established	6	19.4%
	Missing	3	9.7%
	Total	31	100 %
2. organization capable to analyse digital evidences	Extremely capable	2	6.5%
	Very capable	4	12.9%
	capable	14	45.2%
	Not capable	8	25.8 %
	Missing	3	9.7%
	Total	31	100 %

Table 4. 3 Digital evidence analysing, collection, preservation and protection in banks

The respondents also indicate the capability of analysing digital evidences. Hence 45.2% of them mentioned there organisation is capable, where as 25.8% indicated no capability at all but 12.9 % of them said there organization is very capable where as 6.5% of the respondents mentioned their organization is extremely capable.

Validity of evidence from NF in legal matter

37% of the respondents indicate network forensic evidences are help full in legal matters and also equal number of respondents indicate it is not helpful at the same time in addition to that 25% of them are not certain on the validity of the evidences from network investigation. This makes the validity of the evidences from network investigation in question.

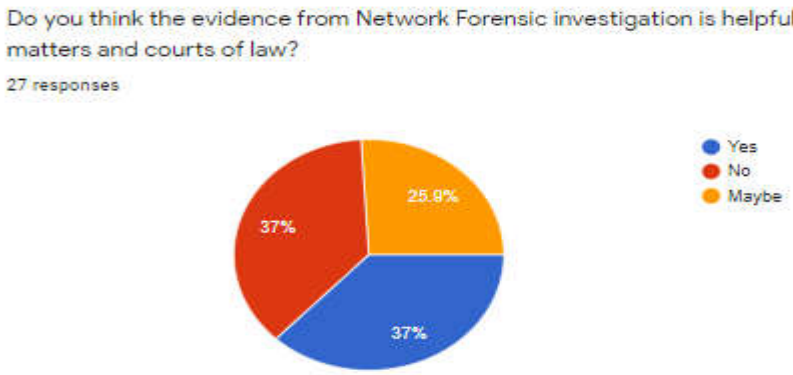

Figure 4. 6 Validity of network forensic in legal matters

Capability of NFR in the organizations

Regarding NFR capabilities respondents were asked to measure the awareness of their colleges with respect to response for network attacks as a first line and 27 out of the total respondents have replayed for a given question and 17 of them indicated employees have no awareness and 10 of them indicated there colleagues are aware of responding attacks during first occurrence.

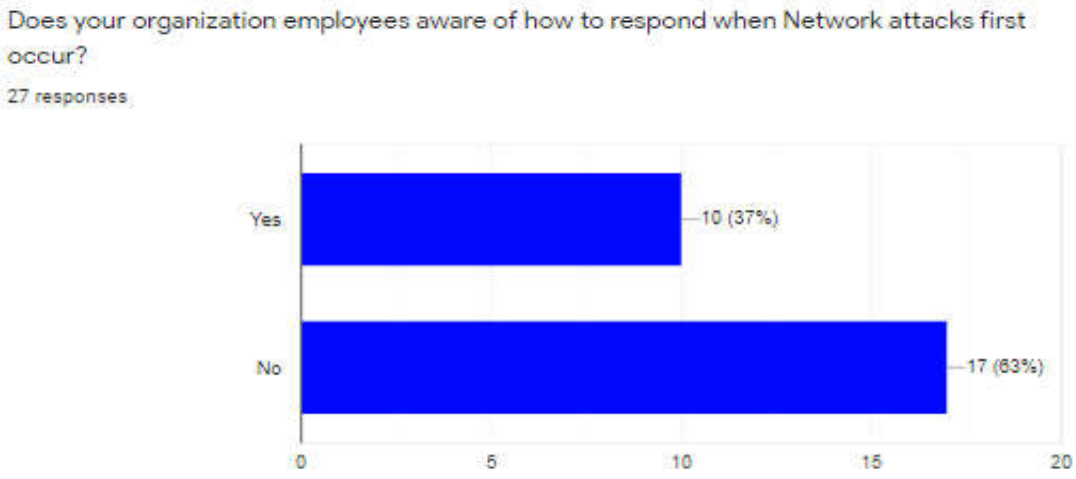

Figure 4. 7 Awareness of NFR

The level of execution according to DFR was also measured and 12 of the 28 respondents said all organizational digital evidence sources has been identified and also equal number of respondents are not aware of the process where as 4 of them mentioned there is no identification of digital evidence sources.

In addition to that 13 of the 28 respondents indicated there organization has a well-planned pre incident data handling while 11 of them don't know the states whereas 4 of them witnessed there organization doesn't have well planned pre incident data handling mechanism.

The pre incident analysis of data on potential digital evidence has been represented in 9 of the 28 organisations and it was not implemented in 3 of them but 16 respondents are not aware of this process implementation on their organization. Moreover incident detection mechanisms has been implemented in 18 of the organisations whereas 7 of the respondents are not certain and 3 of them witnessed no incident detection mechanism in there organisation.

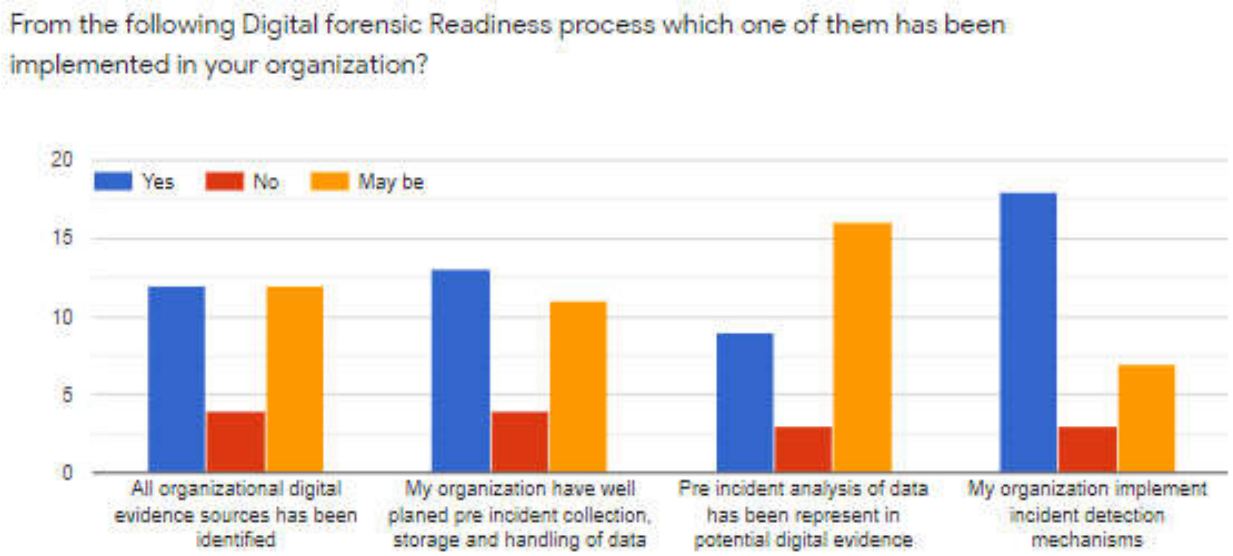

Figure 4. 8 DFR process implementation in an organization

From NFR perspective 32.3 % of the respondents aggread on capablity of network incident investigation according to information system architecture in there organization and 35.5% of the respondents confirmed there organization doesn't have defined informaion architecture while 22.6% of them are not certain on the capablity.

The maintainance of governance documents in the organizations have mesured according to the update time variation and 38.7% of them said the standard procedures and job aids maintained when ever the updates are needed as if 35.5% of respondents indicated betweeen three to six month diffrencce maintainance is taken place and 6.5% mentiond once in a year there organization maintain those documents hince 9.7% of the respondents are not aware of the documentation process.

