A FRAMEWORK FOR THE SECURE CONSUMERISATION OF MOBILE, HANDHELD DEVICES IN THE HEALTHCARE INSTITUTIONAL CONTEXT

K.T. KATIVU

2017

A FRAMEWORK FOR THE SECURE CONSUMERISATION OF MOBILE, HANDHELD DEVICES IN THE HEALTHCARE INSTITUTIONAL CONTEXT

By

Kevin Kativu

Submitted in fulfilment of the requirements for the degree Doctor of Philosophy to be awarded at the Nelson Mandela Metropolitan University

April 2017

Promoter: Prof Dalenca Pottas

DECLARATION

I, Kevin Kativu (s207059581), hereby declare that the thesis for Doctor of Philosophy is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

..... (Signature)

Kevin Kativu

ACKNOWLEDGEMENTS

First and foremost, I wish to thank the Almighty God through whom, the successful completion of this study was made possible.

I wish to express my sincere gratitude to the following:

My promoter: Professor Dalenca Pottas: There are no words that can adequately express my gratitude. Having guided me through both a masters and doctoral degree you have had a massive impact on the person I am and the person I will become. Thank you.

My dear family: Patrick and Lynette Kativu, loving sisters, Patricia, Chiona and Ronia for the belief, motivation and support when I needed it the most.

Editorial: Tsitsi Gwatiringa for the immense support through the study and for your willingness to read through my work.

Participants in the study: Thank you for welcoming me in your community and guiding me through the successful gathering of the data. I sincerely hope the findings from this study will be impactful and be of relevance to you.

Expert Evaluators: Thank you for your timely feedback and your constructive evaluation of the output of this study. Your observations and suggestions have made a significant impact to the outcomes of this study.

My friends and colleagues: Too many to mention, I thank you all for the support and walking this journey with me.

Funding: The NMMU Department of Research Capacity Development for the financial support;

ABSTRACT

The advances in communication technologies have resulted in a significant shift in the workplace culture. Mobile computing devices are increasingly becoming an integral part of workplace culture. Mobility has several advantages to the organisation, one such example is the “always online” workforce resulting in increased productivity hours. As a result, organisations are increasingly providing mobile computing devices to the workforce to enable remote productivity at the organisations cost. A challenge associated with mobility is that these devices are likely to connect to a variety of networks, some which may insecure, and because of their smaller form factor and perceived value, are vulnerable to loss and theft amongst other information security challenges.

Increased mobility has far reaching benefits for remote and rural communities, particularly in the healthcare domain where health workers are able to provide services to previously inaccessible populations. The adverse economic and infrastructure environment means institution provided devices make up the bulk of the mobile computing devices, and taking away the ownership, the usage patterns and the susceptibility of information to adversity are similar. It is for this reason that this study focuses on information security on institution provided devices in a rural healthcare setting.

This study falls into the design science paradigm and is guided by the principles of design science proposed by Hevner et al. The research process incorporates literature reviews focusing on health information systems security and identifying theoretical constructs that support the low-resource based secure deployment of health information technologies. Thereafter, the artefact is developed and evaluated through an implementation case study and expert reviews. The outcomes from the feedback are integrated into the framework.

CONTENTS

List of Tables

LIST OF FIGURES

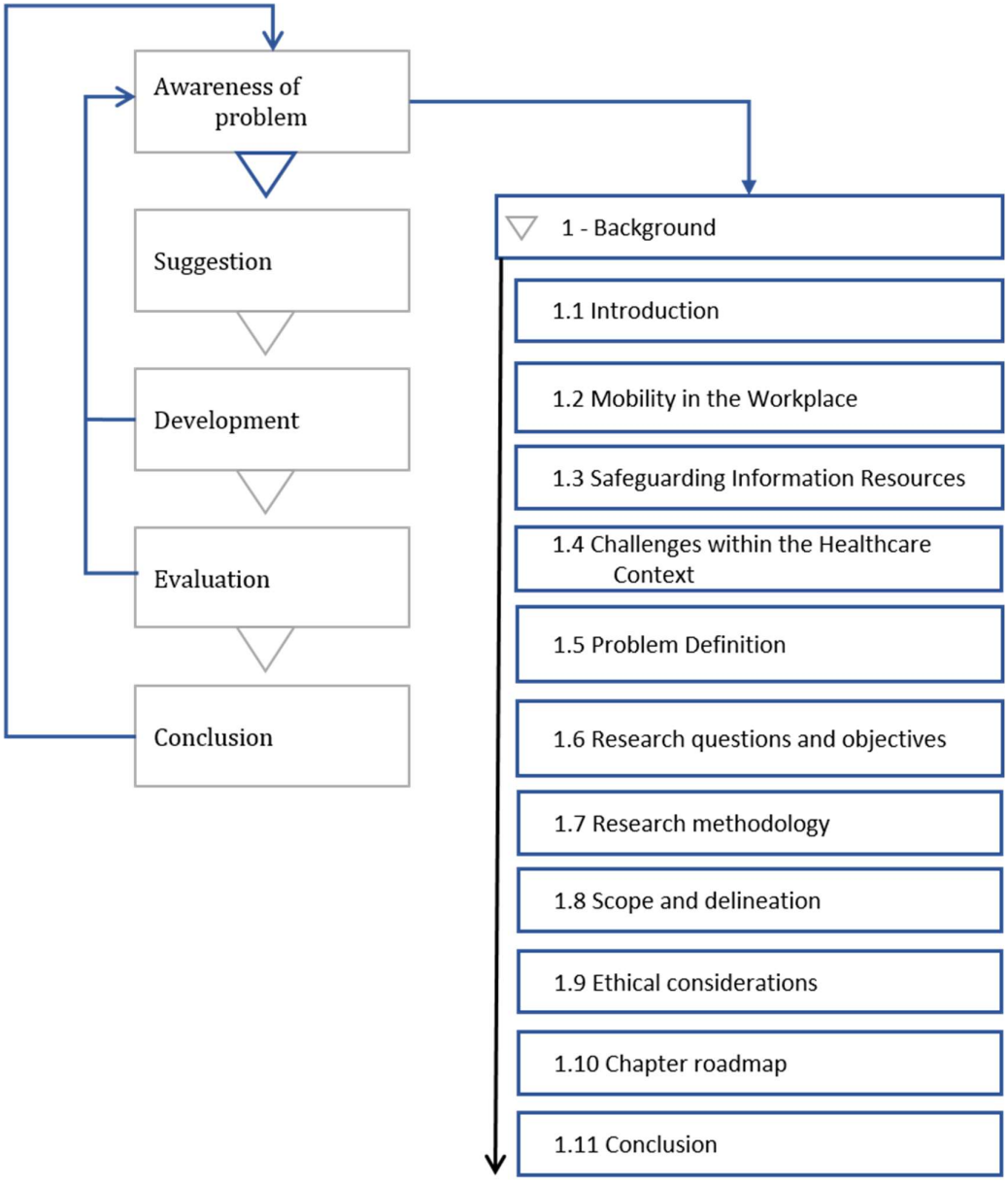
LIST OF ABBREVIATIONS AND ACRONYMS

Acronym	**Description**
BYOD	Bring Your Own Device
BYOPC	Bring Your Own PC
BYOS	Bring Your Own Service
CHW	Community Health Worker
DSR	Design Science Research
ECTA	Electronic Communication and Transactions Act
HCP	Healthcare Provider
HIA	Health Information Applications
HIS	Health Information Systems
HIT	Health Information Technologies
ICT	Information and Communication Technologies
IPD	Institution Provided Device
IS	Information Systems
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Mobile Information Management
POPI	Protection of Personal Information Act
SANHA	South African National Health Act

LIST OF APPENDICES

Appendices are listed at the end of this document and are available in the included CD.

1. BACKGROUND



1.1 Introduction

The proliferation of mobile computing devices such as smart phones, tablets and small form factor computers has improved the mobility of the health workforce. This growth has been supported by the rapid propagation of wireless infrastructure and the subsequent deployment of consumer communication networks such as 3/4G. The result is that access to resources and the ability to provide services remotely has greatly improved owing to the extended capacity availed through mobility. Mobile computing devices are increasingly finding roles in the working environment as productivity devices.

The ubiquity of intelligent mobile devices along with the increasing processing capacities have opened the doors to new levels of operational efficiency in the workplace (Allam, Flowerday, & Flowerday, 2014). Moreover, organisations are learning to embrace personal devices as employees are increasingly choosing to use their personally owned devices for both personal and work related activities due to their familiarity and comfort with these devices (Scarfo, 2012).

A significant driver of mobility has been the strong growth of the application markets and development communities. Consumers and organisations alike are increasingly finding value in the highly competitive mobile applications market. The net result of the dual role of personal computing devices is the transformation of traditionally hobbyist or media consumption to productivity devices.

In an American survey conducted by Accenture in 2011, 23% of the employees sampled were already making routine use of personal technology tools at work with a further 29% making use of these tools at least once a week (Harris, Ives, & Junglas, 2011; Marshall, 2014). Additionally, in a survey conducted by Harris Interactive and ESET, more than 80% of employed adults use some kind of personally owned device for work-related functions (Morrow, 2012). This phenomenon has been termed the consumerisation of IT.

1.2 Mobility in the workplace

Mobility is an overarching reference to technologies enabling remote employee productivity. In addition to smartphones and tablets, mobility refers to portable computing devices such as laptops and small form factor tablets. Arguments surrounding the exclusion of laptops and netbooks as mobile computing devices (Blaya et al. 2010)

have largely been deemed obsolete as these devices are increasingly becoming smaller and lighter thereby enhancing portability. Additionally, the battery life of some modern laptops can mirror that of smartphones and tablet computers. Moreover, with the ubiquity of solid state storage, these devices are now more robust and shock resistant.

Mobile computing devices are typically used to access the resources on the corporate network and offer the added flexibility of enabling employee productivity from anywhere without the limitations of time or access to a workstation (Morrow, 2012). These devices are typically battery operated and connect to wireless networks. Such mobile devices are a sub-aspect of the broader term ICTs.

The value of ICTs in the workplace cannot be overstated. Information is the lifeblood of an organisation and ICTs are the infrastructure on which information is transmitted, stored and retrieved. As technology advances, the processing capacity of computing devices continues to grow. Moreover, the packaging of computing devices is shifting significantly towards small form-factor mobile computing devices.

Consumerisation is one such trend in which consumer oriented devices are increasingly finding roles in the work environment (Disterer & Kleiner 2013). In the IT context, consumerisation describes the dual application of computing devices for personal and work related activities. In effect, the consumerisation of mobile computing devices describes the phenomenon of employees using their personally owned devices to perform work-related activities. This phenomenon has been given the term "Bring Your Own Device" (BYOD). Allam, Flowerday and Flowerday (2014) suggest that employees and managers are aware of the benefits of BYOD and the productive gains of having a continually connected workforce. Increasingly, support for BYOD is being viewed as a talent recruitment and retention tool as the younger, more tech-aware generation of employees enters the labour market (Cheston, 2012; TechTarget, 2012).

BYOD is not without its own pitfalls. A consumer-owned device by definition is one that has not been configured or locked down by the institutions' IT department (Thomson, 2012). An indirect consequence related to the co-habitation of personal and work resources is the increased workload on the corporate IT departments, which traditionally issue and control the technology that employees use to do their jobs. In addition to protecting their traditional networks and infrastructure, corporate IT is now being asked to manage technology that they perhaps did not procure or provision (TechTarget, 2012). Consequently, organisations' information systems may be exposed to rogue applications that either do not meet the security requirements of the

organisation or contain malicious code designed to compromise the organisations' information resources.

Mobile computing can provide significant benefits to organisations. One such benefit is an "always online" workforce who may voluntarily or involuntarily be extending their productive hours by constantly having access to work related resources. While beneficial for the organisation, the inability to disconnect from work may have a negative effect on the employee's personal time. It is commonplace for organisations to subsidise or completely absorb the cost of mobile computing devices for their employees. These devices have been termed IPD's (institution provided devices).

1.3 Safeguarding information resources

As mobile computing devices increasingly interact with the organisational information system, new challenges pertaining to the security of information accessible through these devices emerge. Mitigating measures such as antivirus / antimalware utilities and mobile device management tools (MDM) have drawn the attention of organisations as a means through which to secure information resources. Liu, Moulic and Shea (2010) describe MDMs as software suites designed to provide an enterprise-level management platform to system administrators.

There are several variations to software suites providing similarly oriented services, for example, Scarfo (2012) identifies and describes mobile information management tools (MIM) as typically cloud based services that manage the security aspects of files and documents synchronised across different devices. Scarfo (2012) further identifies mobile application management tools (MAM) as applying only to specific applications and not the whole device. This provides a sandbox type environment where an application can be isolated for security purposes.

However, a lack of criteria to evaluate the effectiveness of MDM systems in providing basic security functions needed by enterprises and whether such functions have been securely and reliably developed (Rhee, Jeon and Won, 2012) has hindered the adoption rates. Additionally, factors such as the higher computational costs (Houlding, 2011), the main focus on device security rather than file security (Romer, 2014), and the workers' view of the limitations placed on the devices (Cheston, 2012) add to the complexity in the decision making processes. Moreover, Gartner estimates that by 2016, 20% of enterprise BYOD programs will fail due to the deployment of mobile device management (MDM) measures that are too restrictive (Steiner, 2014; Willis, 2014).

The net result is that while MDMs, MAMs and MIMs have to some degree offered control mechanisms to remediate the security challenges introduced by enabling BYOD, these measures are still to convince the corporate communities and their employees.

Other tools such as antimalware / antivirus software provide an application level barrier to software based threats. As tried and tested interventions, these tools have become the mainstay across a wide range of devices, however, they are limited to software / intrusion related threats.

The area of focus in this study is the secure consumerisation of mobile computing devices (particularly Institution Provided Devices) for the delivery of health related services in the rural health context. For the purposes of this study, the consumerisation of mobile computing devices is an over-arching reference to institution provided devices that are used productively in the work environment. The following sections provide context to the focus area.

1.4 Challenges within the healthcare context

A principal challenge associated with the use of mobile computing devices in the healthcare context revolves around the question: *how to secure the patients' personal information so as to address their privacy concerns* (Alexandrou and Chen, 2014). The use of mobile computing devices in healthcare institutions would be to facilitate the generation of and access to patient information such as EMRs from anywhere at any time. Consequently, unmanaged personal devices presently pose a security risk to the institution administration and to the general public.

Romer (2014) suggests that technological revolutions such as consumerisation tend to be a *'double edged sword'* because the perceived benefits bring along a new set of security threats. As a result, organisations and enterprises are faced with the increasing need to introduce regulatory measures to securely integrate these devices within the workplace. A direct consequence is that the consumerisation momentum is greatly reduced and in some instances stalled until suitable controls are put in place. Proceeding without adequate security controls can expose information security vulnerabilities which could compromise the security of the information resources. A precursor to the establishment of security controls is an in-depth understanding of the security challenges involved.

Marshall (2014) identifies 5 key challenges that can be associated with mobile computing in healthcare:

1. Security: Identified as the foremost concern. According to the Ponemon Institute (2014), criminal attacks on healthcare organisations in the United States of America have increased 100% since 2010.
2. Governance: Protocols, practices and guidelines are a prerequisite for any successful BYOD program. However, Marshall (2014) notes how many of the organisations permitting BYOD have no formal policies.
3. Legislation: Enforcing legislative requirements on personally owned devices may prove to be a challenge. Institutions have to comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), The Health Information Technology for Economic and Clinical Health (HITECH) Act, and in the South African context, the Protection of Personal Information (POPI) Act. Enforcing measures to ensure legislative compliance on unmanaged devices is a complex affair.
4. Device type: Allowing employees the room to choose their preferred device may present interoperability challenges regarding the operating platforms. Additionally, security requirements differ across platforms. This has the potential of creating security loopholes.
5. Internet dependency: An influx of devices requesting the same resources may overwhelm the existing communications infrastructure. Mansfield-Devine (2012) points out that BYOD increases the demand on existing communications infrastructure resources and this inevitably will increase the demand for end user support (Niehaves, Köffer, Ortbach, & Katschewitz, 2012). The healthcare environment has very little tolerance for system downtime because of the critical nature of their activities.

In addition to understanding the security challenges, organizations must identify what they consider their information assets and the type of information they need to protect.

To give a broad indication of the impact of mobility in the global healthcare context, in an American survey conducted by Aruba Networks (2012) on health mobility trends indicated that Electronic Medical Records (EMRs) were the most commonly supported applications within healthcare institutions with 60% of the sampled institutions indicating their desire to enable these applications on mobile devices and smart-phones. By the same token, 85% of the sampled institutions allowed physicians and staff Wi-Fi access but only 8% granted full access to the hospital network with user owned devices. The results of the survey indicate that an apprehensive approach is being taken in

allowing user device access on the hospital network. The supporting infrastructure in the resource-rich settings means greater connectivity and consequently greater risk.

In rural, remote and resource constrained settings, mobile computing devices can be a cost effective means of health service delivery. However, the infrastructure to support secure operations are minimal and at times none existent. However, social circumstances and the dissimilar exposure to technology may affect the risk profile favourably in such environments. Consequently, resource constrained settings such as rural communities are likely to experience a different or unique set of security challenges.

1.5 Resource constrained settings

In the context of this study, resource constrained settings can be described as geographical areas/communities characterised by a shortage of skilled human and infrastructure resources. A consequence of the lack of skilled labour is the prevalence of task shifting. Task shifting can be described as the redistribution of medical and health service responsibilities from qualified health professionals to health workers with less training and qualifications (Agyapong, Farren, & McAuliffe, 2016; Daniels, Clarke, & Ringsberg, 2012; Heunis, Wouters, Kigozi, Rensburg-, & Jacobs, 2016; WHO, 2008). This problem is particularly severe in sub-Saharan Africa (Gupta & Dal Poz, 2009) and has been compounded by the persistent migration of skilled health care workers to 'greener pastures' in the more urbanised environments (Schrecker & Labonte, 2004).

Infrastructure resources include telecommunications systems, electricity supply, water supply and road network infrastructure (Fox & Porca, 2001). The lack of infrastructure resources has a negative effect on the ability of organisations to reach patients and deliver the required health services thereby reducing the capacity for health service delivery.

The reduction in service delivery capacity has highlighted the potential role for ICTs in community-centric solutions that leverage technology. However, the prevalence of the skilled labour shortage and consequential task shifting means less qualified health workers are given responsibilities that may sometimes be beyond their abilities. Consequently, some best operating practices may be overlooked potentially creating room for vulnerabilities in the health service delivery process. Braun, Catalani, Wimbush and Israelski (2013) advocate that mobile technology can potentially enhance the capacity of health workers to take on new and challenging tasks, particularly collecting

complete, timely and accurate health data for field-based research and providing health care services in the field with fewer errors and higher adherence to protocols. In order to take advantage of these mobility tools, an emphasis must be placed on ensuring health workers understand how to use the information systems in a manner that does not compromise the confidentiality, integrity and availability of the health information that is stored or transacted on these tools and devices.

1.6 Problem definition

As discussed in section 1.4, mobile computing devices can potentially enhance the productive activities of health workers. This is particularly true in rural settings where the infrastructure challenges necessitate mobility technologies and mechanisms such as BYOD and IPDs to reach patients who are unable to come to seek health services on their own accord. Electronic Medical Records have facilitated mobility by allowing medical practitioners to travel between locations while remaining connected to the information systems that facilitate the retrieval and modification of patient data (Alexandrou & Chen, 2014). Conversely, Moyer (2013) suggests that at the present day, the potential cost associated with security breaches, theft and loss associated with BYOD seem to outweigh the gains of allowing the use of personal mobile devices in healthcare environments. The problem is compounded in the rural health context where the technical skills / know how and financial resources required to implement security controls are typically scarce. The problem to be addressed in this study is subsequently stated:

> The lack of tried and tested low-resource solutions to facilitate the secure use of mobile computing devices in rural health settings is a significant barrier to ICT driven improved healthcare access and service delivery.

1.7 Research questions and objectives

The following research questions and objectives were identified as appropriate statements of intent in an effort to address the problem:

1.7.1 Primary research question

How can low-income community based rural healthcare providers leverage existing resources to safeguard health information?