Statistics

		System Architecture	Governance Documentation
N	Valid	28	28
	Missing	3	3

Figure 4. 9 System Architecture and Governance Documentation usage Statistics

Questions	Description	Frequency	Percentage
Does your organisation have defined information system architecture capable of network incident investigation?	Yes	10	32.3 %
	No	11	35.5 %
	Maybe	7	22.6 %
How often your organization maintains governance documentation and the standard operating procedures and job aids?	Once in a year	2	6.5 %
	Between three to six months difference	11	35.5%
	When ever needed	12	38.7 %
	Not aware of it	3	9.7 %

Table 4. 4 NFR indicators in the banks

NFR cost according to challenges that are faced on the organizations

Regarding cost of NFR 28.6% of respondents implicate NFR cost is much more than the investigation cost after an incident and equal number of respondents also mentioned NFR cost is not higher than the investigation cost in there organisation hence the rest of 42.9% are not sure on the cost comparison between NFR and investigations after an incident.

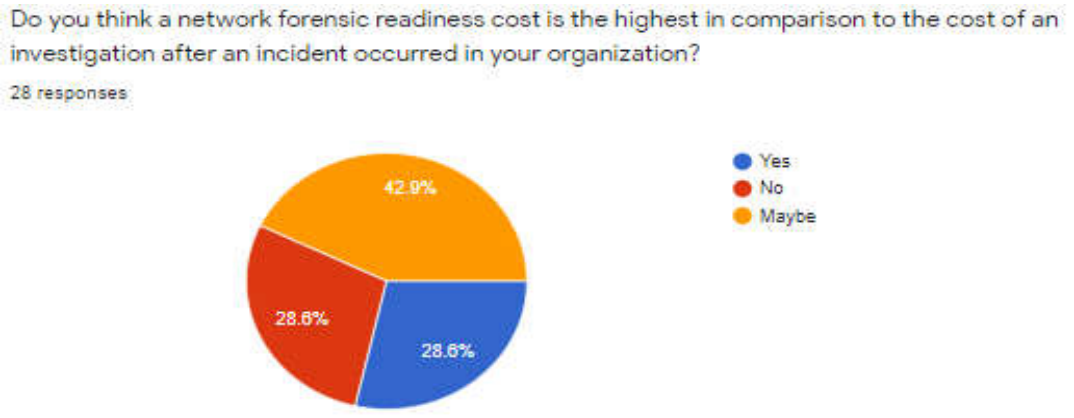

Figure 4. 10 Comparison of NFR cost to the cost of investigation

More over the NF or investigation challenge is extremely high according to the respondents while 50% of them agreed on it and 32.1% of them also mentioned it is high where as 17.9% of them said the challenges are measured as it is good. From the respondents replay we understood the NF investigation is challenging in the country.

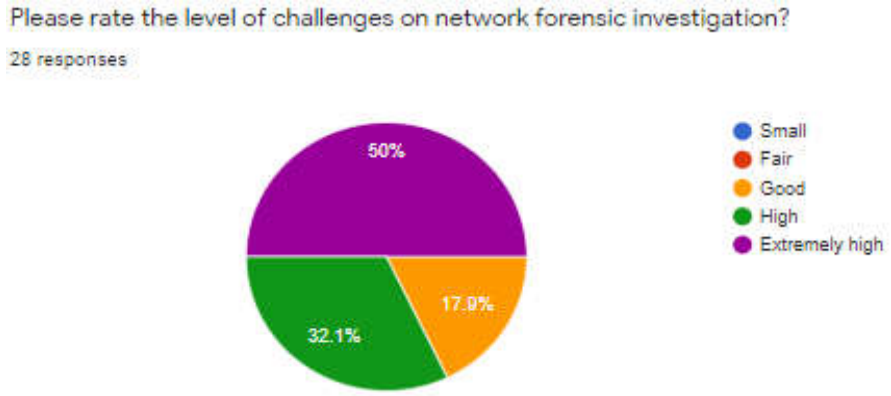

Figure 4. 11 Challenges on NF

59.3% of respondents indicate NF findings have been reported fully and the chain of custody is proper where as 22.2% of them said it is not applied and rest of 18.5% also mentioned that there might be proper reporting and recording on digital evidence but not certain on it.

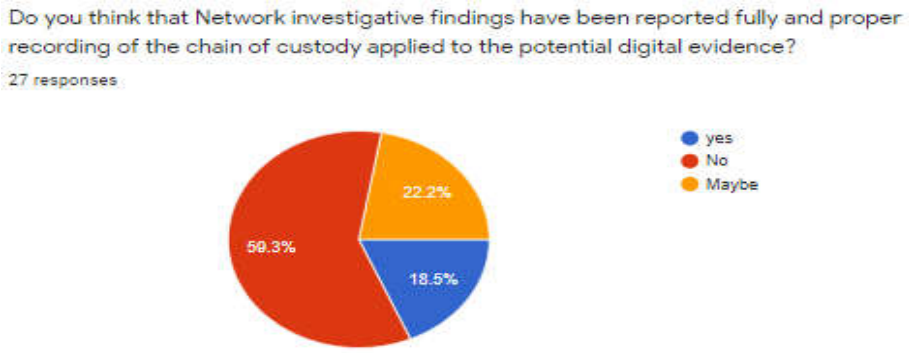

Figure 4. 12 Rate of reporting and recording of NF findings

In addition to NF investigative findings report and record rate the highest challenges has been listed out according to respondents experience and lack of qualified professionals has been mentioned as the highest impact on the NFI process and covered 50% of the replies while luck of finance or budget is the second highest factor according to the respondents which is 28.6% of them give rate plus juricidical struggles take the 17.9% of the respondents replay. While the rest of the respondents mentioned lack of understanding on the importance of NF as a challenge.

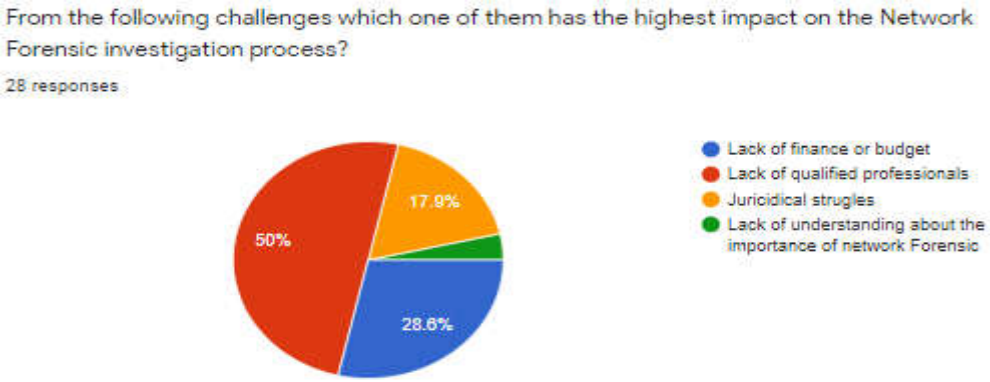

Figure 4. 13 Challenges on NF

4.2 Interview Analysis

The interview was conducted using Google meet, and there were 11 questions in total concerning Ethiopian banks NFR. The overall part of the interview is translated from sound to written format. The Interviewees responded to all the questions in Amharic, which is the Ethiopian local language, even if the questions were in English. Interviewees are also organized into six categories based on core points to study Ethiopian banks' NFR process, and the respondents are kept anonymous and mentioned in the future text with acronyms R1, R2, R3, and R4.

- The purpose of NFR and benefits that organizations gain
- The challenges to implement NFR in organizations
- Gaps observed for NFR in organisations
- Methods to improve NFR
- Benefit of investment on NFR and expectation for the future
- Observed capability of data gathering, storage and handling in Banks

The purpose of NFR and benefits that organizations gain

The interviewees were asked to demonstrate the function and benefit of NFR for an Ethiopian bank to determine the purpose of NFR. Below, are the respondent’s responses in a table format.

Interviewee	Response
R1	“The NFR allows organizational retrievals of network-based evidence simple and painless, and it also allows the banks to streamline its operation before an incident. An organization will be beneficial since the targeted areas of attacks are identified.”
R2	“NFR helps organizations to actively collect digital evidence using log files, emails, Network traffic records, and backups to combat forensic criminals. Banks will be beneficial regarding the process of information gathering in a lawful manner so that NF can be carried out with the expense equal to the severity of the organizational incidents.”
R3	“NFR ensures any investigation regarding an attack has the least amount of impact on the organization. It is beneficial to handle the investigation without interrupting the business or with small disruption on the service of the organization.”
R4	“NFR helps the law enforcement bodies by underlining the favourable effect of evidence on the legal matters.” “NFR can be an indicator whether Banks assets have been handled with care or not and whether they are beneficial for organizational governance. “

Table 4. 5 Benefit of NFR

The challenges to implement NFR in Banks

The interviewees were asked to explain the challenges of implementing NFR for an Ethiopian Bank to determine the challenges to implement NFR. In the table below, you will find an overview of the respondent’s responses.

Interviewee	Response
R1	"Observed challenge on identifying digital evidence sources in an organization Since the information's that need to be secured are not protected under security policies so there is a fear of loss of data even in the process of devices identification which might contain evidence log files."

R2	“For quite some time, there have been issues with the tools that have been integrated on firewalls and IDS to collect traffics, and failure has been observed in collecting all of the desired traffic data's since a large amount of data storage space is also needed to store all evidence."
R3	"Considering the applicability of ISO standards and other international cyber laws in the context of Ethiopia situation to enforce FR properly."
R4	"Due to a lack of commitment from managerial hierarchies and a lack of funding for the procedures that should incorporate in the pre-incident planning, the readiness process becomes a challenge."

Table 4. 6 Challenges to implement NFR

Gaps observed from NFR in Banks

Those interviews asked to identify and elaborate observed gaps in those banks about NFR to understand how they can handle the NF investigation process after an incident.

Interviewee	Response
R1	“The provided attention to update network security and integrate the newly defined technologies to the organisational network since there is a lot of observation regarding knowledgeable employees who can operate a given technology in a proper way and understand how to respond for the alerts generated from IDS.” “Network penetration tests externally are not taken as a culture in most banks to assess the security states of the organisation network ”
R2	“Monitoring tool warnings that are wrong or incorrect highlight the carelessness and adoption of such alerts, making it difficult to respond to the correct intrusion.” “The lack of well-organized and defined network security policies, furthermore the trend of implementing job aids in every

	department to protect the organizational system from disruption and balance the business.”
R3	“Practices of documenting incidents is poor and there are limitations in the use of platforms that facilitate the documentation of significant changes. Furthermore, inaccurate timing for the erase of data from the backlogs is common which registers changes of the network activity”
R4	“Problem of a standard architecture for network infrastructures cause difficulties to come up with the solutions and hard to investigate after an incident.” “There is observation of gap to report attacks on time before much damage occurs”

Table 4. 7 Gaps observed from NFR

Methods to improve NFR

To understand which FR approach was applicable and the capability of data collection, storage, security, and analysis, the interviewees were asked how to enhance the NFR of banks in the observed current situation.

Interviewee	Response
R1	“Network penetration testing externally with an individual or entity who doesn’t have access to the bank’s infrastructure in order to assess the level of network security in the hackers mind-set and identify business’s vulnerability” “understanding the event log analysis on the IDS/IPS to identify the most targeted network device in the network and improve the readiness of the device and secure it so much professional incident analysts are needed”
R2	“Work on the capability of active strategies which lead to go out and tackle the expected attack from the hackers since the outcomes are more feasible and the readiness of the banks will also increase to achieve this goal ”

	"Embracing new technologies as AI for pattern recognition and other log data comparison with saved signatures " "Those banks are also expected to have a budget even more than other budgets that they have to improve NFR"
R3	"Each bank has to decide on the investment of buying tools which are deception based and make a fake connection to trap hackers, the concept is new but it is becoming widely implemented in different countries financial network since the forensic investigator can accurately determine the situation."
R4	"Employees should receive proper on-the-job training in network security to increase awareness of access limits and authority to erase data; each employee's access to each system should be limited according to the role and work load that he or she has." "Exchange of experience with other cyber security stakeholders, such as INSA contextually and other banks' security teams, to gain the most experience and be prepared based on cases that have occurred in those sectors."

Table 4. 8 Methods to improve NFR

Benefit of investment on NFR and expectation for the future

To clarify whether the value of NFR outweighs the cost of investigation and future expectations regarding NFR, Interviewees were asked if investing in the NFR mechanism is beneficial or not to understand the cases according to attacks and damages on Banks infrastructure.

Interviewee	Response
R1	"Stack holder's strong bond to work together for a better result is expected including design application of NFR policy in the bank and guide for the policy design is expected from INSA."
R2	"Make NFR a culture is future expectation of Ethiopian banks as the vulnerability for attacks are increasing "

R3	“Investing in the NFR helps the banks save money that they spent for foreign cyber security professionals because employee skill development and technology engagement are included in the budget.”
R4	“Expect to develop clear incident handling practices which bank's IT security managers approve.” “Development of training on usage of tools implemented for pre-incident analysis and incident responses expected and beneficial for the banks since a wide gap in incident handling has been observed.”

Table 4. 9 NFR investment benefit

Observed capability of data gathering, storage and handling in Banks

To understand the banks' current state on the data gathering, storage, and handling, the interviews were asked their observation on the processes regarding their implementation.

Interviewee	Response
R1	“The capability of most banks on data storage and collection of evidence is good. However, they still need to strengthen their database management system for more immeasurable output of security. The PDE can be stored safely per each user's identity, making the investigation after an incident easier.” “The applicability of information security policies is present, which is a backbone for collecting accurate data. However, there are observations on applying the designed policies to the branch banks, which is a gap for the banks to collect effective data during an incident.”
R2	“Inapplicability of using Collected data stored in a full-fidelity format on a database, including the packets from the network for analysis and making the task for incident response and DF easier. This is observed because of unclear network structure of the banks ”

R3	“There are departments in all of the banks as incident response teams with subdivisions to handle incidents seen as a good practice and modern, but some banks give all the authority to handle related risks to this specified department. This shows an autocratic problem of information handling, and the retention and erase of collated data will be decided with this team which leads to unbalance problem.”
R4	“During an incident, those banks work with INSA to solve difficult attacks, but the investigation is difficult since there is an information exchange gap and there are difficulties to identify evidence sources.” “Modern monitoring tools are applicable this days like SIEM and other tools for network flow capturing and analysis”

Table 4. 10 Data collection

5. Results and Discussion

In the previous chapter, the survey results have been analysed, which focused on the research objectives based on the sub-objectives. This chapter presents results and discussion of data collected via the questioners.

The collected data has been analysed and discoursed to get the study's major output and give necessary recommendations; the research's important findings have discoursed below. Based on the findings, a presentation will be made on the research objectives and organized as follows. 5.1 evaluation of the survey analysis 5.2 evaluation of NFR practice 5.3 How to maximize the ability to collect valid digital evidence and minimize NF cost during an incident.

5.1 Evaluation of the survey analysis

How NFR is beneficial to the Banks of Ethiopia regarding cost.

Since FR is a business concern in banks, the degree to which it followed would be determined by the bank's ability to get a good return on its investment. The risk assessment is the most significant in determining whether or not FR is needed. Concerning risk assessment, it is better to get ready even if the risk assessment would say that risk has not been observed.

The main goal of analysing the benefit of NFR and according to cost is to clearly find out the current state of banks plan and investment in the area of NFR and determine how valuable is the implementation of NFR according to the challenges observed in the NF and the continual observation of incidents in the organizations. We studied whether the cost for NFR is high regarding the costs after an incident in the banks which is an indicator for NFR attention.

On the research, the risk assessment has taken place at first to check out the investment on the NFR is considered as a must according to the challenges faced after the incidents have occurred in the organization's network. The information gathered from the respondents implicates that the challenge for investigation after an incident in their organization is high and they also agreed on the lack of budget or finance is the second factor next to the qualified professionals in the investigation process since the investigation process takes time and money. This can be considered an implication for organizations to invest in tangible and intangible resources to fulfil the incident's reediness. It is challenging to come up with a solution after the incident.