1.7.1.1 *Secondary research questions*

i. What are the elements of health information systems security?
ii. What contextual mechanisms can be deployed to safeguard health information?
iii. How can low-income community based rural healthcare providers identify contextual resources for safeguarding health information?

1.7.2 Primary research objective

Develop a framework that facilitates the identification of contextual resources to develop health information security controls that facilitate the secure use, storage and transmission of health information in a resource constrained setting.

1.7.2.1 *Secondary research objectives*

i. Identify the elements of health information systems security.
ii. Identify mechanisms and constructs that can be deployed to facilitate the security of health information.
iii. Develop context-aware mechanisms for the identification of resources that facilitate the safeguarding of health information in a low-income community based rural healthcare setting.

1.8 Research methodology

According to Hevner, March, Park, and Ram (2004), the design-science paradigm seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artefacts. The goal of this study is to develop an artefact in the form of a framework to support secure consumerisation of IT in healthcare and therefore, the design science paradigm is most appropriate. This study follows the design science process informed by Kuechler and Vaishnavi (2008) (figure 1-1) and is guided by the seven guidelines to design science research as put forward by Hevner and Chatterjee,

(2010) and Hevner et al., (2004). The research process is guided by 5 activities which are subsequently discussed.

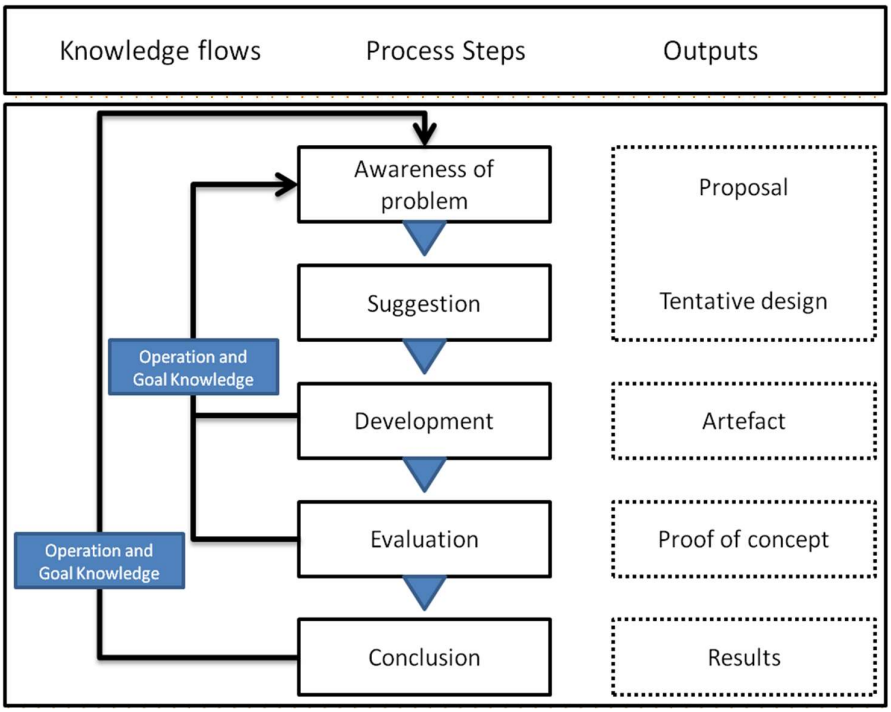


Figure 1-1: Design Science Research Process (*adapted* Vaishnavi and Kuechler 2004)

Awareness of Problem: The problem to be addressed in the study is identified.

Suggestion: The constructs of the artefact are proposed.

Development: An initial artefact is assembled utilizing the identified constructs.

Evaluation: The artefact is evaluated to establish utility, quality and efficacy according to the requirements of design science.

Conclusion: In this phase, the findings of the study are published.

This study was conducted in two phases which represent a search and design phase and a development and evaluation phase. In the search and design phase, an in-depth literature review was conducted to establish the background and present state of health information systems and threats to health information. Moreover, the information security requirements were discussed.

In the development and evaluation phase, the framework was developed and evaluated through the use of a case study, scenarios and expert evaluations. Table 1-1 summarises the research methods applied in the study.

Table 1-1: Research Objectives and Associated Methods

	Data Collection	Data Analysis	Evaluation	
	Literature Review	Argumentation	Case Study	Expert Evaluation
RO. 1	*	*		
RO. 2	*	*		
RO. 3	*	*	*	*

The research protocol employed in the study is further expounded in Chapter 2.

1.9 Scope and delineation

Design science artefact performance is strongly related to the environment in which it operates, consequently, an incomplete understanding of that environment can result in inappropriately designed artefacts (March & Smith, 1995). In defining the confines in which this study was conducted, the following factors should be taken into consideration:

1. The study refers to BYOD as an overarching reference. The data collected in this study was specific to IPDs.
2. Data was collected primarily in the rural Eastern-Cape province of South Africa although the results may be generalisable to other similar contexts.
3. The output of this study is aimed at solving a rural health specific problem and the output may not be applicable in urban environments.

The output of any research study is influenced by the environmental variables that may be unique to a particular context. This study was conducted in Mbashe Municipality in the rural Eastern-Cape Province of South Africa. StatsSA (2011) has the total population in the municipality listed as 254,909 with 38% of the population between the ages of 0-14, 53,9% between 15-64 and the remaining 8.1% beyond the age of 65. An estimated 50% of the households have access to electricity and 76.8% of the population has access to a cell phone. Employment rates are typically low which is characteristic of most rural

settings. The environmental constraints of the context present a unique opportunity for a research study of this kind.

In an effort to understand the environmental context, the researcher was actively involved in the day-to-day activities of the selected institution for a period of six months. In this period, the workflow and work practices of community health workers was investigated and day-to-day challenges were identified. The specific names of the participating institution and individuals have been kept confidential according to the ethical requirements.

The organisation selected for the study trains, equips and deploys community health workers within the community to deliver health related services focusing on non-communicable diseases. The community health workers are equipped with small form-factor mobile computing devices (netbooks) and are given training on the use of these devices and the resident health applications. The organisational structure consists of managerial staff, community health workers (CHWs) and IT / technical support personnel mostly recruited from within the local communities. Additionally, the organisation maintains dialogue with the community by engaging members of the community as advocates for the healthcare programs. The organisation provides health service support and patient screening in the community and at the time of writing, had been in contact with at least 35 000 patients.

1.10 Ethical considerations

When conducting research involving human subjects, the following three ethical aspects are to be considered:

- Respect for persons – this requires that the participants enter into the research voluntarily and with adequate information.
- Beneficence – researchers are obliged to give forethought to the maximisation of benefit and reduction of risk that might occur as a result of the research investigation.
- Justice – this is concerned with the fairness in distribution. If participants are not selected on an equal basis, an explanation as to why there is inequality in the selected should be present (The National Commission for the Protection of Human Subjects of Research, 1978).

Ethical clearance was sought and obtained from the Nelson Mandela Metropolitan University and is attached as appendix II.

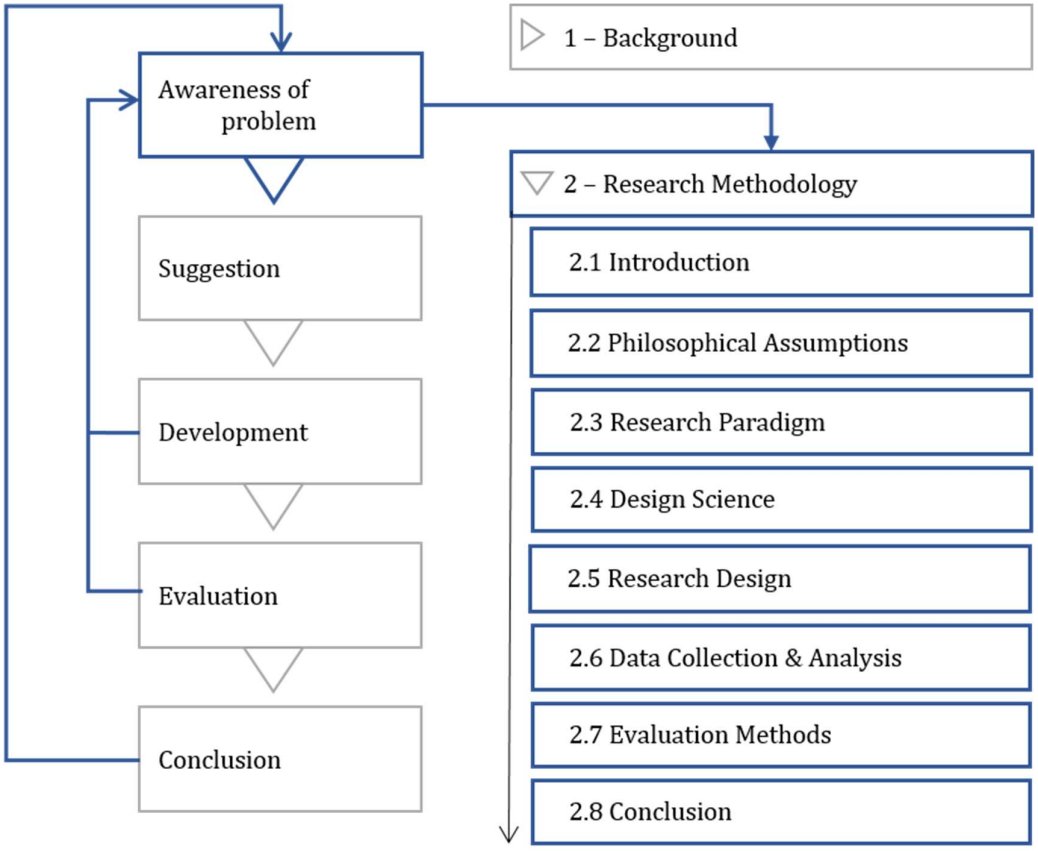
1.11 Chapter roadmap

	Description
Chapter 1:	This chapter presents the background and motivation for the study. The research questions, objectives and methodology are presented and subsequently addressed in more detail in the following chapters.
Chapter 2:	Chapter 2 presents the research philosophical alignment and research protocols used in addressing the research objectives stated in this chapter. This chapter additionally discusses the research instruments employed in this study.
Chapter 3:	Chapter 3 discusses health information technologies and the security implications surrounding the use of technology in the delivery of health related services. Additionally, this chapter identifies the key factors to be addressed in order to ensure health information is securely managed.
Chapter 4:	Discusses the theoretical constructs that lend a unique perspective to this study. These constructs form the basis on which elements that constitute the framework output of this study are developed.
Chapter 5:	The elements identified in the previous chapters are systematically assembled into a framework that consists of theoretical constructs together with guidelines for its deployment.
Chapter 6:	Presents a systematic analysis of the findings from the case study in which the framework was applied. This chapter forms part of the evaluation activities of the thesis.
Chapter 7:	The chapter presents the outcomes of the expert evaluations of the framework.
Chapter 8:	Concludes the study by discussing the research objectives and the point throughout the study in which they were addressed.

1.12 Conclusion

This chapter presented the background and motivations for this study. The research alignment, process and methods selected to meet the research objectives were discussed and motivated. On conclusion of this chapter, the first activity in the design science research process (Awareness of problem) had been achieved. Chapter 2 expands the discussion on the research protocol introduced in this chapter.

2. RESEARCH METHODOLOGY



2.1 Introduction

Chapter 1 presented the background of the research area and the motivation for embarking on this research journey. Moreover, the chapter discussed the research questions and objectives addressed in this study. The chapter concluded by briefly outlining the envisaged research methodology, the scope of the study and presenting the outline of the chapters to follow.

This chapter expands the discussion on the research methodology presented in Chapter 1 Section 1.7. The objective is to present the research methodology in a manner that facilitates replication.

The chapter leads by discussing the philosophical assumptions that influence the selection of the research paradigm. Thereafter, a presentation of the research design ensues structured according to the two phases as discussed in Chapter 1 section 1.7. The chapter proceeds to discuss the data collection methods, data analysis techniques and concludes by presenting the evaluation methods.

2.2 Philosophical assumptions

Philosophical assumptions define approaches to view the world and its truths, thus, the philosophical alignment of a researcher will influence the way knowledge is studied and interpreted. Research paradigms are distinguished by the way they interpret the philosophical assumptions.

The research philosophy outlines the perspective or "world-view" from which a researcher studies the subject area. Lincoln and Guba (1990 p.17) describe the world-view as *"a basic set of beliefs that guide action"*. In conducting a research study, the philosophical alignment of the study influences how the researcher makes sense of the phenomena observed or measured and is a critical aspect in defining the research direction and output. Four philosophical assumptions are subsequently discussed (Iivari, 1991).:

Epistemology – these are assumptions concerned with the nature of the scientific knowledge about a phenomenon under investigation.

Ontology – studies the assumptions made about the phenomenon under investigation.

Methodology – is concerned with the study of research methods.

Axiology (ethics) – concerned with the responsibility of the scientist for the consequences of his / her research and its results.

The following section discusses three research paradigms considered for this study and motivates a selection.

2.3 Research paradigm

As discussed in section 2.2, philosophical assumptions influence the selection of a research paradigm. The term 'research paradigm' essentially defines a set of assumptions, concepts and practices that influence the way one seeks to understand. This section discusses the most prevalent research paradigms.

2.3.1 Positivism

Positivistic researchers believe in a single reality, which can be measured and known. Cresswell (2014) argues that knowledge developed through the positivist "lens" is based on careful observation and measurement of the objective reality. Positivism is generally aligned with the natural sciences (Lewis, Saunders, and Thornhill, 2007) and emphasises the use of existing theory to develop hypotheses. Positivism takes on a contrast to the deductive, theory-testing approach (Cunliffe, 2010) and leans towards quantitative methods of inquiry although qualitative data can be produced (Hussey & Hussey, 1997).

For the purposes of this study, positivism is deemed inappropriate as the objectives of this study aim to unearth the underlying variables that contribute towards the assembly of a framework. This requires an in-depth understanding of the context, a requirement that does not play to the strengths of the positivist philosophy.

2.3.2 Interpretivism

Interpretivist researchers seek to understand through interpretation where the positivist researcher seek to quantify and measure. Interpretivists believe in the possibility of an existence of different truths that are influenced by experiences, beliefs and values. The objective of interpretivism is to uncover the underlying meaning of phenomena. Van Maanen (1983, p. 9) describes interpretivism as *"an array of interpretative techniques which seek to describe, decode, translate and otherwise*

come to terms with the meaning, not the frequency, of certain more or less naturally occurring phenomena in the social world".

The researcher engages with the phenomena within its context in an effort to understand the cause of the phenomena. The nature of interpretivism entails the use of qualitative research methods, however, as stated by Guba and Lincoln (1994), the choice of qualitative versus quantitative methods is secondary to the choice of paradigm since both qualitative and quantitative methods of inquiry can be used in either paradigm.

Interpretivism is a candidate for this study, however, this research study is problem centred and the exploratory nature of interpretivist research may not be the most ideal in these circumstances.

2.3.3 Pragmatism

Donley and Grauerholz (2012) describe the pragmatist world-view arising out of actions, situations, and consequences rather than antecedent conditions as found in positivism. The design world-view adopts a pragmatist epistemology (Kuechler & Vaishnavi, 2008). Creswell (2008) further suggests that pragmatists adopt a problem centred approach with a real-world practice orientation. Pragmatism has been identified as a viable alternative to positivism and interpretivism (Goldkuhl, 2004).

Pragmatic researchers believe in a constantly changing reality and therefore do not align with either positivism or interpretivism but rather adopt the best method to solve the problem at hand. Pragmatism argues that the most important determinant of the research philosophy adopted is the research question, the requirements that stem from the research question subsequently determines which research approach is better suited to addressing that particular question (Saunders et al. 2007).

The pragmatism school of thought considers practical consequences or real effects to be vital components of both meaning and truth (Johnson, Onwuegbuzie, & Turner, 2007). Hevner et al. (2004) and March and Smith (1995) emphasize a pragmatic-driven research process and emphasize the development of artefacts as a DSR output. This study adopts the pragmatist view of design science.

Table 2.1 summarises the philosophical assumptions associated with the research paradigms discussed.

Table 2-1: Philosophical Assumptions (Kuechler & Vaishnavi, 2008; Morgan, 2007, 2014)

		Philosophical Assumptions			
		Ontology	Epistemology	Methodology	Axiology
Research Paradigm	Positivism	Single stable reality	Objective	Experimental Quantitative Hypothesis testing	Truth prediction
	Interpretivism	Multiple realities	Subjective	Interactional Interpretation Qualitative	Contextual understanding
	Pragmatism	Constantly changing reality	Intersubjectivity	Dependent on research question	Utilitarian

2.4 Design science

Gregor and Hevner (2013) identify design science research as a perspective within information systems research that focuses on ICT related artefact development. The design science research paradigm branches off information systems research and focuses on the development of artefacts that address a given need/problem relating to information and communications technology (Weber, 1987). Moreover, design is described by Peffers et al. (2006) as the act of creating an explicitly applicable solution to a problem.

The aforementioned descriptions lend credence to the conclusion that design science is fundamentally, a problem solving paradigm (Hevner et al., 2004). The authors' description established the design science research paradigm as one that *"seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts".*

The use of the design science research (DSR) approach encompasses the creation of artefacts and artificial systems with the aim of solving an identified problem (Baskerville, 1999; Hevner, March, Park, & Ram, 2004). March and Smith (1995) describe research activities in design science as consisting of a build and evaluate aspect. The build aspects refer to the construction of an artefact, furthermore, this aspect seeks to demonstrate that such an artefact can indeed be constructed. The evaluate aspects refer to the

development of evaluation criteria that can be used to assess the artefact performance against those criteria.

Typical DSR artefacts include constructs, algorithms human/computer interfaces, system design methods, models, frameworks, management policies, and full system instantiations (Gregor & Hevner, 2011).

2.4.1 Motivating design science

Having established the intent to identify contextually unique constraints and develop a solution that addresses the challenges faced in the environmental context in the research objectives, design science emerges as the appropriate paradigmatic alignment. Rittel and Webber (1973), and Brooks (1987) [as cited in Hevner & Chatterjee (2010)] suggest that design science inherently addresses what have been described as "wicked problems". Amongst the characteristics listed for wicked problems, the (1) unstable requirements and constraints based on ill-defined environmental contexts, and (2) a critical dependence upon human social abilities (e.g., teamwork) to produce effective solutions are specifically relevant to the context of this study. It can therefore be inferred that this study seeks to address "wicked problems" and the design science research paradigm is well suited for the task. The following section discusses the prescribed guidelines for conducting and evaluating good design science research.

2.5 Research design

Hevner and Chatterjee (2010) propose a list of seven design science research guidelines to evaluate a design science research project. These guidelines will be used in this study to ensure that the key aspects of a design science research project are rigorously addressed.

Design as an artefact - Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.

i. **Problem relevance** - The objective of design science research is to develop technology-based solutions to important and relevant business problems.
ii. **Design evaluation** - The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
iii. **Research contributions** - Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.

iv. **Research rigour** - Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.

v. **Design as a search process** - The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.

vi. **Communication of research** - Design science research must be presented effectively to both technology-oriented and management-oriented audiences.

The goal of this study was to develop an artefact to facilitate the secure consumerisation of mobile computing devices in community based rural healthcare environments. This entails the development of an artefact which, in the context of this study, manifests as a framework. The design science paradigm was identified as appropriate in addressing the objectives of this study.

The research follows the design science process informed by Kuechler and Vaishnavi (2008) and is guided by the seven guidelines to design science research as put forward by (Hevner et al., 2004; Hevner & Chatterjee, 2010). The research process has been divided into two phases as described in section 1.7 and the two phases are subsequently discussed and illustrated in figures 2-1 and 2-2 respectively.

2.5.1 Phase 1 – Search and design

Phase 1 (figure 2-1) incorporated the first two activities of the research process, namely; awareness of the problem and suggestion. A brief description of what the first two activities entail follows.

Awareness of Problem:

According to the model presented by Kuechler and Vaishnavi (2008), all design begins with awareness of problem. Hevner et al. (2004) suggest that a design science research project seeks a solution to a real-world problem. It is therefore essential that the problem is thoroughly investigated and well defined in order to provide a functional solution.

In this initial activity, literature on the background to the research area was explored in an effort to establish the various influences and identify the specifics surrounding the problem area. This activity is presented in Chapter 1 of the thesis.