Challenges On NF

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Good	5	16.1	17.9	17.9
	High	9	29.0	32.1	50.0
	Extremely high	14	45.2	50.0	100.0
	Total	28	90.3	100.0	
Missing	System	3	9.7		
Total		31	100.0		

Figure 5. 1 Evaluation on FR challenge

On the other hand the banks security professionals were asked that how much the cyber and network attacks are affecting their organizations in the year 2020 and more than half of them has mentioned it was increasing for the specified year and this is also observed as the other reason for how much organizations should develop NFR and generate all feasible solutions. The increasing number of incidents is the factor for the organisations to give attention for NFR and help them to generate all possible solutions.

The Ethio-CERT, a department with in the INSA in charge of the protection of financial institutions and key Ethiopian infrastructures also mentioned that the number of cyber-attacks on financial institutions has increased with a large number of scale (INSA, Information Network Security Agency, 2020). The observation of increasing number of incidents is the second reason why cost for the readiness process is worthy to defend the public and organisation's interest since bank's have a lot of customers.

Network Attacks Observation On The Year 2020

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Increasing	19	61.3	61.3	61.3
	Decreasing	2	6.5	6.5	67.7
	Remain the same	6	19.4	19.4	87.1
	Not known	4	12.9	12.9	100.0
	Total	31	100.0	100.0	

Figure 5. 2 Observed attack evaluation

By assessing the challenge on NF and the number of incidents based on the survey we can conclude that cost of NFR or investing on NFR is worth it for the banks to minimise the challenge after the incident and to come up with best solutions. The risks assessment indicates cyber security and network attack is highly observed, therefore banks are expected to invest on the readiness of the security equal to other investments.

The budget for NFR is identified as a top listed gap in the banks based on the interview analysis. Equal number of respondents on the survey also mentioned as NFR cost is the highest comparing to cost of investigation after an incident in their organisation this indicates the present values given for the cost of NFR in some banks is good and they are giving some attention for their organisation IT security but equal number of respondents also mentioned investigation cost is higher than the readiness cost in their organisations so this is another indicator that there is still a trend to focus on the issues after an incident.

NFR cost is higher in comparison to cost of investigation in my organisation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	8	25.8	28.6	28.6
	No	8	25.8	28.6	57.1
	May be	12	38.7	42.9	100.0
	Total	28	90.3	100.0	
Missing	System	3	9.7		
Total		31	100.0		

Figure 5. 3 Comparison of cost between NFR and Investigation

How capable are the banks on DF process implementation?

The Scope of this subject includes the evaluation of the banks on data collection, preservation, protection and analysis .This indicates how the banks are capable of performing every process this is an indicator for the banks capability to perform digital investigation easily which is evaluated by DFR practices.

From survey results, 38.8% of the respondents mentioned that their bank's ability to perform DF effectively. However, 51.7% indicate that the bank they are placing cannot perform the DF processes properly. This can indicate banks' low performance on the collection, preservation, and presentation of digital evidence. In addition to that, interviewees mentioned the low performance of digital evidence source identification and improper way of information handling and retention of important data's; this can be taken as a gap for proper way of data preservation and protection since it is considered as an input for the investigation.

The analysis of digital evidence is also covered here. The analysis relates to the description and evaluation of digital evidence from PDE sources according to ISO/IEC 27042:2015(E). 45.2 % of the banks have been identified with a capable performance of the analysis using tools even if their performance is not high. In addition to that, limitations in the use of platforms have been mentioned, and the problem of facilitating significant changes is observed. There have been issues with the tools integrated on firewalls and IDS to collect traffics, and Failure has been observed in some banks. These all are indicators of the analytical capabilities of the banks.

According to ISO/IEC 27042:2015(E), data analysis must concern with using established processes. This means the analysed data will be acceptable if it passes through proper pre-incident and post-incident practices to be valuable since it is easy to capture every detail. From the collected data, 29% mentioned the pre-incident analysis of data represented in PDE, which is the smallest number from the total. This might be an indicator of software barriers for pre-incident analysis. The above all are indicators of capability for collection, preservation, protection and handling of data.

How much NFR is necessary for the Banks?

The necessity and use of NFR is clear on the contextual observation of those banks since 83.9% of respondents stated that they experience a cyber-security breach and from the most common listed attacks, malware, DDOS, and Business email compromise taken the lead. From these results, we can understand how much those banks should give attention since most of them experience those attacks.

NFR is important because it is mentioned that without the business interruption, NF will be handled since PDE are identified, and retrievals of network-based evidence will be simple and painless. The information after an incident will also be gathered according to the law that is the core use mentioned regarding the sampled banks.

How much evidences are help full in legal matter?

To evaluate the helpfulness of NFR in legal matters, a question was conducted. Half of the respondents agreed that the evidence from NF is helpful, and good practices have supported this idea in the data collection and partial organizational information security policy implementations. In contrast, the other half disagree with this point of view. However, from the overall data, we can measure the support of network evidence in the court of law with factors like data handling practices and the storage and retention of data, including the documentation of single evidence.

Recognize half of the banks who invested in the NFR are gaining a good result compared to those who did not give much attention according to data investigation and presentation in a court of law. Governance documentation and the standard operating procedures and job aids have been updated frequently from the total observation, which is 74.2%; this is also an immeasurable indicator since it is easy to tackle an incident and gather all needed information, but a large percent of the respondents also show their organization is not implementing well-designed system architecture capable of network incident investigations.

Improper chain of custody and reporting of data has been observed widely. More than half of the respondents indicated that this is also a barrier to representing evidence in the court of law. There is a practice of finding foreign professionals because of difficulties in an investigation and gap analysis of network attacks from most banks.

5.2 Evaluation of NFR practices

The survey result reveals that banks are experiencing cyber security breaches continually. The revelled results underlined that NFR is necessary for organizations since cyber breaches are getting high from time to time.

The author classifies the difficulties in Ethiopian Banks regarding NFR into three principles: people, process, and technology. These three pillars are taken since they are basic for banks.

People

The study results indicate that Banks employee awareness is a primary barrier for the NFR process, and the Lack of qualified professionals can be mentioned as the second factor for the process considering people.

- Lack of awareness

Banks employs are not aware of ways to respond when an attack take place at the base line. Hence this leads the organization to complication so employees should have awareness on basic security lessons.

- Lack of skilled person

The absence of professionals with important NF investigation skills has been challenging for organizations when Network attacks or cyber incidents occurred.

Almost half of the respondents indicated evidence from NF is not valid in legal matters; this issue has a direct connection with the lack of knowledge and skill of professionals on evidence collection and handling in addition to organizational forensic readiness.

The ISO/IEC 27001:2013(E) stated that an individual working in organization should be aware of the information security policy, his or her contribution to the effectiveness of information security management system and implementation of information security management system (ISO/IEC 27001, 2013).

Depending on the standards organizations are advised to develop policies in order to strength the security. Give trainings and creating awareness among employees impact building a secure positive environment and is part of the policy making. Lack of mechanisms to report the incidents also found in Ethiopian banks and it is also another gap which discourages employees to take care of incidents in a professional manner (Yohannes, Lemma, & Solomon , 2019).

Awareness influence organizations a lot since employees are most vulnerable link; therefore, serious attention on incident handling, incident reporting and risk management are needed. Keshnee and Elias's findings on Ethiopian organizations stated that the communication and awareness coordination efforts are largely informal and mired by lack of planning and managerial commitment (Keshnee & Elias, 2020). A study by yohannes, Lessa and Negash stated that lack of security awareness among the staff is a challenge of information security management at Ethiopian banks (Yohannes, Lemma, & Solomon , 2019).

In the other hand, the lack of skilled professionals in an organization has the highest impact on network investigation process. This factor has influence on the capabilities of an organization in recognizing, investigating and responding to the incident.

Process

According to NFR process, some challenges have been identified from the study. Since the following processes are the basic to strength NFR the following are the observed ones.

- Insufficient capability of collecting preserving and protecting digital evidence
- Lack of analyses of digital evidence
- partial missing of organizational digital evidence source identification
- Absence of defined information system architecture
- unsatisfactory pre-incident data analysis
- Lack of reporting and proper recording of the chain of custody

The ISO/IEC 27043:2015(E) stated that activities for pre incident gathering, storage, and handling of potential digital evidence should be planned and implemented in an appropriate manner. Those banks are not effective on those processes and even there is no proper evidence collection mechanism which has been established in some of them.

In order to make the evidence feasible in the court of low after an incident the pre incident gathering, storage and handling processes are basic. As discoursed by Tan forensic evidences from a network devices can be collected from logging soft wares and hardware devices this might include proxy servers, DHCP servers, Dial-up servers, VPN, Routers, firewalls, IDS and DNS (Tan, 2001).

Identification of the sources for use full data before an incident is a primary step for NFR process to easily catch the gaps but mentioned that this process has not been satisfactory in there organization according to the expectations from the organizations. The ISO/IEC

27043:2015(E) stated identification of which device is the source of the data lead us to potential source of the digital evidence so minimizes the time that we spend after an incident.

Lack of defined information architecture is mentioned as a barrier for network incident investigation. According to ISO/IEC 27043:2015(E) The information architecture include installations of new software, hardware and policies which are indicators for the readiness processes in the organisation. Policies according to ISO/IEC 27001:2013(E) help the organizations information security and suggested as a base line for organisation to communicate improvement of information security management and other information security issues.

The respondents mention the absence of a strong architectural structure for information security in Ethiopian banks; this is an indicator of ISIM policies' absence. A recent study also strengthens the idea of the absence of ISIM policy documents and lack of participation of stockholders, plus indicates Ethiopian organizations are susceptible to information security incidents.

Lack of pre-incident analysis of digital evidence in the organisations has been observed. This has a big influence when a network attack occurs in the specified organization. Identifying incidents using tools and software and giving input for the detection process is the basic step to handle attacks easily. Banks should develop their capability according to this process. This study also mentions some banks implement global well-known and recommended IDS in Ethiopia, even if they are few.

Lack of reporting and proper recording of the chain of custody is also mentioned as an issue by the respondents on network-based investigations. This indicates that the necessity of chain of custody does not gain much attention, and the reporting of evidence is not accurate. From the study, we observe that every process has a relation, and the absence of one has a higher impact on the other. According to studies, there are no ways to report an incident in Ethiopian organizations, so the challenge began. The reporting of an incident is made on the CERT website. The investigation, reporting, and chain of custody will be handled in collaboration with the federal police.

Technology

Technology is another factor for the Banks NFR from the most known technical factors lack of tools for investigation and record-keeping are mentioned as the most alerting ones. Below are list of observed gaps regarding tools.

- Issues with analytical tools
- Monitoring tool problem like false alerts
- Familiarity of tools integrated with IDS

5.3 How to maximize the ability of collecting valid digital evidence and minimize the cost of NF during an incident

The ability of collecting valid network based evidences is maximized when an organization is ready forensically. In this result and discussion part the author revisited the ISO/IEC 27001:2013(E) which clearly states the requirements for the assessment and treatment of information security risks tailored to the needs of the organisations.

In addition to the ISO standards we referred African union convention on cyber security and personal data protection which states the principle of lawfulness and fairness of personal data processing. On the convention article 13 sub article 2 which states the collection, recording, processing, storage and transformation of data shall be undertaken lawfully, fairly and non-fraudulently (The member state of AU, 2000).

The convention also stated that data collection shall be undertaken for legitimate purpose and shall be adequate, relevant and non-excessive according to the purpose collected and processed on article 13 sub article3 a and 3b (The member state of AU, 2000).Therefore Ethiopian banks follow the convention hence they are in the continent and they should take responsibility to full fill the required criterion to collect digital evidence.

According to the study, the performance of NF is low for network attacks, which indicates the banks are missing activities that should be taken place before the incident. In advance, this can be an indicator for the maximization of cost for the investigation and a lot of time wastage according to ISO/IEC 27043:2015(E).

To maximize ability of collecting valid digital evidence, banks should consider giving employees training and awareness regarding cyber security and information handling. ISO/IEC 27035 supports Collaboration with the proper stakeholders to handle incidents and make incident management policies, making available access for communication with government, and other stakeholders will help to address outsides the box. The National information security policy of 2011 also support making policies and frameworks based on the specified structure of the policy. Having a well-structured incident management policy is expected.

Increasing the storage space of databases to save all the acquired data and minimize unauthorized persons access to a system can be considered as a way to maximize the ability to perform better digital evidence collection in addition to that organizational management communication with the IT security professionals and having a budget for recent AI-based technologies that can identify any attack easily can be implemented to make the incident detection response and analysis easier, and the log files for investigation can be accessible. This all are factors to maximize ability of digital evidence collection and in advance cost for investigation will decrease.

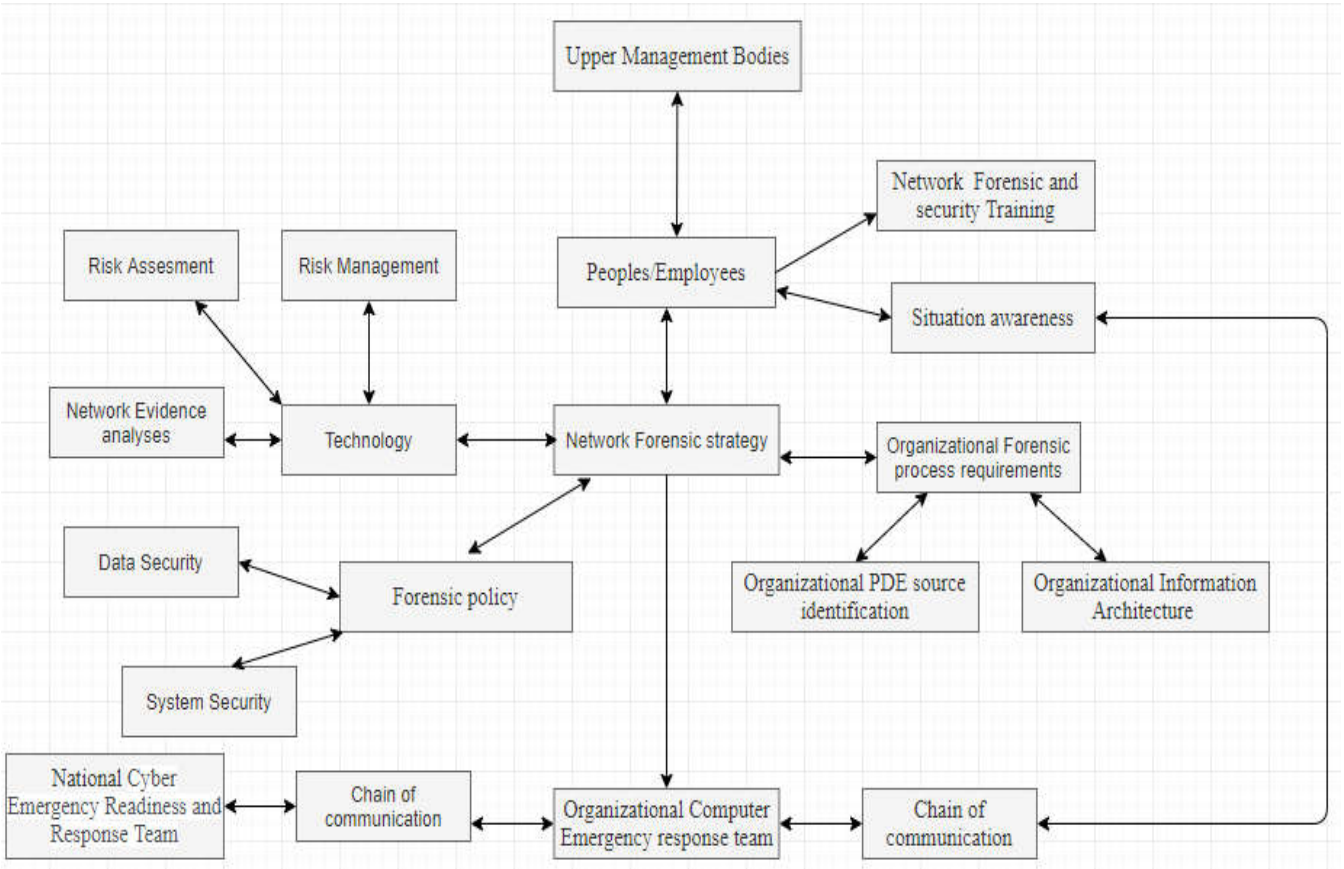

Figure 5. 4 Proposed Frame work to maximise the ability to collect valid NE and minimise cost of NF.