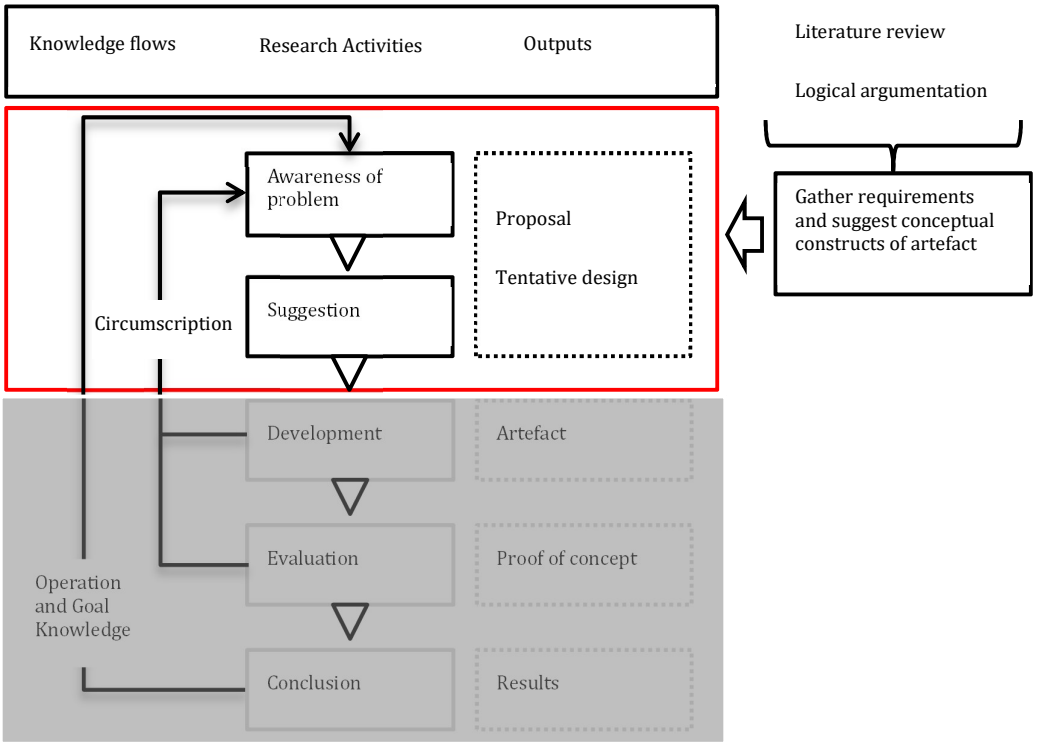


Figure 2-1: Research Process - Phase 1 – Search and Design

Suggestion:

Drawing from the problem, a suggestion for the problem solution was formed. This process was aimed at establishing the conceptual constructs that can be included in the artefact. This activity is reported in Chapters 3 and 4.

2.5.2 Phase 2 – Development and evaluation

In this phase, the output of the suggestion activity was carried over and iteratively developed into a solution that meets the stated primary objective of the study. This phase is illustrated in figure 2-2 and a brief discussion of the activities in this phase ensues.

Development:

This was an iterative activity following from the suggestion activity in phase 1 and drawing input from the evaluation activity in phase 2. An initial artefact was assembled and incrementally improved to incorporate the findings from the evaluation activity. The development activity is presented in Chapter 5 of the thesis.

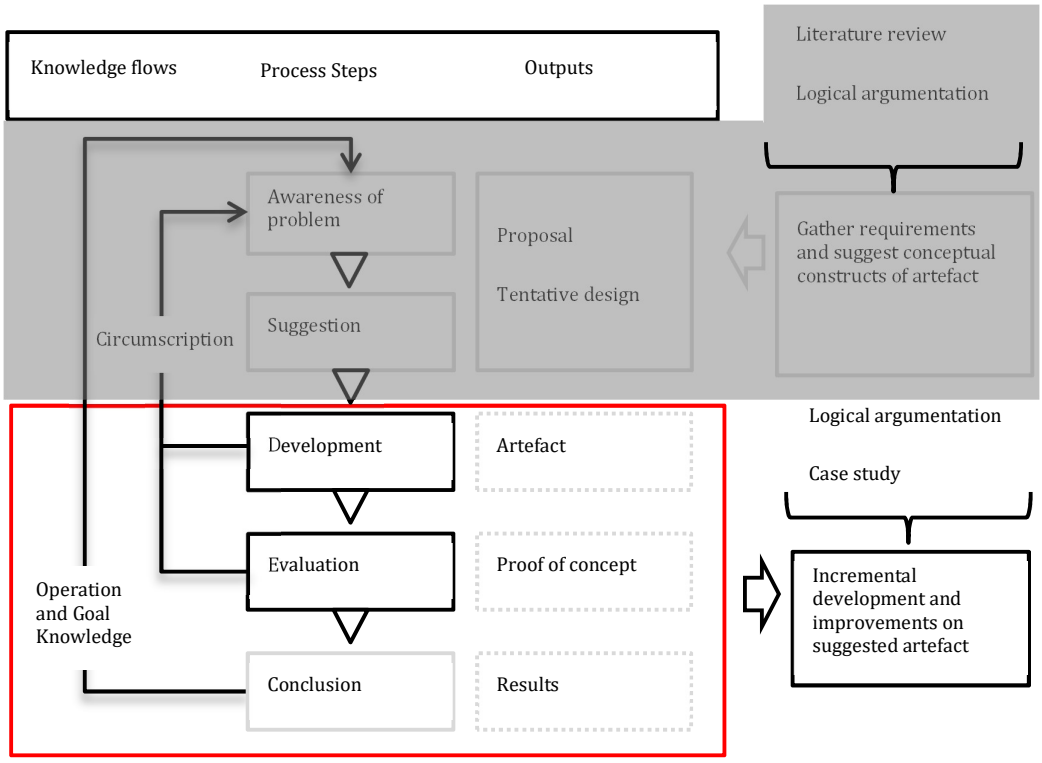


Figure 2-2: Research Process - Phase 2 – Development and Evaluation

Evaluation:

The evaluation activity was twofold and incorporated a case study to demonstrate the application of the framework and expert evaluations through the use of illustrative scenarios to determine whether the framework adequately addresses the stated problem and proposes a functional solution that is both novel and intuitive. Chapters 6 and 7 present the evaluation activities.

Conclusion:

In this activity, the findings of this study were published. At the time of writing, the study culminated in the following outputs:

- Publications in conference proceedings (refer to page 160)
- Documentation in the thesis.

2.6 Data collection and analysis

This section discusses the methods used for data collection and analysis during the problem awareness, suggestion and development activities of the research process. The methods relevant to the evaluation activity are discussed in section 2.7. The individual

methods are subsequently discussed. Cassel and Symon (1994) note how research methods are not confined to the quantitative or qualitative approach, but rather depend on the underlying epistemological assumptions. As discussed in section 2.3.3, this study adopts the pragmatism research paradigm which entails the selection of research methods based on the identified need.

2.6.1 Literature reviews

The scope limitations that are characteristic of research studies require that the researchers rigorously and systematically locate, assess and aggregate the outcomes from studies related to a particular topic of interest. A literature review is important in ensuring the researchers understand the topic, are aware of the existing knowledge surrounding the topic, how it has been researched and the main issues that exist (Hart, 1998).

The objective of a literature review is to come to an objective summary of the relevant evidence as presented by fellow researchers in the field (Brereton, Kitchenham, Budgen, Turner, & Khalil, 2007). This view is supported by Onwuegbuzie, Leech, and Collins (2012) who suggest that a literature review allows the researcher to learn from the ideas and experiences of other researchers in the same field of interest.

According to Webster and Watson (2002), a well-structured literature review is concept-centric, meaning the concepts determine the organising framework of a review. An alternative approach is Author-centric and is primarily concerned with summarising reviewed documents, however, as suggested by Webster and Watson (2002), this technique fails to synthesise the literature. A well synthesised review expedites the research process and avoids unnecessary duplicity where conclusive evidence has been gathered (Onwuegbuzie et al., 2012).

The literature review for this study was conducted in two parts and is presented across two chapters. The first chapter (Chapter 3) investigates the delivery of a secure information-rich healthcare service seeking to identify the elements of health information systems security. The second chapter (Chapter 4) discusses the theoretical constructs that form the foundations and are the basis upon which the artefact is developed and evaluated.

2.6.2 Logical argumentation

Logical argumentation is essentially a dynamic dialogue between a persuader and a persuadee (Kraus, Sycara, & Evenchik, 1998). The objective of this dialogue is for the persuader to put forward a convincing argument (defined by Simon, Erduran and Osborne (2006) as the substance of claims, data, warrants and backings that contribute to the content of an argument) in an effort to have their intentions accepted by the persuadee.

Gordon and Walton (2009) describe an argument as linking a premise to a conclusion and infer that if the premise is accepted, then the argument, if good, lends weight to the conclusion. Toulmin developed an argumentation pattern which illustrates the structure of an argument in terms of an interconnected set of constructs discussed as follows: (Erduran, Simon, & Osborne, 2004):

Claim – Described as a claim put forward for public acceptance

Data – Evidence to support the claim

Warrants – Provide the link between the data and the claim

Backings – Evidence to strengthen the claim

Rebuttals – Circumstances in which the claim would not hold true

Toulmin's argumentation pattern has been typically used as a framework for defining arguments (Erduran et al., 2004) . The framework shows the relationship between the constructs as illustrated in figure 2-3.

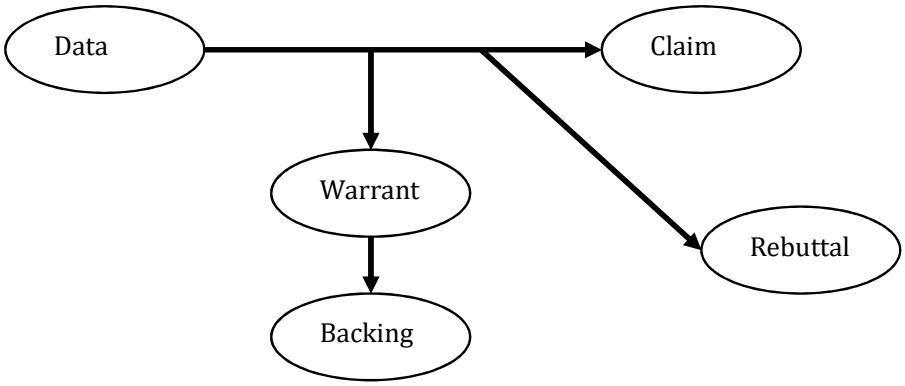


Figure 2-3: Toulmin's Argumentation Pattern

Hitchcock and Verheij (2006) interpret the model as *"what is the claim; what is the ground; how is the step from the ground to the claim warranted"*. Argumentation is employed in this study with the intent to synthesize views (premises) from different authors into a cohesive informed conclusion. Logical argumentation was employed extensively in the suggestion and evaluation phases of the study.

Suggestion: Consensus regarding health information systems security and the conceptual perspectives through which contextual information security could be promoted was established.

Evaluation: The lessons learnt from the case study together with the feedback from the evaluators was logically argued to provide input into the development activities. Findings from literature are argued against the findings from case study in an effort to determine the cause of possible disparities and to further substantiate corroborating arguments. Additionally, findings from the case study were argued against those from the expert evaluations to establish consensus on the requirements of the framework application.

2.7 Evaluation methods

In order to ensure that the developed artefact addressed the needs of the intended users, while making a contribution to the body of knowledge surrounding health information security in rural communities, the artefact had to be rigorously evaluated. This was done through the use of a case study and expert evaluations as mentioned in section 2.5.2.

> *"The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods" (Hevner & Chatterjee, 2010 pp)*

Pries-heje, Baskerville, and Venable (2008) identify evaluation of DSR as being either ex post or ex ante and describe the two approaches as being dependent on whether the artefact or the search process is being evaluated. Ex ante evaluation can be used to assess an artefact before its construction whereas ex post evaluation can be used to assess an

instantiated artefact (Prat, Comyn-Wattiau, & Akoka, 2014). Figure 2-4 illustrates the distinction between the two evaluation approaches.

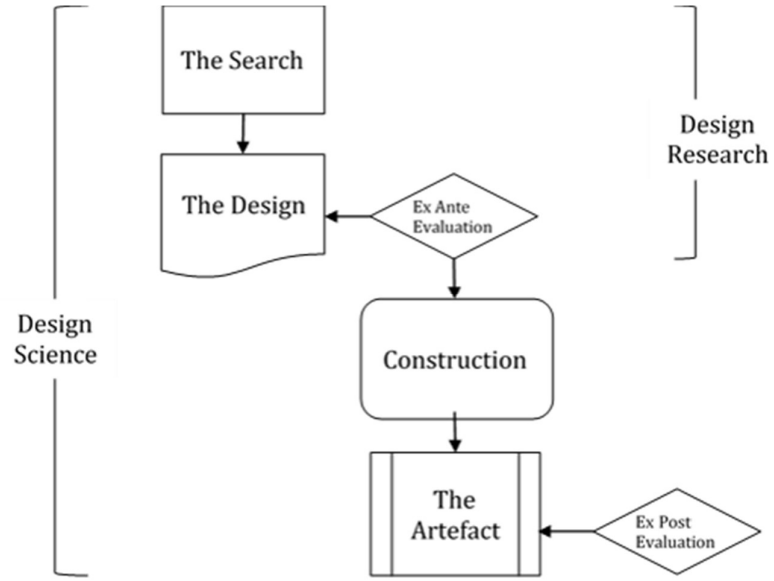


Figure 2-4: Ex ante versus ex post in DSR (Pries-heje et al., 2008)

This study adopted multiple post evaluations including a case study and expert evaluations. The case study (presented in Chapter 6) is naturalistic and is evaluated ex post. The expert evaluations (presented in Chapter 7) were based on an artificial scenario and are also evaluated ex post. Figure 2-5 illustrates the selected evaluation techniques.

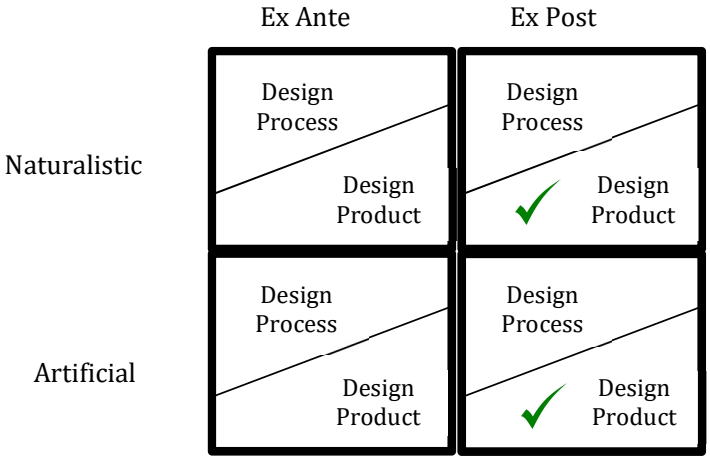


Figure 2-5: Evaluation Techniques

The motivation for the use of case studies and exert evaluations (through illustrative scenarios) as evaluation methods is drawn from Table 2.6 sourced from Hevner et al. (2004).

Table 2.6: Possible Evaluation Methods in Design Science Research (Hevner *et al*., 2004)

Design Evaluation Methods	
Observational	Case Study: Study artefact in depth in business environment
	Field Study: Monitor use of artefact in multiple projects
Analytical	Static Analysis: Examine structure of artefact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artefact into technical IS architecture
	Optimisation: Demonstrate inherent optimal properties of artefact or provide optimality bounds on artefact behaviour
	Dynamic Analysis: Study artefact in use for dynamic qualities (e.g., performance)
Experimental	Controlled Experiment: Study artefact in controlled environment for qualities (e.g., usability)
	Simulation – Execute artefact with artificial data 4.
Testing	Functional (Black Box) Testing: Execute artefact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artefact implementation
Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artefact's utility
	Scenarios: Construct detailed scenarios around the artefact to demonstrate its utility

The design evaluation methods employed in this study falls into the observational and descriptive categories. A case study was conducted to study the artefact in its designated context and this is reported in Chapter 6. Additionally, illustrative scenarios were developed and presented to experts who provided an informed argument regarding the efficacy of the artefact and this is reported in Chapter 7. The following section discusses the evaluation methods employed as part of this study.

2.7.1 Case study

Case studies are a frequently used qualitative research strategy. Bromley (1990, p. 302) describes a case study as a *"systematic inquiry into an event or a set of related events which aims to describe and explain the phenomenon of interest"*. Hartley (2004) further explains how the case study seeks to provide an analysis of the context and processes which shed light on the theoretical issues under study.

In conducting a case study, the specific contextual relevance of the requirements determines whether the researcher will choose a single or multiple case study. Creswell (2014) notes that multiple case studies can be used in instances where generalizable results are sought. Creswell (2014) further notes that the more cases the researcher investigates, the more generalizable the results of the analysis.

When the goal of the research is to produce an output that can be applied to a broad range of the units identified for investigation, multiple case studies are a persuasive route. However, when the study aims to obtain an in-depth perspective, a single case study provides rich data concentrated on the context.

This study adopts a single case study to serve as a demonstration of the application of the framework. As part of the case study, questionnaires were developed and distributed to participants within the targeted context.

2.7.1.1 *Questionnaires*

Saunders et al. (2007) suggest questionnaires as appropriate data collection methods for explanatory and descriptive research. Despite their association with quantitative research,

According to Saunders et al. (2007), questionnaires can either be self-administered or interviewer-administered. Self-administered questionnaires are completed by the respondents in the absence of the researcher, this could either be electronically or

physically completing mailed documents. Interviewer administered questionnaires are recorded by the interviewer based on the responses of the participants.

Chapter 6 section 6.2.1 provides a detailed discussion of the construction and execution of this research instrument.

This study employs qualitative questionnaires as a research instrument. The questionnaires were developed during the time spent at the organisation. Questionnaires were distributed to community healthcare workers with the aim of establishing their day-to-day routine that involves the use of computing devices. Furthermore, the questions seek to gather some insight into the security consciousness of the rural community and the community health workers regarding health related information. The questionnaire used in this study is attached as Appendix 3 and is further discussed in Chapter 6 section 6.2.1.

2.7.1.2 *Sampling – The Organisation and participants*

Ritchie and Lewis (2014) suggest that working through organisations which provide services to or represent particular populations can aid in the generation of a sample frame for populations which cannot be identified easily. This approach was adopted in this study and the participating organisation was selected though the use of convenience sampling and purposive sampling.

Convenience sampling enables the researcher to select the subjects based on accessibility and 'ability' to participate (Ritchie & Lewis, 2014). The organisation had to meet the criteria of being a community based rural healthcare provider and being easily accessible to the researcher.

Purposive sampling enables the researcher to make a sample selection based on a participants' disposition to provide information that is deemed to be relevant to the study (Barbour, 2001), This view is further supported by Elo et al., (2014) who describe purposive sampling as a suitable sampling technique for qualitative studies where the researcher is interested in informants who have the best knowledge concerning the research topic. Additionally, Jansen (2010) suggests that a purposive sample should represent diversity within a target population. In the context of this study, the diversity lies in the varying experience and exposure to the technological tools and operating procedures at the chosen organisation.

The organisation employs community health workers who make extensive use of technology in the delivery of health services and others who do not. Purposive sampling

was used to identify the personnel who would have the relevant exposure to be able to provide meaningful feedback. Twenty-five community health workers were identified as suitable candidates for the study and were subsequently approached with an optional request to participate to which they all accepted without obligation.

2.7.2 Illustrative scenarios

Peffers, Rothenberger, Tuunanen and Vaezi (2012) describe the use of illustrative scenarios for evaluation purposes as the application of an artefact to a synthetic or real-world situation aimed at illustrating suitability or utility of the artefact. This view is supported by Maguire (2001) who describes scenarios as detailed realistic examples of how users may carry out their tasks in a specified context. Peffers et al., (2012) found that illustrative scenarios were the second most used method of evaluation based on their sample of design research outputs. The frequency of use of illustrative scenarios points to the suitability of the method for DSR evaluation. On this basis, illustrative scenarios have been selected as an evaluation method in this study.

The framework developed in this study is contextual and it follows that the resulting output is likely to be specific to that context. The scenarios staged for the purposes of this study are loosely based on a real world scenario with some contextual variables altered in order to avoid inadvertently identifying the organisations involved through potentially recognisable unique characteristics. The evaluation scenario is presented in Chapter 7 and the evaluation tools developed are attached as Appendices V, VI and VII.

2.7.3 Informed argument

To obtain a comprehensive assessment of the research output requires the involvement of domain experts from multiple fields. Each participating expert will be tasked with evaluating the framework though a detailed narrative of its application in the illustrative scenario.

The experts selected for participation consisted of academics with extensive experience in the field of Health Information Systems, ICT for Development, and senior IT employees working with the health information systems of the participating organisation. A detailed discussion on the expert evaluation is presented in Chapter 7.

The scenario has been modified in line with the ethical requirements as discussed in Chapter 1 section 1.9 to ensure that no information that can be used to identify the participating institution or individuals will be published. In an effort to evaluate the

individual process components, a panel of experts was established. The panel consisted of multi-domain experts. The composition of the sample is illustrated in figure 2-6 below.

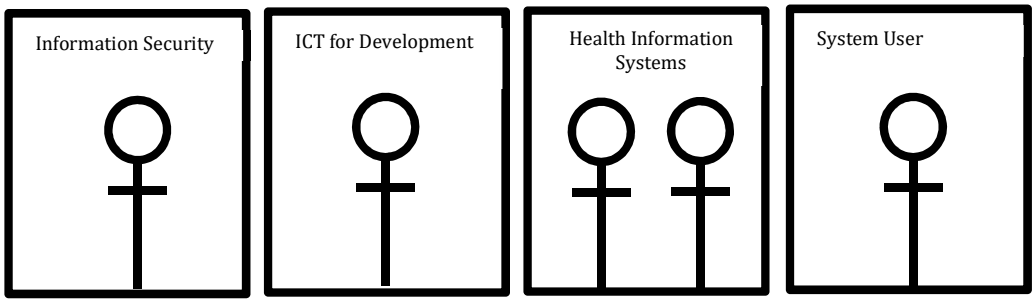


Figure 2-6: Domain Experts

The assembly of multiple domain experts was motivated by the process developed in this study. It was important to ensure that the process was sensible in an information security perspective, an ICT for Development perspective, health information systems and from the perspective of a potential user of the system.

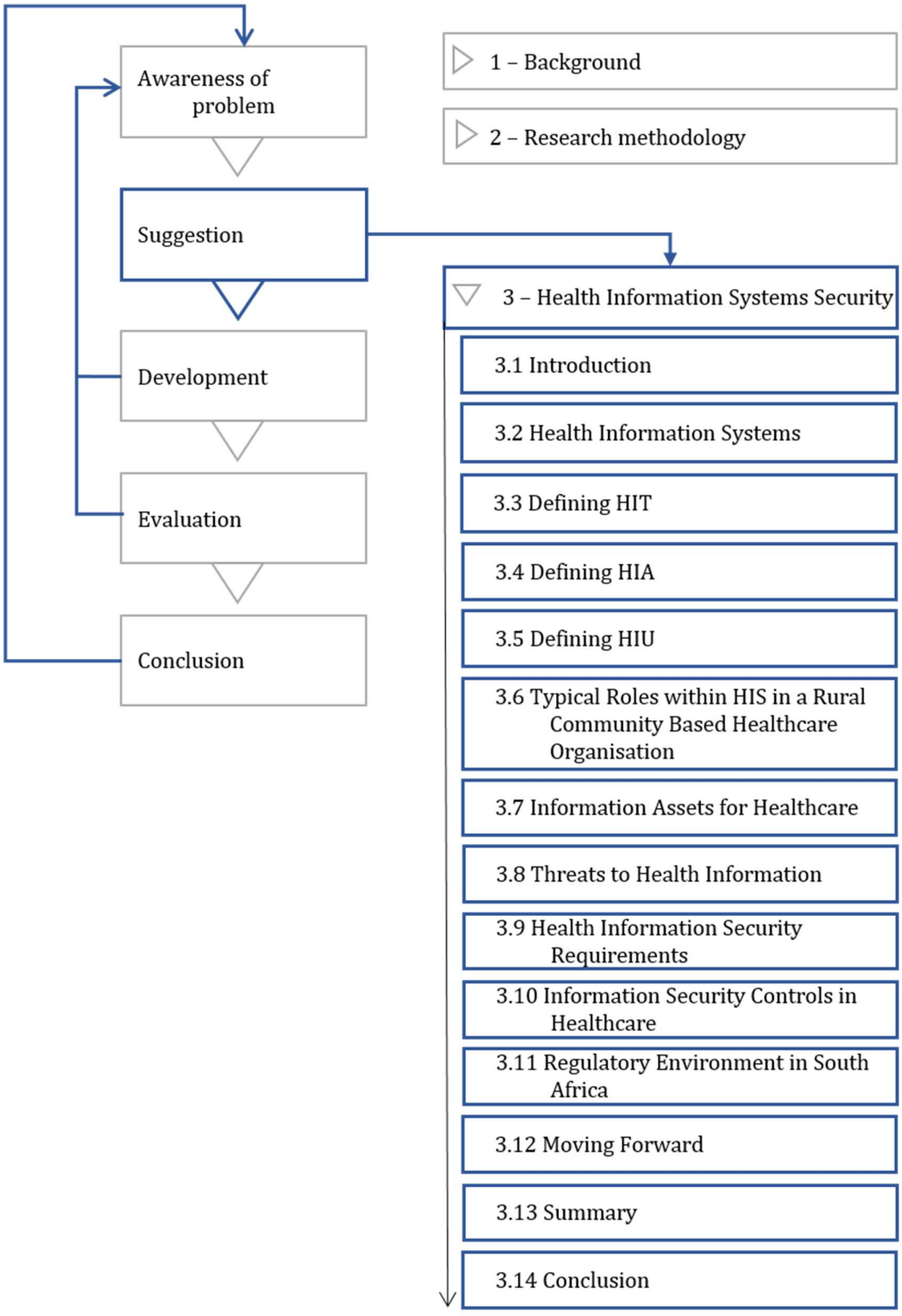
The experts panel was tasked with evaluating the activities that make up the framework, the simulated output of the framework and the framework as a whole. Each expert was invited to participate and was provided with a short description of the framework, the activities, a scenario depicting the application of the activities and the sample output from the process. The participants were then asked to complete a worksheet which evaluated each of these components. The documents are included as Appendices V, VI and VII respectively.

2.8 Conclusion

This chapter outlined the research philosophical alignments, research paradigms subscribed to and the research instruments employed in this study. Design science was selected as the research strategy and the supporting methods for inquiry, analysis and evaluation discussed. Chapter 3 is the first stage in the suggestion phase of the research design. The objective of Chapter 3 is to synthesise the existing literature surrounding health information systems and the security implications.

SUGGESTION

3. HEALTH INFORMATION SYSTEMS SECURITY



3.1 Introduction

This chapter investigates the human, informational and technological aspects involved in facilitating a secure health information system (HIS). Three common HIS components are used to structure the discussion, namely, Health Information Technologies (HIT), Health Information Applications (HIA) and Health Information Users (HIU). A definition of information assets in the healthcare context follow and the chapter continues to discuss the interaction of the aforementioned factors in the delivery of a secure information-rich healthcare service.

3.2 Health Information Systems (HIS)

Information systems generally consist of data, information technology, processes, and users as suggested by Wager, Wickham Lee, and Glaser (2009). In this study, these elements are consolidated into three categories of Health Information Users (users), Health Information Technologies (information technology and processes) and Health Information Applications (data and processes). Health Information Systems branch off information systems and are primarily concerned with enabling data collection, processing, analysis and reporting of health information. Musgrove et al. (2000) describe a health system as consisting of activities whose primary purpose is to promote, restore or maintain health. Borrowing from this description, HIS are responsible for the information that feeds into the health systems. The HIS components of HIT, HIA and HIU are subsequently discussed.

3.3 Defining HIT

Health Information Technologies refer to the devices and computer networks that support the information system rather than the system itself (Fernando & Dawson, 2009). This view is supported by Walker et al. (2005) and Zeng, Reynolds, and Sharp (2009) who describe the purpose of HITs as the use of devices for the management of information to facilitate its timely availability in order to ensure that it is available to the right person where and when required. The deployment of HITs has also been viewed as a means to reduce the costs associated with the delivery of quality care. An emphasis is commonly placed on HIT as not being the end solution but rather a means to an end solution. We can accordingly conclude that HITs are not HISs but crucial components within.

3.4 Defining HIA

Health Information Applications is a broad term that encompasses a wide range of health information tools. Typical applications that fall into this classification include teleradiology, health screening, patient managements systems and other research based health information systems. The growth in adoption of HIAs can in part be attributed to the changing nature of information distribution spurned by the rapid growth of network and internet based services (Tonks & Smith, 1996). In addition to providing access to patient information, HIAs also facilitate access to critical medical information, help management cut costs and enable remote delivery of health services (Raghupathi & Tan, 2002).

HIAs are typically multi-user applications providing interfaces for interaction in different user roles. Traditionally, the focus has been on developing applications for use by medical practitioners and health information was looked from the perspective of the healthcare practitioner (Eysenbach, 2000). Recent advances in information technologies has seen growing expectations for patients to manage their own care through increased access to their health information and increased responsibility for managing the information (Adams, 2010). Health information applications are integral in facilitating access to patient information from the role of the medical practitioner, the patient and any other authorised stakeholders.

HIAs are resident on HITs and consequently, their availability depends on that of the HIT. HIAs provide the interface through which HIU interact with the HIS. Interaction depends on the functional role of the user. Data entry users may be responsible for recording patient information but may not necessarily be granted access to the records once recorded. Other roles such as medical practitioners may be given access to both the recording, and retrieval functions of the health information system.

3.5 Defining HIU

Health information users are the role-players in the health service delivery process. HIUs include everyone involved in the health service delivery process from the health care providers (HCP) side. This includes the management, technical support and CHWs role. HIUs will typically make use of HIAs that are resident on HITs. HIUs (employees) present the largest vulnerability surface area in a health information system (Dhillon, Oliveira, Susarapu, & Caldeira, 2016; Flores & Ekstedt, 2016; Van Niekerk & Von Solms, 2005;

Shropshire, Warkentin, & Sharma, 2015), thus, adequate controls must be put in place to address the challenges at the HIU level.

The roles within the domain of HIU are subsequently discussed.

3.6 Typical roles within HIS in a rural community based healthcare organisation

Health information users typically span across multiple organisational units/departments. Within each of the departments, the users are likely to have different requirements of the information system. Rural community based healthcare organisations typically have shallow organisational hierarchies, consequently, there is a smaller classification of roles. As discussed in section 1.9, four core role-players were identified from the context in which the study was conducted and their specific roles are elaborated as follows:

Organisation Management role:

- **Information custodian** – This is the party responsible for the storage of the data. Additionally, it is the responsibility of this role to ensure that the data is stored, accessed and transacted securely in a manner that does not compromise the confidentiality, integrity and availability of the information.
  The organisation primarily needs access to the data for management and reporting purposes. These users have no direct need to make any changes or alterations to the stored information.

IT / Technical Support role:

- **Information Management** – This party is responsible for the day-to-day administration of the information systems. Their role requires administrative access to the information system enabling them to make changes to the data. This role should be carefully managed and audited to ensure the integrity of confidentiality, integrity and availability of the stored information.

Community Health Worker roles:

- **Information users** – These users primarily add data to the information system and are limited in their ability to recall stored information beyond checking for duplicates and editing biographical details. At this stage, data omission and input errors can affect the integrity of the recorded data. Additionally, malicious users

at this level can deliberately inject false or artificial data in the information system if access is obtained.

Witmer, Seifer, Finocchio, Leslie, & O'Neil, (1995) broadly define community health workers (CHW) as *"community members who work almost exclusively in community settings and who serve as connectors between health care consumers and providers to promote health among groups that have traditionally lacked access to adequate care"*.

These users primarily view the stored data and have no direct need to make any changes or alterations to the stored information. The compromise of this role has few effects on the integrity of the data, however, patient confidentiality can be breached.

Community Member roles:

- **Information providers –** These users do not necessarily have any further interaction with the information beyond providing it. Subjects do however benefit from the services rendered based on the analysis of the information they provide.

3.7 Information assets for healthcare

Information is a critical requirement for the well-being of an organisation. Brotby (2006 p. 12) notes how "*Information and the knowledge based on it have increasingly become recognised as information assets"*. Accordingly, the information resources of an organisation have an attached value. The attached value allows for the information resources to be classified as information assets. Information assets in the healthcare context can be described as information and other resources that support the information systems that enable the operational use of health information. By virtue of being an asset, these resources have value to the health service delivery process and must be adequately maintained and protected in order to sustain the operations of the HIS. Assets can generally be classified as either tangible or intangible. Information is an intangible asset and in the scope of healthcare, will take one of the following forms (Matshidze & Hanmer, 2007):

- **health status information:** morbidity and mortality, births, deaths, injuries and disease burden
- **health related information:** demographic, socioeconomic, residential and other related information

- **health service information:** utilisation of services taking into account the level, rate and intensity, and quality of care
- **health management information:** administrative, financial and other management related information.

Information stored in medical / health records is considered sensitive and the loss or unauthorised access to such information may have severe repercussions on the individuals whose information has been compromised as well as the organisation whom was trusted with the confidentiality of this information. The Ponemon Institute (2016) reported that, nearly 90 percent of healthcare organizations represented in their study had a data breach in the past two years (2014-2016) with nearly half of those having more than five data breaches in the same time period. The most common sources of cyber-attacks were ransomware, malware and denial-of-service attacks while significant emphasis was placed on employee negligence, mobile device insecurity, use of public cloud services and employee owned devices. This once again emphasises the critical role of the user in safeguarding health information. The following section discusses the common threats to health information.

3.8 Threats to health information

The introduction of mobile computing devices in health service delivery has added to the complexity of securing information as data is no longer accessible from a single manageable location but through multiple terminals thereby increasing the vulnerability surface area of the information. It is therefore important to establish a foundation from which advanced security measures and implementations can be built upon.

Healthcare organisations typically handle large amounts of confidential medical and patient data, consequently, they need a secure information asset infrastructure in order to mitigate against the growing threats to confidential information. Failure to adequately protect confidential information may have serious legal ramifications for the HCP. HCPs have put in place measures to protect against the persistent information threats by establishing security programs guided by international standards and best practices. The goal of these programs can be described as follows:

> *The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents and records, from their creation and use to their final archiving or destruction. (Smallwood & Blair, 2012 p.4)*

ISO 17799:2005 defines a threat as *'potential cause of an unwanted incident, which may result in harm to a system or organization'* and a risk is the *'combination of the probability of an event and its consequence'*. Davis, Schiller, and Wheeler (2010, p. 441) add to the description by defining a threat as *"a potential event that, if realized, would cause an undesirable impact".* Advances in communication systems and the ubiquity of connected computing devices has significantly increased the exposure of health information to information threats. The impact of these threats is dependent on the vulnerability of the information assets. Davis et al. (2010 p.441) define vulnerabilities as *"the absence or weakness of cumulative controls protecting a particular asset".* By definition, threats and risks are not the same although they are frequently discussed in the same context.

The health information sector has recently become a focus point for malicious activity. IBM (2016) has found a concerning shift in focus from financial services to healthcare. They report that in 2015, the health industry was only the 6th most targeted industry, this changed dramatically in the space of 1 year and as at 2016, healthcare services were the most targeted industry with over 100 million healthcare records reportedly compromised.

The following section aims to classify the threat categories that may persist in a typical workplace. The discussion leads by discussing environmental threats and man made threats. The discussion expands on the man-made threats by categorising the threats as either internal or externals. A further breakdown of the man-made categories includes hostile structured and unstructured threats and non-hostile structured and unstructured threats. McCumber (2005) illustrates the various threat categories (Figure

3-1) which have been used to structure this discussion. The most commonly prevalent threats to health information are subsequently discussed.

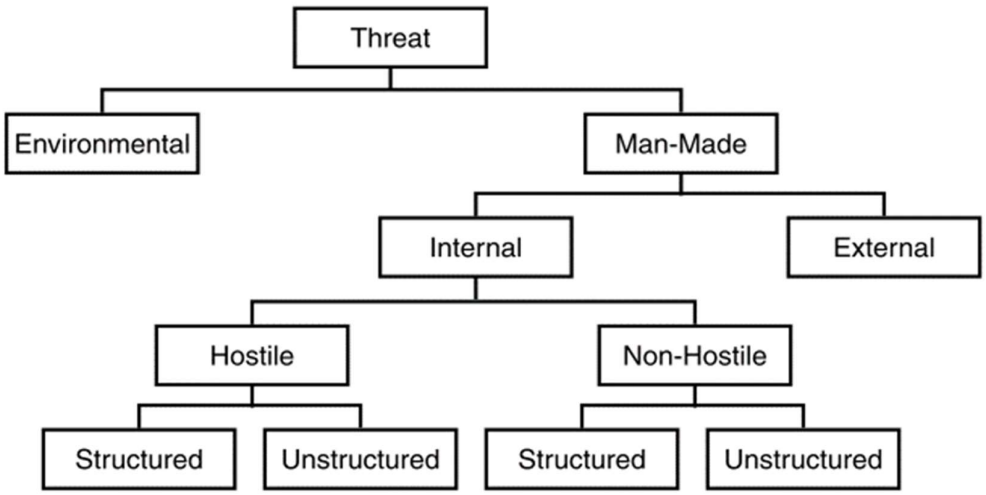


Figure 3-1: Threat categories (McCumber, 2005)

3.8.1 Environmental threats

Environmental threats emanate from the operational environment, thus, the different environments will experience different threats. The underlying understanding of environmental threats is that closely controlled environments are less susceptible to environmental encounters because the organisation can exercise greater control within the environment. Open environments are less manageable and as a result, security considerations tend to be reactive. Most healthcare environments are open as they require interaction with patients. Internal controls (*controls developed for use within the organisation*) are likely to be more effective protection mechanisms as the environment is unpredictable.

3.8.2 (Man-Made) Internal threats

Crossler et al. (2013) classify insider actions that pose threats to organisational information as either intentional (hostile) and unintentional (non-hostile). These are further labelled as deviant behaviour and misbehaviour respectively. Internal threats can be described as those that originate from within an organisation. According to Leach (2003), internal threats are the result of poor user security behaviour. Leach goes on to suggest that internal threats are possibly the largest source of an organisation's security pain. IBM Security (2015) research has shown that in the year 2014, 55% of all attacks

were carried out by either malicious insiders or inadvertent actors. It is therefore imperative that organisations assess the propensity to internal security threats and proactively identify mitigating measures in a timely fashion so as to minimise the adverse effects of a potential internal security incident (Morrow, 2012). Internal threats can manifest in different forms, a view supported by Lee, Lee, and Kim (2016) who identify ignorance, mistakes and deliberate acts by authorised employees as significant determinants for security failures. Some of the more common manifestations are subsequently discussed.

3.8.2.1 *Administration mistakes (non-hostile)*

Thomson, Von Solms and Louw (2006) describe the erroneous actions and behaviour of employees when handling information within an organisational context as one of the biggest threats to information security. This view is supported by Davis et al. (2010) who identify the human factor as being the cause of most security violations.

Administrative mistakes can be classified as misbehaviour as they are not malicious in intent. Typical examples of administration mistakes would be the unintentional disclosure of sensitive information by an employee. This could be the result of misinformation or perhaps in more targeted scenarios, the employee may fall victim to a social engineering attack. An equally significant aspect lies in the infrastructure administration mistakes. These are more technical mistakes that potentially create security holes through which malicious activity may thrive. An example of this would be user accounts that are unnecessarily granted administrative permissions or the user accounts of employees who have since left the organisation remaining active.

3.8.2.2 *Careless insider behavioral internal breaches (non-hostile)*

Security carelessness is described by Chu and Chau (2014) as a common type of information security deviant behaviour and based on Crossler et al. (2013) definition, the intentional nature of carelessness places it firmly in the category of deviant behaviour. Niehaves et al. (2012) note how careless employees do not take responsibility for the security of consumer IT and as consequence, are likely to use it inappropriately. Chu and Chau (2014) further explain that carelessness involves employees omissive activities when using computers or handling information in their day-to-day activities. However, careless insider behaviour is not classified a malicious (Smallwood & Blair, 2012) but rather stemming from lack of awareness and diligence in duty.