This section also introduced a framework that fulfils the gaps observed in the banks' NFR process and show good ways to facilitate the readiness before an incident. The frame work is based upon the ISO/IEC 27035 and ISO/IEC 27043:2015(E). It includes Technology, Forensic policy, organisational forensic processes requirements and employees or people under the NF strategy since this all should be considered for NFR practices.

The framework indicates there should be communication between an employee and the managerial organs to fill gaps regarding the budget for the NFR and the attention needed in the area. There also indicated an NFR strategy that collaborates the technology, organizational process requirements, and Forensic policy. The facilitated communication between the Organisational CERT and Ethio-CERT is also needed since it is not that visible in the real-life application; furthermore, employees need awareness of NF processes and data handling mechanisms in addition to IT security practices. The communication between organizational CERT and Employees can be considered an additional asset for improving vulnerability and having good situation awareness regarding the current or updated areas.

The model strengthens the Organisational process requirements by stressing out the Organizational PDE source identification and Organizational Information Architecture. Those processes are crucial for NF investigation, including the Risk Management, Risk Assessment, and network evidence analysis tools.

6. Conclusion

The study questions are generated based on the ISO/IEC 27043:2015(E) to understand the case of Ethiopian banks network forensic readiness practices and find out the gaps which lead the banks to high cost after an incident and generalize what should be improved to maximize the capability of digital investigation to tackle cyber and network attacks and minimize the price after an incident.

The study results have been based on the banks' IT department since the IT security team is handling the banks' infrastructural security. Incident response and handling are taken place on the specific incident management teams under the IT department. In addition to that, no one can observe the banks' current scenario related to NFR practices and processes than those employees since they are much near applying the NFR processes. The budgets for the NFR also be used through this team, and whenever an incident occurred, they were supposed to add some values on the response and data handling plus provide the information needed during an investigation since they know the listed PDE sources. Results indicate the interviewees are aware of the readiness and investigation process well than any other DF processes.

Regarding the cost analysis, risk assessment was done to elaborate whether investment on the readiness is worth it or not, and the challenges for investigation after an incident in the banks are high and financial barriers have been mentioned as a factor. The year 2020 is considered as the highest observation of incident according to the previous years, so investing in the NFR is necessary and should get attention in this case, but half of the responses indicate there is still a trend to focus on the issues after an incident than having a cost for NFR. In this section, it was challenging to find out every bank's budget on the NFR process, and the banks are not willing to share the cost details after an incident compared to their investments. But it is observable that implementing NFR is valuable to solve the investigation cost after an incident and maximize Network investigation ability in the banks.

The study covers the current reality of banks' capability of collecting, preserving, protecting, and analysing digital evidence. The Interviewees pointed out they observed their banks' unsatisfactory performance on collecting, preserving, and protecting the digital evidence and balanced understanding of digital evidence analysis. Low performance of digital evidence source identification and improper way of information handling and retention of essential data’s

has also been observed. Analysed data will be acceptable if it passes through proper pre-incident and post-incident practices to be valuable since it is easy to capture every detail. The observation of pre-incident analysis of data represented in PDE even if there are indicators like incident detection and alerting tools problem which should get attention, which is the smallest number from the total response indicates a gap in the software barriers for pre-incident analysis, and there was huge information gap observed according to this process.

The necessity of NFR for the banks is evaluated on the contextual observation of banks relating to the incidents experienced, and NFR is essential because it is mentioned that without the business interruption, NF will be handled since PDE are identified, and retrievals of network-based evidence will be painless and straightforward. The support of the evidence in the court of law measured based on data handling, storage, and retention of data, including the documentation practices in the banks IT governances and there are best practices regarding governance documentation and standard operating systems and job aids revision according to the updated contextual manners but Organisational system architecture are not well-designed for network incident investigation in most banks.

The evidence from NF investigation is not helpful and valid in legal matters and court of law; besides, an improper chain of custody and data reporting has been observed widely, which affects the proper evaluation of evidence. The awareness gap of employees regarding network attacks as a first responder leads the banks to a more complex situation.

To have an immeasurable structured NFR, Ethiopian economic institutes should improve the practice of focusing on after incident activities and give attention to the pre-incident processes and develop solid cyber security and effective investigation attacks without interrupting the business. Observed gaps on the policy and strategy preparations was indicated from the interviewee's point of view in those banks.

Developing a culture of communication with the managerial bodies and controlling the applicability of proper on-the-job training in network security to increase awareness of access limits and authority to erase data also make a network penetration test by external professionals, developing a clear system architecture for network infrastructures, provide attention for network security and have a well-organized and defined network security policies are findings from the study to maximize NF and minimize cost or in other words to develop NFR in the banks.

Partial implementation of PDE source identification is the significant indicator for minimization of the capability of NF in the banks since it is difficult to identify the access logs, and unclear pre-incident collection, storage, and handling of data have been observed. The interviewees strengthened this concept since observation of monitoring tools problem on the wrong or incorrect warnings and documentation of significant change culture is insufficient. There also have been issues in most banks with the tools that have been integrated on firewalls and IDS to collect traffics, and failure has been observed in collecting all of the desired traffic data's since a large amount of data storage space is also needed to store all evidence. Miss information regarding the pre-incident analysis of data from the employees has made the outputs unpredictable. Still, many responders indicated the pre-incident analysis has been implemented widely, which are change tracking software's as intrusion detection software's and antivirus software's and good observation on incident detection mechanisms according to the responders can be mentioned as a strength.

Banks can maximize the ability to collect valid digital evidence by indicating clear PDE source identification, improving the quality of pre-incident analysis tools and incident detection, alerting tools usage, and accuracy. In addition to that, the observed gap in collecting, preserving, protecting, and analysing digital evidence as an organization should get attention. To minimize Network forensics' cost during an incident, budgets for the NFR to maximize digital evidence usage are suggestible since more attention and budgets are for the after incident activity in most banks currently.

The study results help the actual world improve the banks' cyber and network security readiness and minimize the gaps observed in the banks' actual-world application related to NF cost. The study's inputs are gained from the employees, so it is applicable for all banks in Ethiopia since its experience is seen as a mirror for Ethiopian banks' sub-branches. The outputs can be relevant and can add value for other organizations, too, since NFR is multi-directional and becoming the target for the near future to tackle cyber-attacks. The Ethio-CERT and the organization's internal CERT's should develop organized communication, and the provided framework is also applicable for any organizational NFR preparation since it is based upon the observed gaps. Following the proposed framework will help facilitate good practice related to NFR and lead the stakeholders to communicate and solve the incidents without damaging their business.

7. Reference

Al-Mahrouqi,, A., Abdalla, S., & Kechadi, T. (2014, 10 29). Network Forensics Readiness and Security Awareness Framework. pp. 3-5.

Anson, S., Bunting, S., Johnson, R., & Pearson, S. (2012). *Mastering Windows Network Forensics and investigation.* Indianapolis, Indiana: John Wiley & Sons, Inc.

Hailu, H. (2015, JUNE 19). *AbyssinaLaw*. Retrieved from https://www.abyssinialaw.com/blog-posts/item/1545-the-state-of-cybercrime-governance-in-ethiopia

Masvosvere, D. J. (2019). A Digital Forensic Readiness Approach for e-Supply Chain Systems. *UPspace Institutional Repository*, 29-30.