3.8.2.3 *Disgruntled employee actions (hostile)*

Moschella, Neal, Opperman, and Taylor (2004) suggest that disgruntled employees pose a greater risk to organisational information than external threats emanating from outside the organisation. This view is supported by Chu and Chau (2014) who suggest that disgruntled employees are more likely to display security deviant behaviour. Disgruntled employees may not be motivated by criminal intentions but may be seeking revenge against an organisation for reasons such as employment termination (Stoneburner, Goguen, & Feringa, 2002), or more ironically, having their personal data accessed as part of deployed organisational security controls (Clarke et al., 2012) amongst others.

Actions taken by disgruntled employees can be classified as security deviant and hostile as the primary intention is to cause harm to the organisation.

3.8.2.4 *Mix of private and corporate database (non-hostile)*

The consumerisation of IT has spurned a previously inexistent phenomenon where organisational data and personal data is co-located. Romer (2014, p.13) subsequently states *"never before has personal data mixed so freely and casually with business information".* A clear delineation between corporate data and private data is important in protecting organisational information. When these two categories of data are mixed, the process of deploying access controls becomes complicated. Mechanisms such a role-based access controls rely on the clear distinction between sensitive and non-sensitive information and binds the different user roles to different classes of information assets. In the healthcare context, storing information such as EHRs with other non-sensitive information like end-user data can significantly compromise the security of the EHR through exposure to internal and /or external malicious user who may exploit the perhaps less-secure non-sensitive information.

3.8.3 (Man-Made) External threats

External threats are typically hostile in nature and driven by criminal intent. Broadhurst (2006) identifies these criminal activities as consisting of interference with lawful use of a computer, dissemination of offensive materials, threatening communications, forgery / counterfeiting, fraud and other activities that involve communication interception, espionage and money laundering. The listed threats primarily entail deliberate attempts from malicious external parties to compromise the information assets of an individual

or organisation. A multitude of external threats exist and this section only discusses a handful of the more common threats.

3.8.3.1 *Cyber-attacks*

Cyber-attacks persist in cyberspace and on internetworked systems (Smallwood & Blair, 2012). The exposure of information in the data collection, processing, analysis and reporting phases may result in unauthorised access to sensitive information. Cyber threats are widespread, increasing in frequency and consequential effect as more organisations leverage the mobility and scalability of cloud based applications and storage (IBM, 2016; Ponemon Institute, 2016). Cyber threats are very unpredictable because of the wide range of possible attacks. These can be as simple as gaining unauthorised access to a weakly secured email account to intercept user authentication tokens and credentials in transit.

Organised cyber-attacks usually involve highly competent user groups who target specific entities with well-structured plans to compromise the information system. Organised criminals are usually driven by the prospect of financial gain and will target anyone from large corporations to individual users. This class of attack is largely opportunistic as it takes advantage of identified loopholes or maliciously source user credentials to execute its attacks.

3.8.3.2 *Corporate espionage*

Corporate espionage attacks are spearheaded by individuals / corporations who may have a desire to either compromise an organisation or obtain sensitive information for personal gain or corporate advantage (SANS Institute, 2007). These types of attacks are more common in highly competitive industries where trade secrets of another entity may be valuable to a competitor. State sponsored attacks are a class of espionage attacks and are driven from political, commercial or military interests of a state.

3.8.3.3 *Social engineering*

Social engineering is described by Flores and Ekstedt (2016) as a behavioural information security threat that relies primarily on the psychological manipulation of people within an organisation. Social engineering is a hostile attack in which an attacker user may masquerade as a legitimate authority or through a series of interactions obtain access to protected or confidential information. Von Solms (2006) notes how the number of social engineering incidents is on the rise and how technical measures alone cannot adequately address this threat. This view is substantiated by Stanton, Stam, Mastrangelo,

and Jolton (2005) who note how behaviour is independent of technical expertise but relies on the intentions of an individual to preserve and protect the organization's IT and resources.

Social engineering relies heavily on a user's lack of awareness of security issues and can be effectively countered by keeping users informed on the nature of a valid request and training them to not give sensitive information whether solicited or unsolicited.

3.9 Health information security requirements

Health information is sensitive and as discussed throughout section 3.8, a multitude of information threats exist. The compromise or misuse of health information can cause financial and reputational harm to information custodian and physical or emotional harm to the patient. It is therefore imperative that a patient's health information is adequately protected and an individual's right to information and privacy are respected. The following discussion briefly describes the information security requirements for healthcare. The discussion leads by identifying requirement that are more specific to the healthcare context before broadening to encompass the generic information security requirements.

3.9.1 Privacy

Privacy refers to the patient's right to information related to a personal medical condition. Additionally, privacy speaks to the patients' rights to decide whether he/she will allow or decline a HCPs ability to either disclose or transmit information to any other party (Appari & Johnson, 2010). The role of privacy as a security requirement is increasingly drawing the attention of regulators as the digital health record grows in adoption and wide scale use. It is therefore imperative that the benefits associated with having digital health records are not eroded by the loss of patient privacy. Healthcare systems must find the delicate balance between provisioning of health services through HITs and respecting the privacy and security needs of the user (Meingast, Roosta, & Sastry, 2006).

3.9.2 Confidentiality

Confidentiality is a means of assurance that information shared is only available to those who have been entrusted with the information. Confidentiality is fundamental

requirement of information systems and as such, any activities concerning sensitive organisational information must be met with controls that secure patient confidentiality.

3.9.3 Integrity

Condition 7 of the POPI Act (The Republic of South Africa, 2013) states that *"A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent*

(a) loss of, damage to or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information. "

Integrity is the requirement that information that is stored or transacted on is not maliciously altered or corrupted in the process. Compromised integrity can have severe repercussions on the patient, for example, critical information such as treatment history and perhaps allergy information are crucial in determining further courses of action. Incorrect information may affect the diagnosis and prescribed course of action which could subsequently affect the patients well-being negatively.

3.9.4 Availability

Availability is concerned with ensuring information services are accessible as and when needed. In the healthcare context, HITs must be able to provide information when it is needed, where it is needed and to whom is authorised to use it. The availability of services is critical in ensuring HCP interventions are carried out timeously. The compromise of availability may have significant effects on a patient's well-being if the practitioner is unable to access critical information that affects a diagnosis of the course of treatment.

3.10 Information security controls in healthcare

A key aspect in information security involves identifying the resources that can be considered information assets and establishing the internal and external value of the assets. Internal value speaks to the value of the resources to the organisation while external value speaks to the perceived value of this information from an external (and possibly malicious) entity to the organisation. This asset value can be used to prioritise

the development of security controls and determine the level of protection that must be provided.

Literature consistently identifies the human (HIU) as the weakest link in an IS chain (Dhillon et al., 2016; Flores & Ekstedt, 2016; Öğütçü, Testik, & Chouseinoglou, 2015; Trinckes, 2012). This 'weakness' can be attributed either to deliberate malicious acts or accidental acts as discussed in section 3.8.1, consequently, there is a growing interest in institutionalising an information security culture in organisations (Dojkovski, Lichtenstein, & Warren, 2007). The human aspects speak to the human interaction with the information system from multiple perspectives. Users have different roles and requirements of the information system, consequently, there is no one size fits all solution for addressing the challenges emanating from this layer.

In addition to the human aspects, the technological resources (HIT) have a role to play in securing health information. As explained in section 3.3, HITs are typically hardware that facilitates the generation, storage and information transactions of an organisation. Security controls at this level include device hardening, physical access controls, dedicated protection devices and controls to abate physical threats such as device loss, theft and damage. Much of hardware security involves ensuring the correct operation of the device and monitoring of component performance and thresholds. Formal controls such as organisational policy can be deployed to govern device handling, transportation, storage and use.

A third level of protection exist at the application level (HIA). Various software controls can be applied to enhance information security and this can be done through mechanisms such as Mobile Device Management systems that manage and if necessary can restrict the operational characteristics of the hardware as a means of disabling inherently insecure features, device recovery tools such as LoJack which can be used to track and recover stolen or missing devices, anti-virus / malware tools that identify security threats and provide mechanisms for prevention and remediation.

Collectively, identifying security threats and prevention mechanisms at these three levels can significantly improve an organisation's information security profile. Two dimensions of security mechanisms as identified by Van Niekerk and Von Solms (2005) are of special interest to this study and are subsequently discussed.

3.10.1 Knowledge mechanisms

Knowledge mechanisms ultimately aim to facilitate information security through cultivating an understanding within each employee of his/her roles and responsibilities and ensuring that he/she is adequately trained to execute their tasks with due diligence (NIST 800-16, 1998, p.3). Knowledge is developed through education and experience, moreover, the sharing of knowledge has been identified as an effective a problem solving tool that can be deployed in a multiuser environment to establish new ideas, or implement policies or procedures (Sohrabi Safa, Von Solms, & Furnell, 2016; Wang & Noe, 2010).

3.10.2 Behavioral mechanisms

Behavioural mechanisms encourage the development of intrinsic controls that leverage off an employees' own belief systems. These mechanisms aim to align the employees' belief systems with the information security compliance requirements of the organisation in an effort to promote an information security conscious organisational culture. Within the dimension of behaviour, Herath and Rao (2009) suggest that security behaviour can be influenced by both intrinsic (motivations that can be considered to emanate from within an individual) and extrinsic factors (motivations that can be considered an outcome of the immediate external environment).

3.11 Regulatory environment in South Africa

The increasing information security incidents in the healthcare environment has necessitated the development of security solutions to protect sensitive patient information. The development of these security mechanisms is guided by existing legislative and regulatory instruments. This section discusses the various regulatory controls and standards that apply to health information in the South African context.

The regulatory environment is very specific on the requirements for entities participating in the respective industries. However, regulatory compliance defines an ideal state that in many instances requires a significant allocation of financial and specifically skilled human resources. Additionally, Van Niekerk and Von Solms (2005) note that it is unreasonable to expect every employee to have full knowledge of the regulatory requirements and /or specifications from standard organisations such ISO (or SANS in South Africa). This poses a particular challenge to rural community based organisations whose staff are typically drawn from low literacy communities.

This section discusses the South African regulations that are applicable to health information and the protection of patient information.

3.11.1 National Health Act (South Africa)

The South African National Health Act was last amended in 2013. The act provides a legal framework that governs the healthcare related activities within South Africa. The act is very broad and for the purposes of this study, the health information related sections of the act is subsequently discussed.

Chapter 6: Operational Management – Health Records Management 62.(1) states that the health establishment must ensure that health records are available when needed to protect users and the health establishment against the risks of delayed, unsafe or inappropriate care (The Republic of South Africa, 2004)

The act prescribes that the health establishment, must:

(a) Implement a record storage and retrieval system;
(b) Appoint a trained and competent member of staff to oversee the information management department;
(c) Train all managers in the use of and interpretation of information for the monitoring, evaluation and planning of services;
(d) Protect the confidentiality and security of health records with appropriate security control measures in the records area in line with the Protection of Personal Information Act, 2013 (Act No. 4 of 2013);
(e) Maintain an archival system for the stipulated duration of time according to the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996; and
(f) Ensure the protection of health records from theft, fire or water damage.

The Act defines clear requirements surrounding the protection of patient information through the implementation of security controls. Moreover, the act stipulates the requirements for health care providers to provide necessary training and skilled personnel for the oversight of information management. These requirements may prove challenging in contexts where the necessary resources to implement the controls are scarce and the skilled personnel are difficult to attract.

3.11.2 Electronic Communication and Transactions Act (2002)

The Electronic Communication and Transactions Act (ECTA) of 2002 was enacted in part, with the objective to prevent abuse of information systems. The act makes provisions for the protection of personal information in Chapter VIII of the act and explicitly states the following mandates:

(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
(8) The data controller must delete or destroy all personal information which has become obsolete.
(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

The mandates of the act essentially emphasise the need for data controllers, in this case, owners of HIS to ensure that information is gathered and /or stored in a secure manner,

for a prescribed period, with the explicit consent of the information owner. The requirements of ECTA are closely related to those of the POPI act of 2013.

3.11.3 Protection of Personal Information (POPI)

The POPI Act was established in 2013 with the aim to *"regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests"* (Parliament of the Republic of South Africa, 2013) . Personal information is information which is about a living identifiable person (a 'data subject') and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature and identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession. The Act additionally defines a classification of special information which encompasses information on (1) Information concerning a child, (2) Religious or philosophical beliefs, (3) Race or ethnic origin, (4) Trade union membership, (5) Political opinions, (6) Health, (7) DNA, (8) Sexual life, (9) Criminal behaviour.

The five specific areas of interest in this study are Information concerning a child, religious or philosophical beliefs, health, sexual life and DNA.

Information concerning a child – Although this information may not be the direct target, it may be inadvertently captured when the patient is a child. It is therefore important that systems are compliant to the requirements of the act when dealing with the day-to-day activities.

Religious or philosophical beliefs – This information may typically be collected as part of the biographical details of an individual. Although this may not have a direct impact on an individual's health outcomes, other issues such as discrimination and persecution may arise as a result of the compromise of this information

Health – Health information may be the primary target of health delivery systems. This information is essential in the facilitation of health services and as such, is a requirement. Measures to ensure the 8 information processing principles are applied when handling this information must be considered from the onset.

DNA – This information may be stored as part of an individual's EHR in situations where laboratory tests are mandated by an individual's condition.

Sexual life – Sexual life information may include number of partners and sexual history. This is typically private information which may be of use for an attending HCP but should be of no concern to anyone other than the owner of the information. Additionally, some health statistics develop their reports based on the number of incidents reported and recorded. This information should however remain confidential.

The POPI act mandates 8 information processing conditions and these are discussed briefly:

Accountability: The responsible party must ensure that the eight information-processing principles are complied with.

Processing Limitation: Processing must be lawful and personal information may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed

Purpose Specification: Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. The responsible party must take steps to ensure that the data subject is aware of the purpose for which his/her personal information is being collected

Further Processing Limitation: This is where personal information is received from a third party and passed on to the responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected

Information Quality: The responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, taking into account the purposes for which it was collected

Openness: Personal information may only be processed by a responsible party that has notified the Information Protection Regulator. Further certain prescribed information must be provided to the data subject by the responsible party including what information is being collected, the name and address of the responsible party, the purpose for which the information is collected and

whether or not the supply of the information by that data subject is voluntary or mandatory

Security Safeguards: The responsible party must secure the integrity of personal information in its possession or under its control by taking prescribed measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information

Data Subject Participation: A data subject has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject and request from a responsible party the record or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information

The Act mandates that personal information processed by public and private bodies be protected against compromise and abuse by establishing minimum requirements for the processing of such information. Non-compliance with the Act could expose the Responsible Party to a penalty of a fine of R10 million and / or imprisonment for up to 10 years.

3.11.4 Local mandates

Local mandates exist below the national level. Typically, in the South African context, this would be the provincial to local municipality level. While policies exist at the provincial level, these are typically high level documents that are almost impossible to generalize across a region consisting of urban metropolitan cities and rural communities on the other end. Many factors such as social cultures can significantly affect the value individuals may attach to information that may be perceived to be sensitive. A typical example is where in rural communities, health information is not considered a secret and in many cases sharing is encouraged so as to de-stigmatise certain health conditions and offer community support through outreach programs. This contrasts significantly with urban metropoles where health information is regarded sensitive almost to the point of secrecy. This results from the fear of prejudice from employers, friends and the general community. The disparities at the community local level highlight the need for specific information security instruments that are built from the respective communities up. Presently, municipalities have ICT policies, which to some extent govern the secure use and transmission of information. However, these documents are generalised and in

many cases will have little to no relevance to the communities in which they are meant to serve. Consequently, compliance becomes an unattainable target.

3.12 Moving forward

As HIUs are the ultimate users of an HIS, this research argues that a traditional top-down approach to security control development in which high level documents such as standards, guidelines and best practices provide the blueprint for control development may not be feasible for smaller organisations operating in resource constrained environments. This argument is based on the premise that controls are developed based on generic guidelines that do not take into account the contextual resources, the environment and challenges that have a bearing on the security of health information. Such approaches may be complemented by resource based bottom up approaches that allow the end users of the system to provide input into the development of HIS controls. To support this argument, Burrows (2009) suggests that such instruments are typically highly structured and require significant commitment and investments for successful implementation. This is of little concern to large organisations with a large IT and Technical department, however, for smaller organisations with little to no IT resources, the traditional route of creating controls based on standards and best practices may prove to be beyond their means. The extent to which controls are required and deployed relies on the organisational requirements and their ability to successfully deploy the controls.

3.13 Summary

This chapter addressed two major focus areas of this study. Firstly, the characteristics and components of health information systems were discussed. This was followed by a discussion on information security in the healthcare context. Moreover, the threats and regulatory controls were discussed.

Figure 3-2 summarises the chapter by illustrating how information assets must ingress and egress the health organisations information systems in a secure manner. These assets are accessible form three levels, namely the information users (HIU). Information assets are consumed by HIUs through HIAs resident on HITs. As a result, the requirements for information security (specifically health information security) must be met at all three levels to ensure the privacy, confidentiality, integrity and availability of stored patient information.

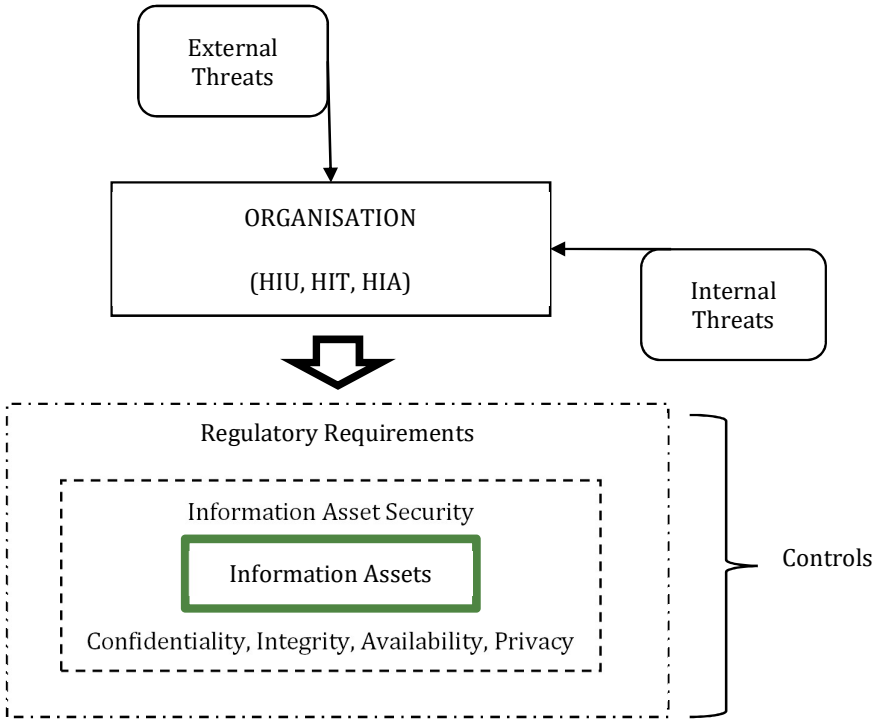
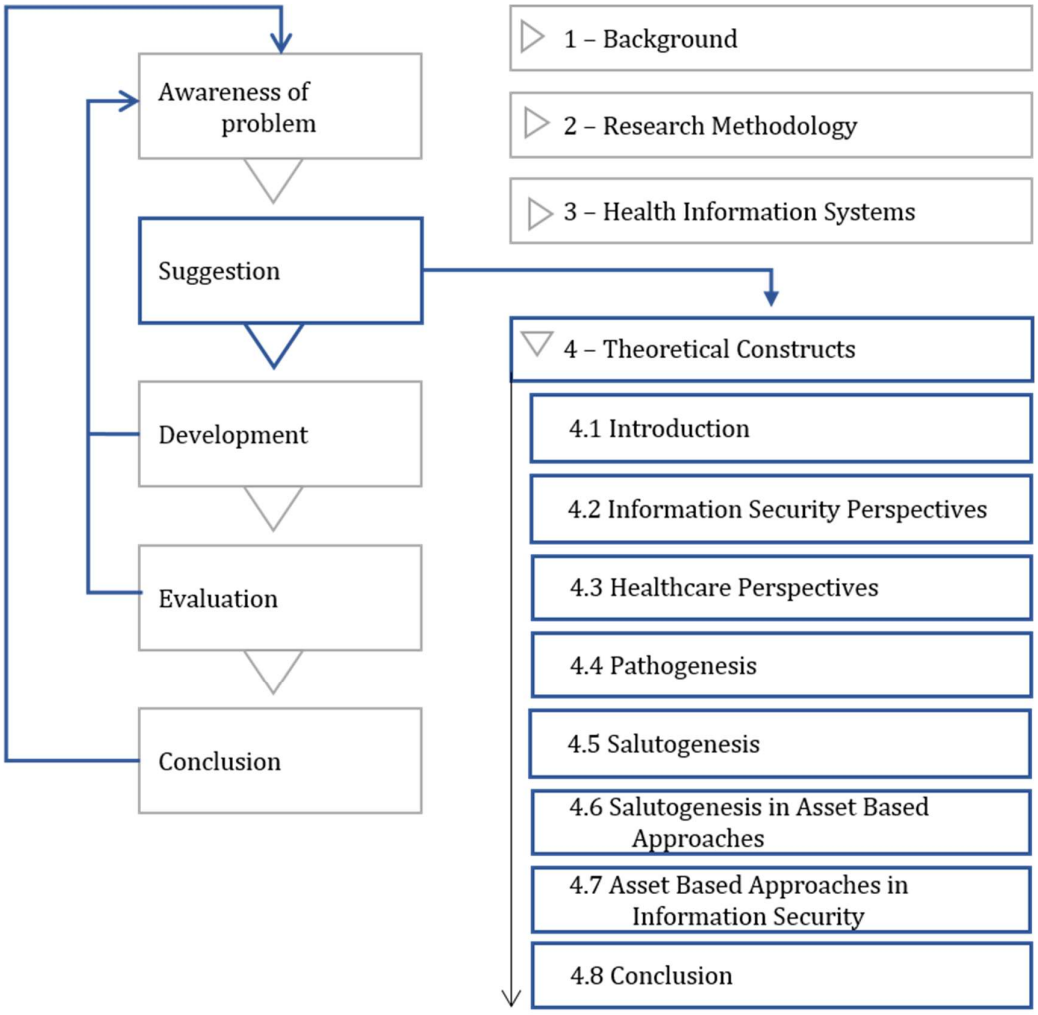


Figure 3-2: Elements of Health Information Systems Security

3.14 Conclusion

The objective of this chapter was to establish the background of HIS in a resource constrained setting. This was followed by an introduction to information security threats and requirements. The chapter examined the various legislative instruments present in the South African context. The chapter concludes by illustrating the interaction the HIT, HIU, and HIA aspect with the threats, security requirements, security controls and information assets. The chapter concluded by discussing the regulatory environment in South Africa. Chapter 4 builds on the outcomes from this chapter by looking at the theoretical constructs that can facilitate the development of an artefact that addresses the security requirements for rural based community healthcare providers. The following chapter builds on the premise discussed in section 3.1.2 and identifies theoretical constructs that can satisfy the requirements for facilitating the secure use, storage and transmission of health information in a resource constrained setting.

4. THEORETICAL CONSTRUCTS



4.1 Introduction

This chapter motivates the selection of the theoretical constructs used in this study. The chapter begins by exploring information security perspectives and motivating a case for the uniqueness of the contextual requirements. Thereafter, related theoretical constructs are identified, their relevance to the IS field discussed and their significance to the study determined. The chapter proceeds to propose a set of contextually relevant theoretical constructs that are carried forward into the framework development. The chapter concludes by motivating the adoption of the two perspectives as building blocks towards the output of this study.

4.2 Information security perspectives

Traditional information technology models adopt a top-down governance approach from which high level documents and controls are developed at the top level of the organisational hierarchy and are filtered down to the rest of the organisation. Brotby (2006) notes how information security must not be regarded as a technical specialty but must be addressed at the highest levels of the organisation. This view is supported in Von Solms and Von Solms (2004) where one of the 10 deadly sins of information security management they identified was not realising that information security governance was a corporate governance responsibility. The authors further add that "*the board of directors as well as top management have a direct corporate governance responsibility towards ensuring that all the information assets of the company are secure and due diligence have been taken to maintain such security"* Von Solms and Von Solms (2004, p. 372).

The need for top-down approaches to Information Security Governance is necessitated by the growing recognition of the critical nature of information to an organisations well-being. The IT Governance Institute, (2003, p. 6) describe enterprise governance as *"a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly"*. Governance occurs at different levels of the organisation following the managerial / team leader delegation hierarchy.

A significant aspect of information security governance is security control development. Figure 4-1 illustrates the governance against the development approaches. The following section discusses information security control development.

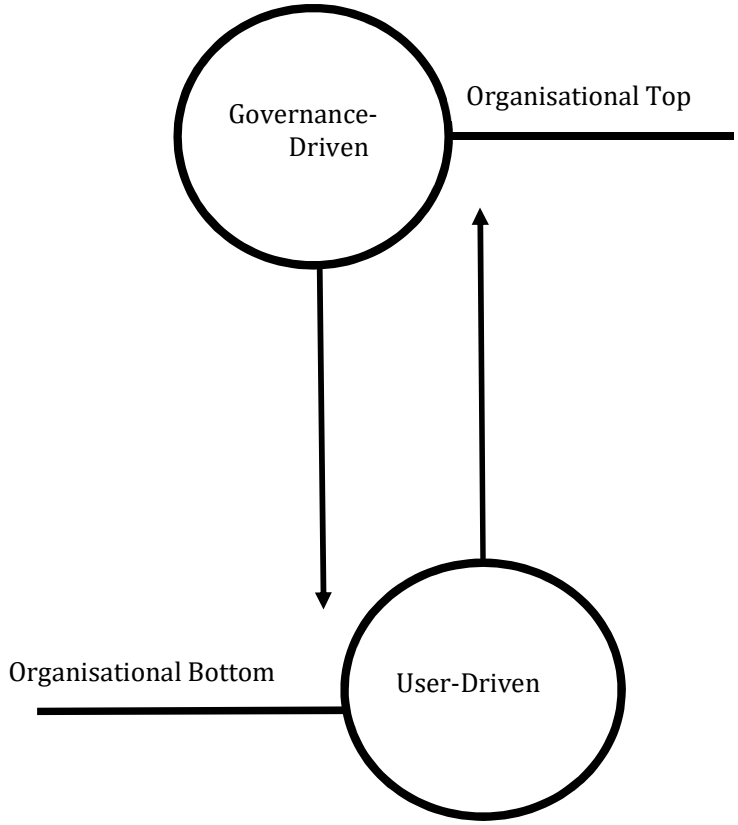


Figure 4-1: Governance vs Development Approaches

Information security control development is a part of any information security program. When dealing with technical controls, Thomson and von Solms (2004) suggest top-down approaches are hindered by their disregard for employees understanding and motivations. While top-down approaches may prove to be effective in medium to large organisations where the organisation has access to significant resources, smaller resource constrained organisations may lack the defined organisational structure to effectively adopt such an approach. This can be attributed to the lack of human, infrastructure and financial resources.

This study makes an argument for the adoption of a bottom-up for security control development. Following the top-down approach for information security control development is resource intensive, resources which are simply not available in the resource constrained context. Adopting this approach would facilitate better

engagement of the intrinsic resources and motivations stemming from the employees and the environment.

The argument emphasises the need to utilise the existing resources that enable information security in conjunction with the need to identify the cause of the challenges. In order to facilitate the development of an artefact meeting this criterion, the salutogenesis and pathogenesis perspectives to healthcare were identified as a suitable theoretical grounding for the development phase of this study. These perspectives are subsequently introduced.

4.3 Healthcare perspectives

Healthcare perspectives describe the different approaches to meeting healthcare objectives. Of particular interest in this study are the health promotion and disease origin perspectives. Traditional approaches to healthcare have adopted a dis-ease origin orientation in which the causes of disease are identified initially before any solutions are sought or developed. The causes of dis-ease are described as 'stressors'.

On the other hand, the health promotion perspectives approach a problem by identifying factors that enable individuals to cope or resist the stress associated with dis-ease (general resistance resources, GRRs) and by doing so, cultivate resistance resources in an effort to overcome dis-ease.

The WHO, (1986) describes health promotion as the process of enabling people to increase control over their health, thereby resulting in improvements to their health.

Lindström and Eriksson, (2006) add the ability to live active and productive lives as an output of health promotion. The two perspectives are illustrated in figure 4-2.

As illustrated in figure 4-2, the traditional disease origin perspectives can be aligned with the pathogenic approaches to healthcare whereas the health promotion perspectives adopt a salutogenic approach to healthcare. The salutogenic and pathogenic perspectives are subsequently introduced and expounded upon.

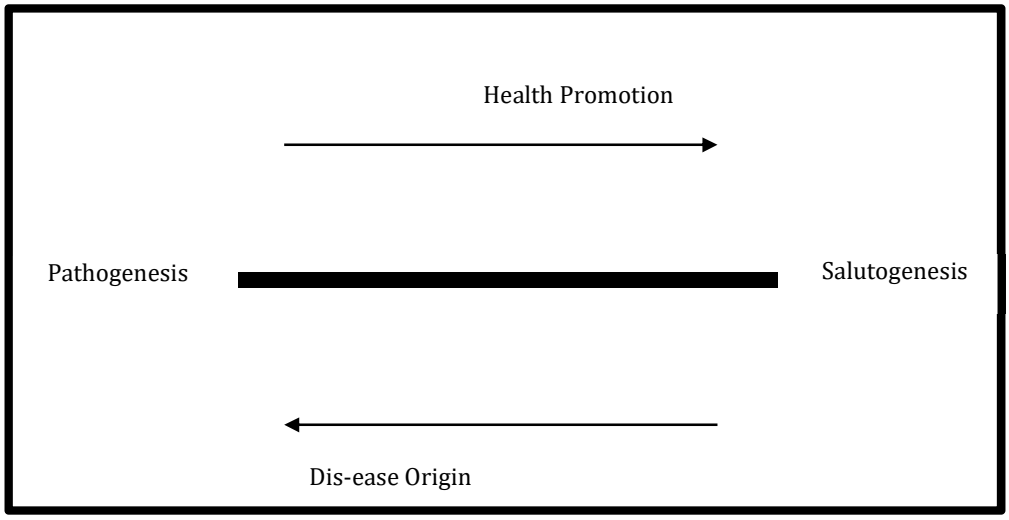


Figure 4-2: Healthcare Perspectives

The salutogenic / pathogenic perspectives on healthcare has traditionally been used in the domain of psychological and mental health. The concept of salutogenesis was derived from the works of Antonovsky (1973) who is generally regarded as the founder of the term. Antonovsky's primary concern was to investigate the origins of health as opposed to the traditional investigations into what causes disease (disease). Salutogenesis can therefore be aligned within the positive domains of health. Promoting positive health outcomes shifts the focus from traditional deficit models that are primarily concerned with identifying intrinsic shortcomings or "the lack of" when exploring a subject matter (Morgan & Ziglio, 2007). Figure 4-3 illustrates the areas of focus within the pathogenic and salutogenic perspectives.

As illustrated in figure 4-3, salutogenic perspectives are concerned with identifying factors that promote wellness, health and ease whereas the pathogenic perspectives are more concerned with factors that cause illness, disease and sickness. The two perspectives are subsequently discussed in greater depth in sections 4.4 and 4.5 respectively.

On the other end of the salutogenesis (health promotion) scale is pathogenesis which is aimed squarely at identifying the cause of dis-ease. Pathogenesis is less concerned with the resources for health and places a greater emphasis on the identification of health risk factors. This perspective relies less on the people's ability to improve their health outcomes and more on the factors affecting the health outcomes.

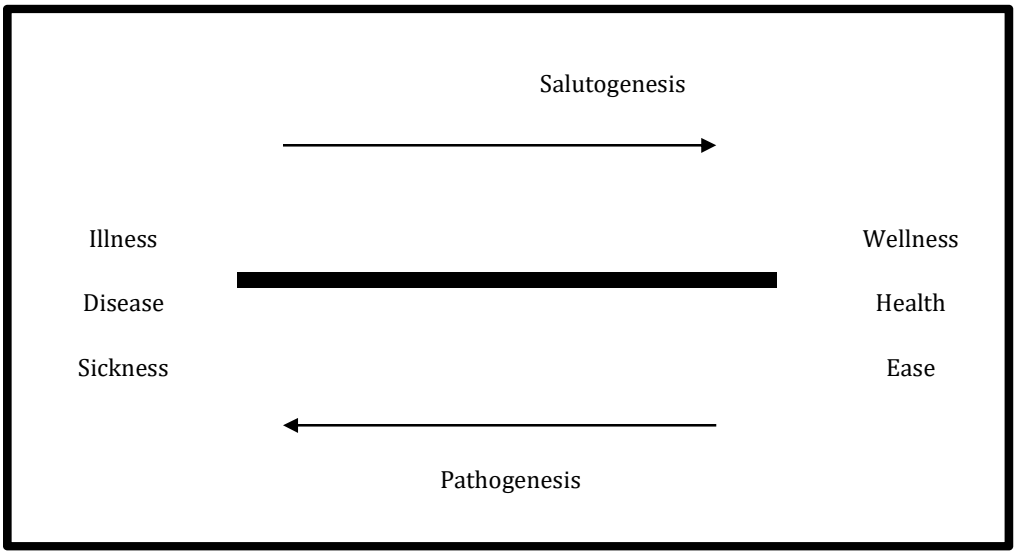


Figure 4-3: Salutogenic vs. Pathogenic Approaches

4.3.1 General Resistance Resources (GRRs)

The General Resistance Resources (GRRs) are the mechanism through which the salutogenic processes operate. Within a salutogenic framework, people reporting greater GRRs will report a greater sense of coherence (SOC) and be more motivated to manage ill health; recognise the challenge(s) underlying illness and believe that resources are available to improve health (Parkin, 2015). Typical examples of GRRs are money, knowledge, experience, self-esteem, healthy behaviour, commitment, social support, cultural capital, intelligence, traditions and view of life. Lindström and Eriksson (2006) stress the importance of people's ability to use the GRRs in order to effectively improve health outcomes. This study argues that the same GRRs can be leverage to improve health information security outcomes without the need for additional investments in infrastructure and resources.

4.3.2 Stressors

Stressors can be described as omnipresent detractors of well-being. The effect of stressors on persons' wellbeing depends significantly on the availability and one's ability to utilise their GRRs (Strümpfer, 1995). Stressors manifest in many different forms but all have the common consequence of creating dis-ease on a person experiencing the stimuli. While primarily investigated from a healthcare perspective, stressors can be a generic reference to any negative stimuli or event that results in a negative outcome for person, group, or entity exposed to the stimuli. Pathogenic perspectives are concerned with identifying the stressors first then subsequently identifying or developing

resources that either prevent or remediate the effects of the stressors. Through experience and the repeated exposure to stressors, individuals, groups or entities increasingly develop a resistance to the stressors by either identifying GRRs or developing coping mechanisms that make the stressors tolerable.

4.4 Pathogenesis

The pathogenesis approach is essentially the antithesis to salutogenesis and as established in section 4.3 is concerned with the origin of dis-ease. That being said, more often than not, both perspectives are used collaboratively to achieve different but essential outcomes. When adopting an salutogenic approach, the origins of the stressors cannot be ignored completely. Pathogenesis has generally been the traditional method of examining health related events particularly microbiology and other medical related fields. The premise of pathogenesis is that a solution to dis-ease can only be discovered after determining what caused the dis-ease. On the other hand, salutogenesis asks "how is it that some people cope and even thrive in an environment with stressors that others succumb to", in other words, what is enabling health in such an environment as opposed to what is causing disease. This study primarily adopts a salutogenic view in the development phase of this study. Salutogenesis is discussed in greater detail in the following section.

4.5 Salutogenesis

Billings and Hashem (2009, p 4) describe the salutogenic approach as one that *"provides a particular perspective to the way health is viewed, which is centred on the discovery and use of personal resources, either inside a person or in the environment, that maintain a healthy status"*. Adopting a salutogenic approach to healthcare emphasises the use of GRRs in coping with stressors that may be caused by or be the cause of ill health. This view is supported by Lindström and Eriksson (2009, p. 19) who define salutogenesis as *"the process of enabling individuals, groups, organizations and societies to emphasize on abilities, resources, capacities, competences, strengths and forces in order to create a sense of coherence and thus perceive life as comprehensible, manageable and meaningful".*

Salutogenesis arose from the need for alternative techniques of evaluating health (Harrop, Addis, Elliott, & Williams, 2006) and as already established is often applied as

an alternative or parallel perspective to the traditional methods of pathogenesis. Lindström and Eriksson, (2006) describe the salutogenic perspective as consisting of three aspects, where:

1. A specific focus is placed on problem solving/finding solutions to health related issues
2. Relevant General Resistance Resources (GRRs) that help people to move in the direction of positive health are identified and …
3. A global and pervasive sense is identified in individuals, groups, populations or systems that serves as the overall facilitator for the Sense of Coherence.

This study investigates four of the constructs identified by Strumpfer (1990) as a collection of independent but relevant constructs. The constructs subsequently discussed are the sense of coherence Antonovsky (1973) , the locus of control (Rotter, 1989), learned resourcefulness and self-efficacy (Bandura, 1989).

4.5.1 Sense of Coherence (SOC)

Strümpfer, (1995) describes the SOC as primarily dispositional as opposed to being reactive/responsive to a given situation. This description is supported by Lindström and Eriksson, (2006) whose description highlights ones' capability to perceive and manage any situation independent of whatever is happening in life.

The SOC uses perception, memory and information processing to appraise the situation (Horn, 2014). This appraisal becomes habitual, leading to the development of sense of coherence through the repeated exposure to situations and sense making (Strumpfer, 1990). Antonovsky defines the sense of coherence as the "*a global orientation that expresses the extent to which one has a pervasive, enduring though dynamic feeling of confidence that the stimuli deriving from one's internal and external environments in the course of living are structured, predictable, and explicable; the resources are available to one to meet the demands posed by the stimuli; and these demands are challenges, worthy of investment and engagement."* (Antonovsky, 1987)

The SOC is described as consisting of three core personality characteristics, namely (1) comprehensibility (making sense of the stimuli in the environment), (2) manageability (coping with the stimuli in view of the available resources) and (3) meaningfulness (an

emotional identification with events in the environment)(Cilliers & Kossuth, 2002; Eriksson & Lindström, 2008; Silarova et al., 2012).

4.5.1.1 *Comprehensibility*

- Comprehensibility refers to the extent to which a person perceives what is happening around them whether internally or externally and making sense of these events.

4.5.1.2 *Manageability*

- Manageability refers to a person's perception that they have adequate resources at their disposal to respond to the health incidents occurring within and around them.

4.5.1.3 *Meaningfulness*

- Meaningfulness refers to a person's motivation to invest, commit and engage the health incidents based on their emotional value of life. Individuals scoring highly in this aspect may tend to view incidents as challenges rather than burdens.

4.5.2 Locus of control

The locus of control speaks to the "dynamic feeling of confidence" that the stimuli can be addressed accordingly. The concept is attributed to Rotter (1966) and is described as the extent to which an individual feels he/she has control over a given situation (Cilliers & Kossuth, 2002). The locus of control can be described as either internal or external where the external individual sees no relation between their behaviour and events and therefore attributes the cause of events to the environment. The internal individual sees the relationship between their behaviour and events and thus feels empowered to alter the outcome through his/her behaviour (Cilliers & Kossuth, 2002).

4.5.3 Self-Efficacy

The self-efficacy is attributed to Bandura (1989) who describes self-efficacy as an individual's belief in his / her capabilities to exercise control over events that affect one's life and to mobilise GRRs and courses of action needed in a given situation. In the workplace, self-efficacy speaks to an individual's confidence in their ability to address a challenge by mobilising intrinsic resources. Self-efficacy can be stimulated in responsive,

encouraging and rewarding environments that value aspirations, engagement and accomplishments (Baloyi, 2006).