Messier, R. (2017). *Network Forensics.* Indiana: John Wiley & Sons, Inc.

Ngobeni, S., & Venter, H. (n.d.). THE DESIGN OF A WIRELESS FORENSIC READINESS MODEL (WFRM).

Tan, J. (2001, July 17). Forensic Readiness. *Cambridge, MA 02139 USA*, 1-2.

(2017, 6 13). Retrieved 10 3, 2020, from ISACA: https://www.youtube.com/watch?v=ZUqzcQc_syE

Adane, K. (2020). The current status of cyber security in Ethiopia.

Agency, I. N. (2011, 09). *The Federal Democratic Republic of Ethiopia National Information Security policy.* Retrieved 2 3, 2021, from INSA.gov.et: file:///C:/Users/Dell/Downloads/National%20Informattion%20Security%20Policy.pdf

Berhanu, N. (2017, 6 23). *aau.edu.et.* Retrieved from AAU Institutional Repository: http://etd.aau.edu.et/bitstream/handle/123456789/13993/NigussieBerhanu_2017.pdf?sequence=1&isAllowed=y

Breitinger, F., & Baggili, I. (2018). Digital Forensics and Cyber Crime. *10th International EAI Conference, ICDF2C 2018 .New Orleans, LA, USA, September 10–12, 2018 Proceedings* (pp. 97-103). West Haven, CT, USA: Springer.

Bultum, A. G. (2014). Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry. *Journal of Management Information System and E-commerce*, 4.

Commission, N. P. (2016, May). *European Union.* Retrieved from Resilience Building in Ethiopia (RESET): https://europa.eu/capacity4dev/resilience_ethiopia/documents/growth-and-transformation-plan-ii-gtp-ii-201516-201920

Danielsson, J., & Tjøstheim, I. (2004, 1). THE NEED FOR A STRUCTURED APPROACH TO DIGITAL FORENSIC READINESS AND E-COMMERCE. *IADIS Internacional Conference e-Commerce* (pp. 3-6). researchgate.net.

Dhumal, M., & Rokade, M. (2020, May). An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots: A Survey. *International Journal of Current Engineering and Technology*, 4-5.

Elyas, M., Ahmad, A., Maynard, B. S., & Lonie, A. (2015, April 17). Digital Forensic Readiness :Experts perspectives on the theoretical freamwork. *Elsevier Ltd*, 74-75.

Englbrecht, L., Meier, S., & Pernul1, G. (2019). Towards a capability maturity model for digital forensic readiness. *Springs*, 4-9. Retrieved from file:///C:/Users/Dell/Downloads/Englbrecht2020_Article_TowardsACapabilityMaturityMode.pdf

Ethiopia, F. D. (2009, Septmeber). *Feredal Democratic Republic of Ethiopia.* Retrieved from INSA.gov.et: file:///C:/Users/Dell/Downloads/National%20Informattion%20Security%20Policy.pdf

Evans, J. K. (2020, 10 25). Getting started in digital forensics. (J. peters, Interviewer) Retrieved from https://www.youtube.com/watch?v=j3lgxdylktM&t=1578s

Eziga. (2019, December 6). *Ezega.com.* Retrieved November 2, 2020, from https://www.ezega.com/News/NewsDetails/7518/INSA-Aborts-Cyber-Attacks-on-Financial-Institutions

Federal Negarit Gazzete. (2013, July 23). Retrieved from https://chilot.files.wordpress.com/2013/10/national-intelligence-and-security-service-re-establishment-proclamation-english.pdf

Federal Negarit Gazzete. (2014, January 2). Information Network Security Agency Re-stablishment Proclamation. Retrieved from https://chilot.files.wordpress.com/2014/09/proclamation-no-808-2013-information-network-security-agency.pdf

Free Training. (2017, Jan 29). Retrieved 1 8, 2020, from Free Training: https://www.youtube.com/watch?v=suYhuJjlEfI

Frincke, D. A., & Popovsky1, E. B. (2007, 7 22-27). Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensic Investigations.

G, G., N, S., I, B., & N, R. (2016, 12 15). Achiving Business Excellence by optimizing Corporate Forensic Readiness.

Garba, A. (2019). A RECOMMENDED DIGITAL FORENSIC READINESS FRAMEWORK FOR NIGERIAN BANKS. *International Journal of Development Research*, 5-6.

Gazeta, F. N. (2011, November 28). *Wordpress.* Retrieved from https://chilot.files.wordpress.com/2012/02/proclamation-no-720-2011-ethiopian-feeral-police-commission-establishment.pdf

Gazeta, F. N. (2018, November 29). Proclamation NO.1097/2018. *Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia*.

Gazeta, F. N. (2018, November 29). Proclamation NO.1097/2018. *Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia*.

Gazette, F. (2014, January 2). Information Network Security Agency Re-stablishment Proclamation. Retrieved from https://chilot.files.wordpress.com/2014/09/proclamation-no-808-2013-information-network-security-agency.pdf

Gazzete, F. N. (2011, November 28). Ethiopian Federal Police Commission Establishment Proclamation. Addis Ababa, The Federal Democratic Republic of Ethiopia.

Gazzete, F. N. (2013, July 23). Retrieved from word press: https://chilot.files.wordpress.com/2013/10/national-intelligence-and-security-service-re-establishment-proclamation-english.pdf

Gebrehawariat, D., & Lessa, L. (2020). Effectiveness of Card Banking Security in the Ethiopian Financial Sector: a Gap Analysis. *Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management* (pp. 7- 9). Harare, Zimbabwe,: IEOM Society International.

Getahun, A. (2018). Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia. *smuc.edu.et*, 50-63. Retrieved from http://repository.smuc.edu.et/bitstream/123456789/5183/1/Final%20thesis%20document.pdf

Herman, M., Iorga, M., Salim, M. A., Jackson, R. H., Hurst, M., Leo, R., . . . Sardinas, R. (2020, August). NIST Cloud Computing Forensic Science Challenges. p. 6.

INSA. (2016, July 7). *INSA.gov.et.* Retrieved February 8, 2021, from file:///C:/Users/Dell/Downloads/Computer%20Crime%20Proclamation%20No.%20958-2016%20).pdf

INSA. (2019). Retrieved October 4, 2020, from https://www.insa.gov.et/

INSA. (2020). *Information Network Security Agency*. Retrieved October 4, 2020, from https://www.insa.gov.et/

ISO/IEC. (2015, 1 3). ISO/IEC 27043:2015(E). pp. 6-20. Retrieved from https://www.iso.org/standard/44407.html#:~:text=ISO%2FIEC%2027043%3A2015%20provides,investigation%20scenarios%20involving%20digital%20evidence.

ISO/IEC 27001. (2013, 1 10). Information technology ,security techniques, information security management systems requirements. pp. 11-12.

Jason, S., & Ivtchenko, D. (2016). *Implementing Digital Forensic Readiness From Reactive to Proactive Process.* Cambridge: Elsevier.

k, R., & H.S, V. (2012, 9 1). The architecture of a digital forensic readiness management system.

Karie, N. M., & Karume, S. M. (2017). Digital Forensic Readiness in Organizations: Issues and Challenges. *Journal of Digital Forensics,Security and Law*, 47-49.

Keshnee, P., & Elias, W. (2020, April). A Coordinated Communication & Awareness Approach for Information Security Incident Management: An Empirical Study on Ethiopian Organizations. p. 14.

Khan, S., Gani, A., Abdul Wahad, A. W., Shiraz, M., & Ahmad , I. (2016, March 9). Network forensics:Review taxonomy and open challenges. *Journal of Network and computer applications*, 2.

lab, K. (2019). *Kaspersky.* Retrieved November 2, 2020, from Kaspersky Security Bulletin: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

M, P Phathutshedzo ; K, R Victor ; I, R A; Venter, H S; C, Kim-Kwang R;. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *elsevier*, 5.