4.5.4 Learned resourcefulness

Baloyi (2006) describes learned resourcefulness as a set of complex behaviours that interacts with the physical and social environment. Learned resourcefulness additionally facilitates learning which progressively builds on an individual's self-efficacy. The construct is attributed to the works of Rosenbaum (1989) who describes it as a behavioural traits necessary for redressive self-regulation / control and reformative self-regulation / control.

Rosenbaum (1989) identifies three phases in the process of self-regulation and these are described by Strumpfer (1990) as the following:

(a) Representation – the period during which the individual experiences, without any conscious effort, a cognitive and/or emotional reaction to changes within him-/herself or the environment;
(b) Evaluation of the changes – initially viewed as either desirable or threatening, then, if threat is appraised, evaluation whether anything can be done about it;
(c) Action – the actions taken to minimize negative effects of the internal or external changes (coping).

While salutogenesis has primarily been applied in health related studies with a focus on overcoming dis-ease, this study aims to abstract the core constructs that define salutogenesis and employ them in an IS oriented healthcare context.

The use of salutogenic constructs to understanding an individual's intrinsic /extrinsic motivations and how the social and environmental aspects affect their behaviour is valuable in identifying processes that cultivate positivity and enhance an individual's ability to resist challenges and cope with and learn from experiences.

The following section details how the salutogenic approach has been adopted for use in the IS context.

4.6 Salutogenesis in asset based approaches

Salutogenic approaches are analogous to asset based approaches. The Glasgow Center for Population Health (2011) list the following characteristics of asset based approaches:

(a) They make visible and value the skills, knowledge, connections and potential in a community
(b) They emphasise the need to redress the balance between meeting needs and nurturing strengths
(c) They are not replacements for attempts to address the structural causes of health inequalities.

The goal of adopting asset based approaches is to identify and utilise existing resources (resources which can be considered analogous to GRRs) that meet the prevailing challenges (coping with stressors). Figure 4-4 illustrates the relationship between salutogenesis and asset based approaches.

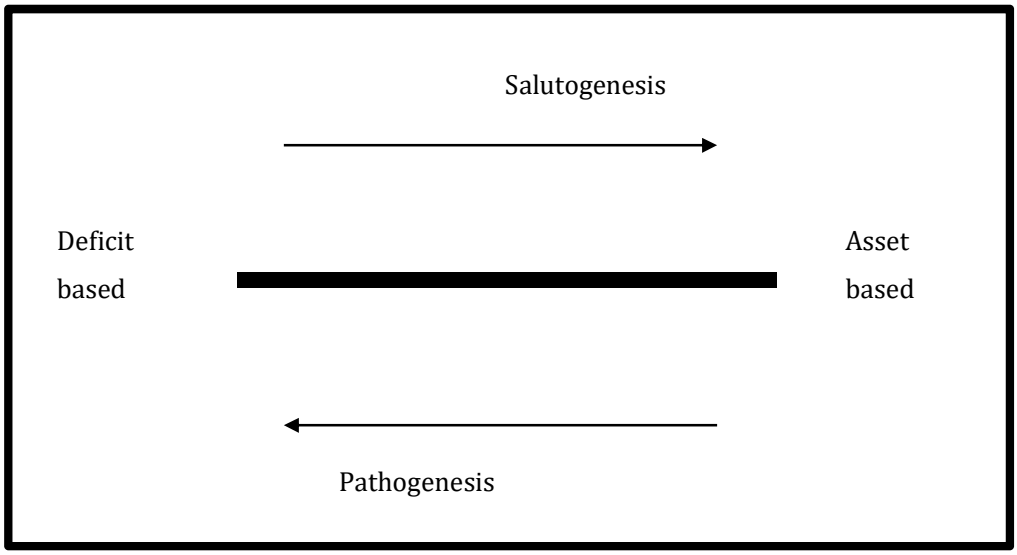


Figure 4-4: Salutogenesis in Asset Based Approaches

On the other end of the scale are deficit based approaches which are analogous to pathogenesis. These are described by Foot and Hopkins (2010, p. 7) as focusing on the *"problems, needs and deficiencies in a community such as deprivation, illness and health-damaging behaviours. It designs services to fill the gaps and fix the problems. As a result, a community can feel disempowered and dependent; people can become passive recipients of services rather than active agents in their own and their families' lives."*

While assets based approaches emphasise the engagement of individual and community resources to solve challenges, deficit based approaches are prescriptive, consequently, as discussed in section 4.6.3, discourages the nurturing of self-efficacy which represents

and individual / community's confidence in addressing a given challenge with the resources available.

Section 3.7 discussed the information assets for healthcare and these are describes as resources or factors that enhance an individual's / community's ability to maintain and sustain health and wellbeing (A. Morgan & Ziglio, 2007). All too often, health measurement instruments focus on measuring ill-health as opposed to adopting a more holistic view on health (Bringsén, Andersson, & Ejlertsson, 2009). Salutogenesis within the context of asset based approaches brings to focus the factors or traits, be it individual, group, or community based that contribute positively to the health outcomes of a community. These traits include a sense of coherence, locus of control, self-efficacy and learned resourcefulness as discussed in section 4.5.

The reality is that the asset and deficit based approaches are simultaneous, co-dependent processes that interact and complement each other to achieve a common goal of improving health outcomes (Foot, 2012). The Glasgow Center for Population Health (2011) suggest that asset based approaches add value to deficit based approached by:

(a) Identifying the range of protective and health promoting factors that act to support health and wellbeing
(b) Promoting the population as a co-producer of health rather than simply a consumer of health care services
(c) Strengthening the capacity of individuals and communities to realise their potential for contributing to health development
(d) Contributing to more equitable and sustainable social and economic development

From a rural health standpoint where fiscal and professional resources are scarce, asset based approaches present opportunities for individuals and communities to redress the challenges independently by identifying and utilising intrinsic and extrinsic resources that are available.

Figure 4-5 presents the asset model as proposed by Morgan and Ziglio (2007). The asset model aims to redress the balance between evidence derived from the identification of problems to one which accentuates positive capability to jointly identify problems and activate solutions, which promotes the self-esteem of individuals and communities leading to less dependency on professional services.

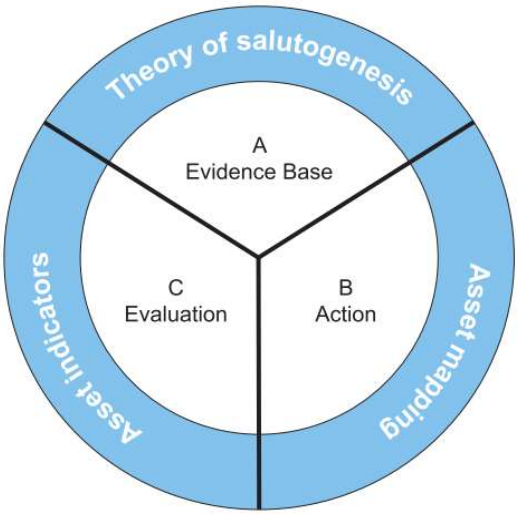


Figure 4-5: Asset Model (A. Morgan & Ziglio, 2007)

The Asset Model presented in figure 4-5, consists of three activities, these are briefly expounded on:

(a) Theory of salutogenesis – the approach adopted to tackle healthcare challenges. The activity involves the identification of health promoting factor (assets / GRRs) and the implications for action.
(b) Asset mapping – The act of initiating a process that fully mobilizes communities to use their assets around a vision and a plan to solve their own problems.
(c) Asset indicators - A shift in focus on the evaluation criteria focusing more on indicators that contribute to improved individual and community health outcomes.

Drawing from the model, bottom up approaches that incorporate the existing assets in addressing the deficit based approach derived challenges may result in more robust, self-propelling healthcare systems. Community involvement in the process imbues a sense of ownership and cultivates self-efficacy. Consequently, adopting the asset based perspectives results in a lesser dependency on external entities, a characteristic particularly important in resource constrained settings. The following section aims to abstract the core constructs of salutogenesis, pathogenesis, asset based perspectives and deficit based perspectives into an information systems context.

4.7 Asset based approaches in information security

The preceding discussions established deficit based and asset based approaches with applications predominantly in the health sciences. This section motivates the relevance of the theoretical constructs in an Information Systems domain. The section aims to identify how the theoretical constructs identified in this study may be adapted into an information security application with real-world applicability in resource constrained settings.

The two approaches, while coming from different perspectives, aim to achieve the same goal of improving the overall health outcomes. The purpose of the preceding sections was to motivate for salutogenic thinking when dealing with problems that involve individuals and communities. As established previously, the human element is the weakest link in information security and because a security system is as only as strong as its weakest link, technological defences are essentially rendered useless without the compliance of the people (Abawajy, 2014; Öğütçü et al., 2015). It can thus be inferred that finding solutions that address the human element of information security will result in a noticeable improvement in the security of an organisation's information assets and enable technological tools to function more effectively.

Sections 3.10.1 and 3.10.2 discussed knowledge and behavioural mechanisms as two significant dimensions in information security. Table 4-1 categorises the salutogenesis constructs discussed in section 4.5 according to the two dimensions.

Table 4-1: Knowledge and Behavioural Dimensions

Knowledge Mechanisms	**Behavioural Mechanisms**
Learned resourcefulness	Sense of coherence
Locus of control	Self-efficacy

Knowledge mechanisms establish an individual / community's fundamental understanding of what is expected, what is possible and what must be done (awareness). Behavioural mechanisms are influenced by the knowledge mechanisms and through experience and exposure.

Traditional information security controls are mostly hardware or software based technological tools that require significant investment in infrastructure and skilled

human resources for successful deployment. Equipment such as firewalls and unified threat management systems are not only expensive, but require highly skilled professional to operate them. The objective of deploying technological tools is to provide solutions to identified problems and /or fill gaps, an approach which is in line with deficit based approaches.

While technological tools and controls are generally tried and tested, the resource intensiveness does not bode well for resource constrained settings. As established in Chapter 1, rural healthcare settings are typically resource constrained and yet are plagued by many of the same health information security challenges found in the urbanised environments. Typical resource constraints include finance, skilled labour, electricity supply, road and transportation networks.

It was established in section 4.2 that information security is directed by corporate governance. At this level, the organisational policy is developed and contains within it, sub-policies that govern specific areas within the organisation's information systems. Table 4-2 presents some of the asset based and deficit based controls typically found within an organisation.

Table 4-2: Asset vs Deficit Based Controls

Deficit Based Controls	**Asset Based Controls**
Physical security	Knowledge mechanisms
Hardware	Behavioral Mechanisms
Software	

Asset based controls can be identified, not to replace deficit based controls, but rather complement these controls by utilising behavioural and knowledge resources to address some health information security concerns. Safa et al. (2015) suggest that users and their perceptions are the centre of the security concept. Figure 4.6 illustrates the central role of the user based on the user roles identified in Chapter 3 section 3.6.

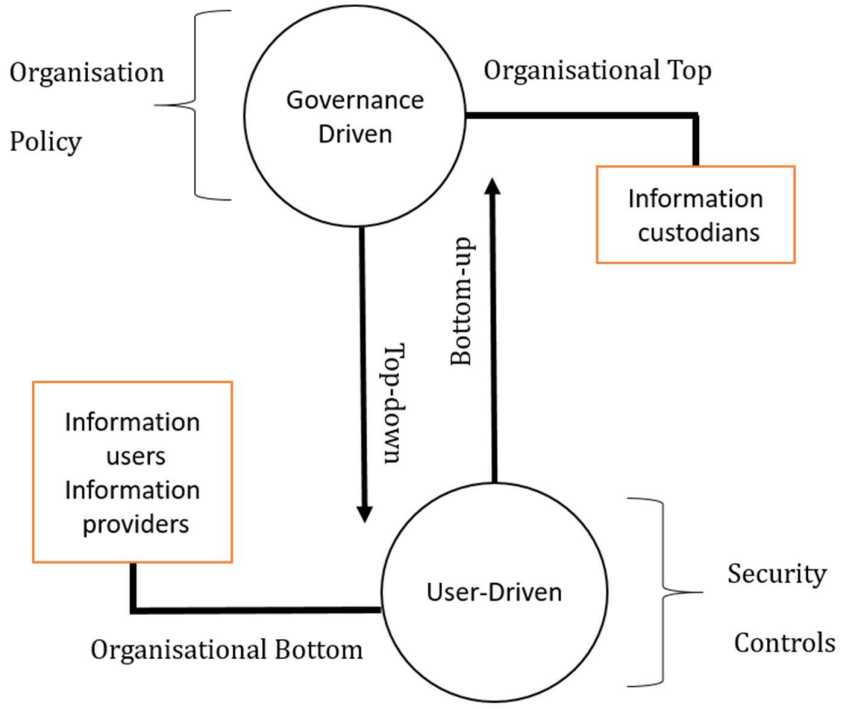


Figure 4-6: Users in Asset Based Approaches to Information Security

Figure 4-6 illustrates the top-down orientation of governance and the responsibilities of corporate governance as the organisation's information custodians. In an asset based approach to information security, the security control development will follow a bottom up approach where the information users (employees within the organisation) and information providers (patients and community members) must provide input into the control development activities in order to successfully identify the intrinsic and extrinsic resources within and outside of the organisation. Adopting an asset based approach to the development activities provides a mechanism through which the contextual differences in each setting can influence the type of controls that are deemed necessary and deployed as opposed to exclusively subscribing to generic instruments (such as standards) that guide the deployment of security controls.

The following section proposes a process flow that allows for the salutogenic and pathogenic dimensions to interplay in the identification of resources and stressors as a means of developing information security controls.

4.7.1 Conceptual Constructs

The salutogenic questions of "what is enabling health" allows for the identification and utilisation of GRRs to improve an individual, group or entities health outcomes.

Limited resource capacity of the rural healthcare environment entails the development of resource-friendly solutions. Figure 4-7 depicts the proposed conceptual constructs carried forward to the development of the framework.

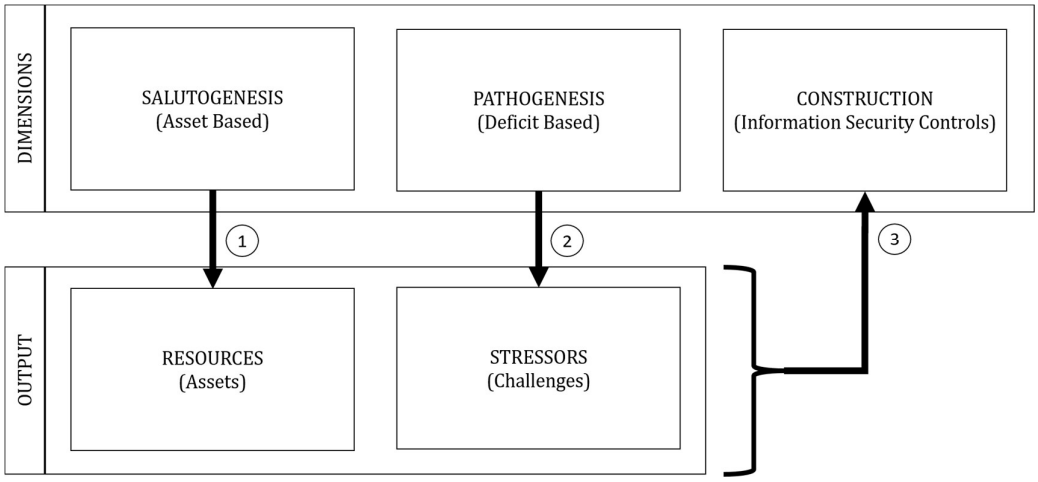


Figure 4-7: Conceptual Constructs

Dimensions – represent the viewpoints from which the problem is approached.

Output – represent the outcomes of the activities conducted in each dimension.

Dimension 1: Identify resources that enable health information security from the HIS elements.

Dimension 2: Identify stressors that pose challenges to information security from the HIS elements.

Dimension 3: Identify the stressors addressable from the identified resources. Non-addressable stressors may require external interventions.

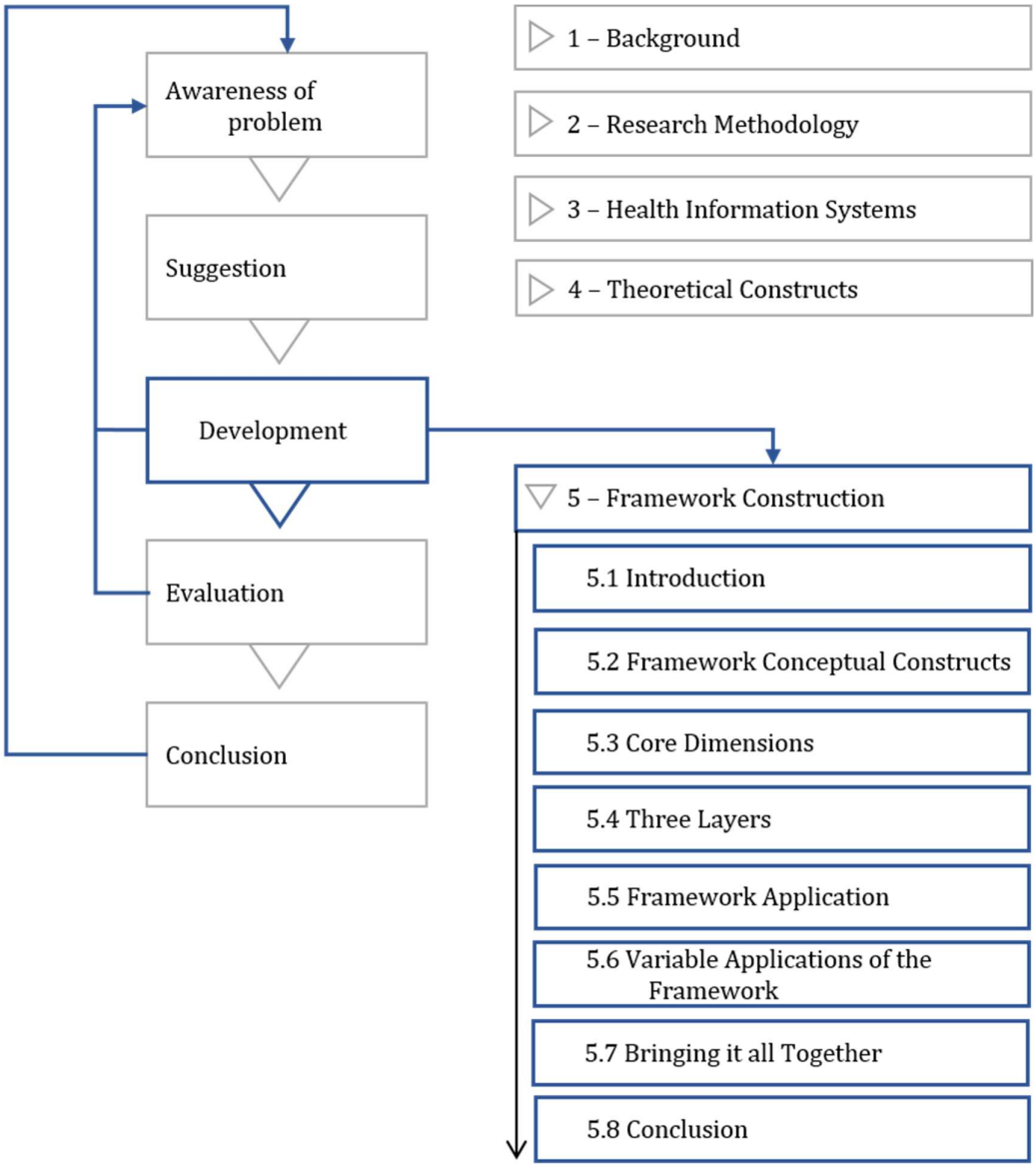
The resulting output from the 3 dimensions encourages the development of health information security controls from a resource-first perspective aimed at the contextual HIS elements identified.