M, P Phathutshedzo ; K, R Victor ; I, R A; Venter, H S; C, Kim-Kwang R;. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *elsevier*, 5-11.

M.Bogale,L.Lessa & S.Negash. (2019). Building an Information Security Awareness Program for a Bank: Case from Ethiopia. *Twenty-fifth American conference on information systems* (pp. 5-6). cancun: Academiya.EDU.

Marczak, B., Alexander, G., Mckune, S., Deibert, R., & Scott, J. R. (2017, December 6). Champing at the Cyberbit Ethiopian Dissidents Targeted with New Commercial Spyware. *The citizen Lab*, 1-3. Retrieved November 15, 2020, from https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Mayunga, M. O. (2019). DEVELOPING AND ASSESSING A CYBER-RESILIENCE FRAMEWORK FOR KENYAN BANKS. *African Nazarene*, 101-103. Retrieved from http://repository.anu.ac.ke/handle/123456789/527

Ministry of Peace. (n.d.). Retrieved October 5, 2020, from https://www.mop.gov.et/web/en/about

Nlar, T. S. (2021). The Future of Armed Conflict in Africa : What Cyber Attacks on Ethiopian Government Tells Us. *SSRN*, 1.

Pui Chow, K., & Shenoi, S. (2010, January 4-6). *Advances in Digital Forensics VI.* Hong Kong, China: Springer.

Reiber, L. (2019). *Mobile forensic investigations A guide to Evedence collection,Analysis, and presentation.* New york, Chicago, San Francisco, Athens, London and other places: by McGraw-Hill Education.

Representative, H. o. (2016, July 7). Proclamation No. 958/2016 Computer crime proclamation. *The Federal Negarit Gazette*, 2-20. Retrieved from file:///C:/Users/Dell/Downloads/Computer%20Crime%20Proclamation%20No.%20958-2016%20).pdf

S.KEMP. (2020, February 17). *Digital 2020: Ethiopia*. Retrieved November 12, 2020, from Hootsuite: https://datareportal.com/reports/digital-2020-ethiopia

S.O'Dea. (2020, Feb 27). Retrieved from https://www.statista.com/statistics/749569/ethiopia-ethio-telecom-data-and-internet-subscribers/

Sachowski, J. (2019). *Implementing Digital Forensic Readiness From Reactive to Proactive Process* (Second ed.). Broken Sound Parkway NW, U.S: CRC Press.

Sathye, M. (1999, 12). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, 324-330.

Singh, A. (2019, November). A digital Forensic Readiness Approach for ransomware Forensic.

Siphon, N. J. (2016, 6). Digital forensic Readiness for wireless local area networks. *University of pretoria*, 64-88.

Siphon, Ngobeni Josian. (2016, 6). *Digital forensic Readiness for wireless local area networks*. Retrieved from UPSpace institutional repository: https://repository.up.ac.za/handle/2263/57497

Stander, A. (2010). A Digital Forensic Readiness framework for South African SME's. *Information Security for South Africa (ISSA)* (pp. 6-7). Research get .IEE Xplore.

Statistics, K. S. (2020, January 28). *Kaspersky .* Retrieved from https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

Tariku, N., & Lessa, L. (2020). Information Technology Disaster Recovery Plan (ITDRP) Framework for banks in Ethiopia. *African conference on information systems and technology* (p. 9). The african journal of information.

Teka , B. M. (2020). Factors affecting bank customers usage of electronic banking in Ethiopia: Application ofstructural equation modeling (SEM). *Cogent Economics & Finance*, 7.

The member state of AU. (2000). African union convention on cyber security and personal data protection. Retrieved from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Watson, D. L., & Jones, A. (2013). *Digital forensics processing and procedures : meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements.* USA: Elsevier.

Woldemichael , H. T. (2020). Emerging Cyber Security Threats in Organization. *International Journal of Information and Communication Sciences*, 2-4.

Worku, E., & Padayachee, K. (2020). A Coordinated communication and awareness approch for information security incident management; An Emprical study on Ethiopian organisations . *Information security incident management coordination* (pp. 118-120). The African journal of information systems,Volume 12, Issue 2, Article 1.

Yohannes, T., Lemma, L., & Solomon , N. (2019). Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis. *Resurch Gate*, 6-9.

Zewude, B. G. (2020). ASSESSMENT ON CHALLENGING THREATS OF CYBER SECURITY AND ITS EMERGING TRENDS ON SELECTED ETHIOPIAN BANKING. *Resurch Get*, 72.

8. Appendix

Appendix 1 Online Questionnaire

1. Gender Female
Male

2. Your age is 18 or less
19-25
26-30
31-40
40+

3. Occupation Governmental or public sector
Private company
Other

4. Have you observed your organisation system or network experience cyber security breaches?
Yes
No
Maybe

5. From the following most common Cyber-attacks which one has your or

	Yes	No	Maybe
Business email compromise			
Website defacement			
Malwares			
Phishing or social engineering attacks			
Distributed Denial of service (DDOS)			
SQL injection attacks			
Cross-site scripting (XXS)			
Session hijacking and man in the middle			

6. Please, rate your organisation's experience of cybercrimes or network attacks in the year 2020 comparing to the previous years?
Increasing
Decreasing
Remain the same
Not known

7. Do you know what digital forensic or investigation is?
Yes
No

8. If your answer is yes about which digital forensic process class are you aware of?

	Yes	No
The readiness processes		
The initialization process		
The acquisitive processes		
The investigative processes		
The concurrent processes		

9. How you rate the level of collecting, preserving, and protecting of digital evidence in your organization.

- Very effective
- Satisfactory
- Not effective at all
- No evidence collection mechanism established

10. Is your organisation capable to analyse digital evidences using tools and record- Keeping?

- Extremely capable
- Very capable
- Capable
- Not capable

11. Do you think the evidence from Network Forensic investigation is help ful and valid in legal matters and court of law?

- Yes
- No
- Maybe

12. Does your organisation employees aware of how to respond when Network attacks first occur?

- Yes
- No

13. From the following Digital forensic Readiness process which one of them has been implemented in your organisation?

All organisational digital evidence sources has been identified

Yes No May be

My organisation have well planned pre incident collection, storage and handling of data

Yes No May be

Pre incident analysis of data has been represent in potential digital evidence

Yes No May be

My organisation implement incident detection mechanisms

Yes No Maybe

14. Does your organisation have defined information system architecture capable of network incident investigation?

Yes No Maybe

15. How often your organisation maintains governance documentation and the standard operating procedures and job aids?

Once in a year ☐ between 3-6 months difference ☐

Whenever needed ☐ not aware of it ☐

16. Do you think a network forensic readiness cost is the highest in comparison to the cost of an investigation after an incident occurred in your organisation?

Yes ☐ No ☐ Maybe ☐

17. Please rate the level of challenges on network forensic investigation?

Small ☐ Fair ☐ Good ☐

High ☐ Extremely high ☐

18. Do you think that Network investigation findings have been reported fully and proper recording of the chain of custody applied to the potential digital evidence?

Yes ☐ No ☐ Maybe ☐

19. From the following challenges which one of them has the highest impact on the Network Forensic investigation process?

Lack of finance or budget ☐

Lack of qualified professionals ☐

Juricidical struggles ☐

Others ☐ _____

Appendix 2 Interview Questions

1. What is the purpose of NFR for Banks and what procedures to follow to fulfill the readiness?
2. How to minimize the cost of DF investigation after an incident according to Ethiopian banks?
3. What are the challenges for implementing NFR in the case of Ethiopian Banks?
4. What makes banks to be called ready forensically and what are Expectations for the future?
5. How does DFR represent as a factor for organizational cyber security?
6. How to implement NFR in Ethiopian Banks?
7. How to improve the readiness of organizations according to cyber security?
8. List of benefits banks will gain after the implementation of NFR?
9. Have you observed well organized FR in the Banking industry and Observed capability of data gathering, storage and handling in Banks?
10. Do you think investing for the readiness process is beneficial according to cost and future expectations regarding budgets for NFR?
11. Measures taken to improve the quality of evidences on the investigation?