4.8 Conclusion

The aim of this chapter was to identify and describe the various constructs that will be taken forward into the development phase of this study. More specifically, the constructs include the salutogenic resources and pathogenic stressors. The chapter led by discussing information security perspectives. This was followed by the identification of salutogenesis as the theoretical perspective in which an emphasis is placed in identifying resources that promote health as opposed to those that identify causes of ill health. This perspective is supported by the analytical lens in which the assets model is applied as a mechanism to identify GRRs and provide a meaningful interpretation of their role in promoting health. Finally, the IS applicability was examined, and a suggestion for the traversal of the three dimensions through the development process was put forward. The following chapter details the development of the framework that leverages the abovementioned components in creating a context aware framework that can be applied in resource constrained settings

DEVELOPMENT

5. Framework Construction



5.1 Introduction

Chapter 4 discussed the theoretical constructs that were adopted for the purposes of developing the framework. The chapter concluded by presenting a suggestion towards the structure and initial components of the framework.

This study culminates in the development of an eight step framework that provides a foundation for the development of context aware health information security systems. The following section provides a breakdown of the assembly process starting with two core dimensions identified in the theoretical constructs chapter and the addition of a third construction dimension. Thereafter, the three elements of an HIS identified in Chapter 3 are incorporated. Finally, step-by-step guidelines of the application of the framework are presented.

5.2 Framework conceptual constructs

The conceptual constructs discussed in this section are the constituent parts of the framework. These constructs were derived from the activities in chapter 3 and chapter 4.

In chapter 3, the three elements of an HIS were identified, these are:

- HIU – Health information systems users including management, IT/technical support and the CHWs
- HIT – Technologies supporting the health service delivery including devices and communication networks
- HIA – Applications interfacing the HIUs and the HITs. These include Health monitoring, tracking and reporting applications.

In chapter 4, two dimensions of the framework were identified, these were:

- Salutogenesis – an asset based approach that emphasises the resources that enable information security (security wellness of the information system).
- Pathogenesis – a deficit based approach that emphasises the stressors that work against information security (challenges to the information system's security wellness).
- The third construction dimension was added to represent the development of controls based on the consolidated output from the first two dimensions.

- In Chapter 4, two categories of HIS factors were identified, these were:
    - Resources – Health information assets that facilitate the safeguaring of health information security
    - Stressors – Factors that pose as challenges to the security of health information.

Figure 5-1 illustrates how the constructs were assembled. A detailed discussion on the assembly of the framework using the aforementioned constructs ensues.

5.3 Core dimensions

Three core dimensions are illustrated in figure 5-1, namely, the salutogenic, pathogenic and construction dimensions. The interaction of the three dimensions is further discussed in the following sections.

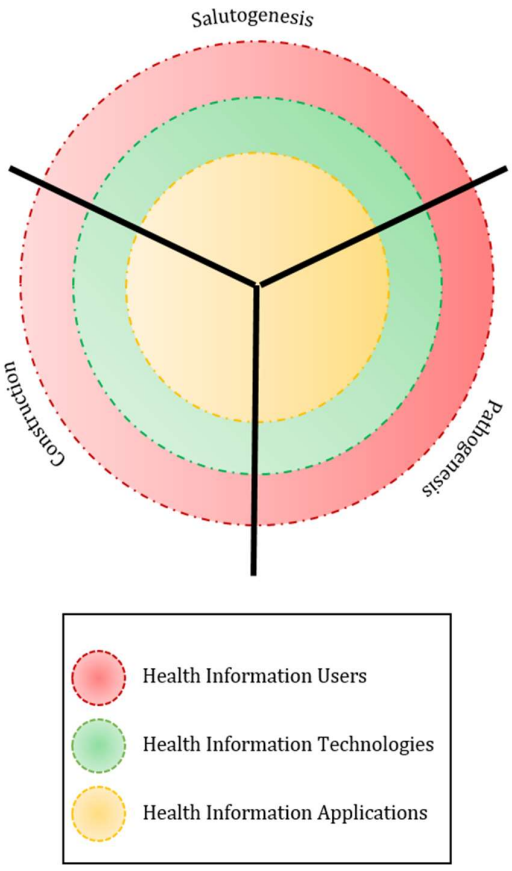


Figure 5-1: Framework Conceptual Constructs

5.3.1 Salutogenesis

The purpose of introducing the salutogenesis dimension is to ensure that any resulting solutions are built with full awareness of the resources available in the environments in which they will be deployed. The salutogenesis dimension is aimed at discovering and documenting resources that can be considered health information security assets. The salutogenesis dimension is followed by the more deficit oriented pathogenesis dimension which is discussed in the following section.

5.3.2 Pathogenesis

The pathogenesis dimension is concerned with the identification of health information security challenges. The pathogenesis dimension follows the traditional pathway for systems development which aims to develop solutions for identified challenges. Following the pathogenesis dimension is the construction as described in the following section.

5.3.3 Construction

In this dimension, controls are crafted by mapping the identified resources to the identified challenges in an effort to address the challenges utilising existing intrinsic and extrinsic resources that are available to the organisation.

5.4 Three layers

The three dimensions discussed in section 5.3 iterate through three layers as represented by the colour coding in Figure 5-1. Each layer represents a control boundary that presents a unique set of resources and challenges requiring a specific set of controls. The layers are listed and subsequently discussed:

- Health Information Users (HIU)
- Health Information Technologies (HIT)
- Health information applications (HIA)

5.4.1 Health information users

This layer represents the human elements in the information security chain. An information system or service system is only as secure as its weakest point, and the human is commonly identified as the weakest link (Morrow, 2012). Working from the bottom-up approach in the typical rural community based healthcare organisation, the users represent the CHWs, the IT/Technical personnel and the organisational management.

Community health workers in the context of this study are involved in the health service delivery and are the primary technology users. As health workers, they are bound by legislative mandates which specify a set of requirements including the requirement that information seen or disclosed by a patient should remain confidential. Consequently, it is the responsibility of the CHWs to ensure their day to day activities are conducted in a security conscious manner and that due diligence has been exercised to ensure the confidentiality, integrity, availability and privacy of patient information.

The IT/ technical personnel are responsible for managing and maintaining the information systems. They provide support to the CHWs in the field and to management for information retrieval and reporting. They too are bound by legislative mandates requiring that their duties are conducted in a security conscious manner. These users typically have extensive access to the information system and thus measures must be put in place to ensure that the users are compliant with the organisations information security requirements.

Organisational management has the responsibility of governing information security, security policies and implementing information security management strategies. Information security management is a critical aspect of the overall security approach as all information security measures and controls must be defined at this level in the form of organisational information security policies.

Figure 5-2 depicts the HIU layer of the framework. The layer consists of the three dimensions with a focus on the contextual human IS aspects of the framework.

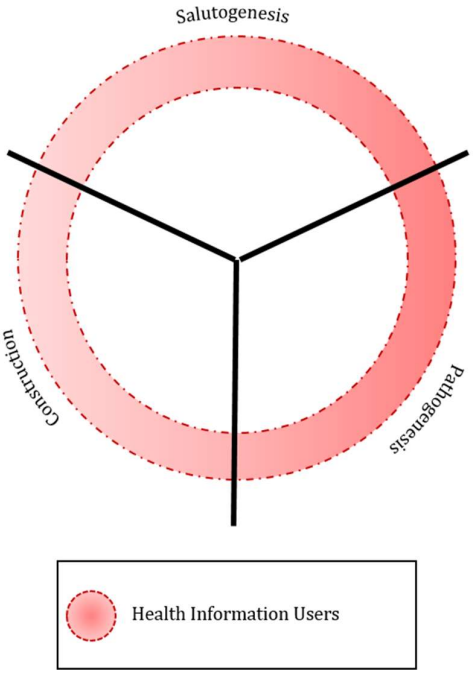


Figure 5-2: Health Information User Layer

5.4.2 Health information technologies

Typically, the infrastructure layer consists of the communications infrastructure and the physical devices. As established in Chapter 3, the infrastructure provides the means through which HIUs deliver services to the patient (CHWs) and the means through which report information is obtained (management). The infrastructure layer is the intermediary layer between the human and application layer, thus, considerations for enabling human and application security must be made at this layer.

Community health workers in the context of this study make use of mobile computing devices and to facilitate the reach into isolated populations, these devices communicate asynchronously with the organisations network. This is primarily due to the lack of telecommunications infrastructure in some areas of the community being served.

Management retrieves statistics and compiles reports based on the information processed. Any loss or compromise of information at this level will directly affect the CHWs ability to perform their duties and management's ability to accurately keep track of key performance indicators. It is therefore imperative that the security resources at this layer are identified and leveraged to overcome some of the security challenges. Figure 5-3 adds the infrastructure layer to the framework.

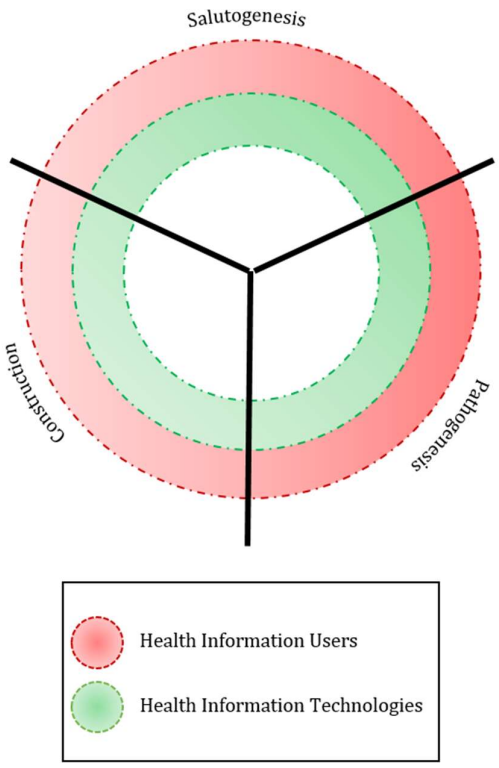


Figure 5-3: Health Information Technologies Layer

5.4.3 Health information applications

The application layer typically consists of database systems and patient management systems. Applications provide the interface through which the HIUs can utilise the infrastructure to deliver health related services. It is imperative that the applications operate in a consistent manner and are adequately secured to protect the information assets. In the context of this study, this layer provides a final organisation-controlled security barrier.

When combined with diligent security controls at the infrastructure and human levels, the resulting solution should prove to improve the overall information security profile of an organisation despite the constraints associated with operating in a rural context. Figure 5-4 adds the application layer to the framework design.

5.5 Framework application

The purpose of this section is to provide guidelines on how the researcher envisions the framework to be applied. The framework consists of eight steps divided between three dimensions (salutogenesis, pathogenesis, construction) that iterate through three layers.

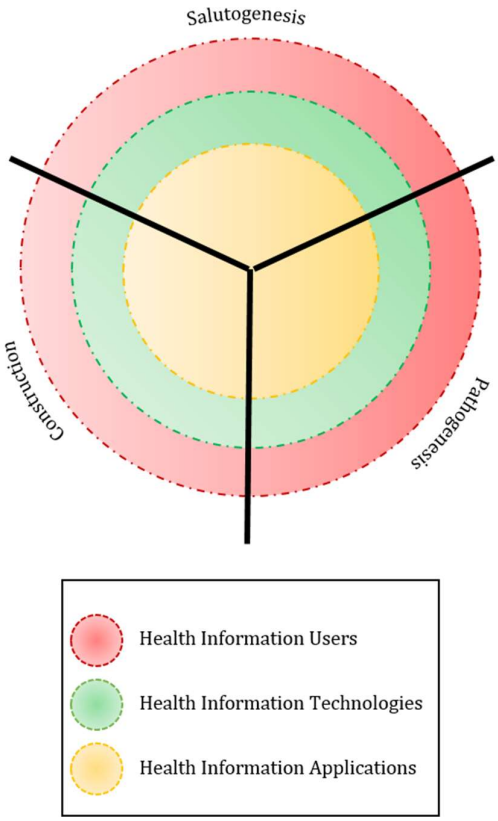


Figure 5-4: Health Information Applications Layer

This section outlines the purpose of each step and provides examples of activities that can be conducted to reach the desired outcome of each step. The complete framework is illustrated in Figure 5-5.

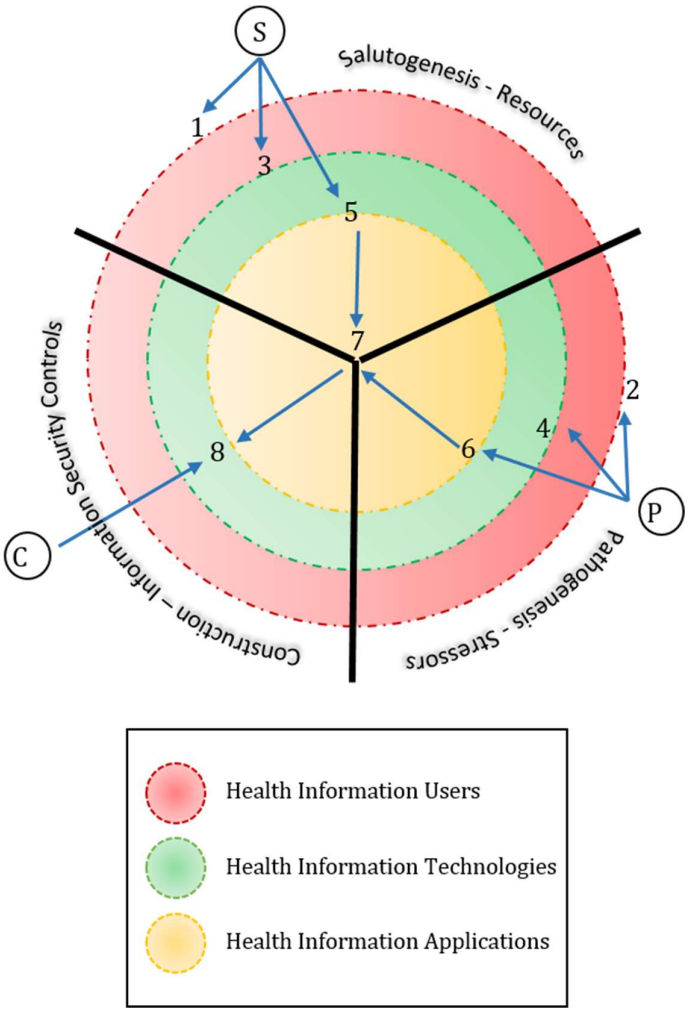


Figure 5-5: Complete Framework

Three layers, HIU (health information users), HIT (health information technologies) and HIA (health information applications) are represented by the red, green and yellow colours respectively. The layers depict three different layers of security identifiable in a rural health context and the individual steps iterate through the layers in an effort to catalogue resources and stressors that have an impact on health information security. The following sections describe the purpose and actions from steps 1 through 8.

5.5.1 STEP 1: Salutogenic [HIU] identify resources

In this first step, health information security resources are identified. Resources at the HIU layer typically consist of intrinsic and extrinsic human factors that promote the secure use, storage and retrieval of health information. This process requires extensive dialog with the organisation management, IT / technical personnel, CHWs and members

of the community (referred to as role-players from henceforth). In addition to identifying the human oriented health information security resources, this step should also explore the workflows and procedures that define the HIUs day-to-day activities. Examples of activities that can be conducted to obtain the required information include the following:

- **Workshops:** Workshops incorporating the various role-players can be setup. The goal must be to create a conducive environment for dialogue. This allows for suggestions and rebuttals internally. This automatically eliminates those variables that may be deemed resources for some role-players but stressors for others.
- **Interviews:** In situations where setting up workshops proves to be challenging, individual or group interviews can be conducted with subsets of the role-players. This activity may be more time consuming and will likely require several iterations to eliminate variables that are not perceived to be resources across the board.
- **Questionnaires:** Questionnaires are an ideal instrument for remote administration. The questions should be open-ended and allow for the participants to add detailed comments in their feedback
- **Observational tag-along:** These can either be scheduled or unannounced. It is important that the observer is familiar with the operations of the organisation and the processes. This would ideally be someone internal to the organisation. The familiarity will allow for accurate interpretation of the observed events.
- **Other inquiry methods:** If the organisation is in a position to obtain the services of experts, methods such as ethnographies and vanguard studies can be adopted. These however may be time consuming and resource intensive.

The activities listed above are mere suggestions. A variety of approaches may be taken to obtain the same information. The underlying constant is that the identified resources must come from the perspective of the role-players and that at least two activities must be conducted in order to corroborate the findings.

The output of this step is a list of intrinsic and extrinsic resources that are accessible to the role-players for the purposes of securing health information. Following the identification of the resources, the next step is to identify prevalent stressors to health information security.

5.5.2 STEP 2: Pathogenic [HIU] identify stressors

This step can be conducted concurrently with STEP 1. The objective is to identify the intrinsic /extrinsic HIU factors that can be considered stressors to health information security within the context. Similarly, this step requires extensive dialogue with the role-players. Examples of activities at this step are similar to those discussed in STEP 1.

The output from this step would be a list of contextual stressors. The overall output from STEPS 1 and 2 is a collection of resources and stressors that prevail at the HIU layer.

5.5.3 STEP 3: Salutogenic [HIT] identify resources

The third step moves onto the HIT layer. The objective of this step is to identify the technology or infrastructure resources that can be considered enablers to promote the secure use, storage and retrieval of health information.

This step involves identifying the infrastructure resources that support the HIS. It requires an intermediate-to-advanced knowledge of the information systems in use and is typically conducted with the inclusion of IT or technical support personnel. However, cognisant of the possible unavailability of such personnel in the rural health context, the device users can provide this information albeit in a limited capacity. Examples of activities at this step are similar to those discussed in STEP 1 and can additionally include upfront activities such as inventory auditing. Ideally, when conducting this step, the participants should include the IT/Technical role-players and organisation management in addition to the CHWs and community members.

5.5.4 STEP 4: Pathogenic [HIT] identify stressors

Following the pattern established in STEP 1 and 2, The pathogenic dimension seeks to identify the stressors. This step can be conducted concurrently with STEP 3 and would employ a similar set of activities. The output from this step would be a list of stressors prevalent at the HIT layer. Examples of activities at this step are similar to those in STEP 1.

Similar to steps 1 and 2, a minimum of two activities must be conducted in order to corroborate the findings from each activity. The overall output from STEP 3 and 4 is a collection of resources and stressors that prevail at the HIT layer.

5.5.5 STEP 5: Salutogenic [HIA] identify resources

This step moves onto the final layer where the application resources that promote the secure use, storage and retrieval of health information are identified. This step requires the input from personnel with an in-depth understanding of the application and other operating system tools that are part and parcel of the service delivery process. The personnel may be part of the HIU, or internal/external developers responsible for the application development. Activities in this step are similar to those in STEP 1. This layer may be the most complex to address because of the vast variety of applications that could be used and the level of expertise required from the participants. In keeping with the objectives of the framework, internal personnel would be in the best position to provide the contextual information required, however, an exception can be made and external application developers may be consulted if deemed necessary and if resources are available.

The output from this step is a list of contextual application resources.

5.5.6 STEP 6: Pathogenic [HIA] identify stressors

Similar to STEP 5, this step requires the input from personnel with an in-depth understanding of the application and other operating system tools that are part and parcel of the service delivery process. The objective is to identify stressors at the HIA layer. In addition to the activities in STEP 5, the parties responsible for implementing the framework may be required to conduct application and operating system tests to identify additional challenges that may prevail. Specialised skill may be required in order to identify some of the more complex resources. Examples of activities at this layer are similar to those in STEP1 and additionally include the following:

- Application testing (black, grey, white box)
- Operating system auditing

The output from this step is a list of contextual application stressors. The overall output from STEPS 5 and 6 is a collection of resources and stressors that prevail at the HIA layer.

5.5.7 STEP 7: Present findings and proposed controls

This step consolidates the identified resources and stressors through a purpose assembled stakeholder panel that consist of the role-players and any information security specialists. The objective of this panel is to verify the validity and relevance of

the identified resources and stressors. The stakeholder panel should be representative of all the parties involved in the health service delivery process including any external service providers.

This step encourages further input in the form of omitted resources/stressors and/or those that may be deemed irrelevant. Corrective action can be taken to ensure the resources and stressors identified are indeed relevant to the context and can be corroborated by the stakeholders.

5.5.8 STEP 8: Construction

The objective of STEP 8 is to establish controls based on the resources identified to address the stressors. As part of this process, the identified resources are mapped to the identified stressors in an effort to identify those that can be addressed by utilising controls derived from the existing resources. The controls leverage the identified intrinsic and extrinsic resources in developing appropriate controls that can mitigate against some of the prevailing health information security stressors. Figure 5-6 illustrates the objective of the construction process.

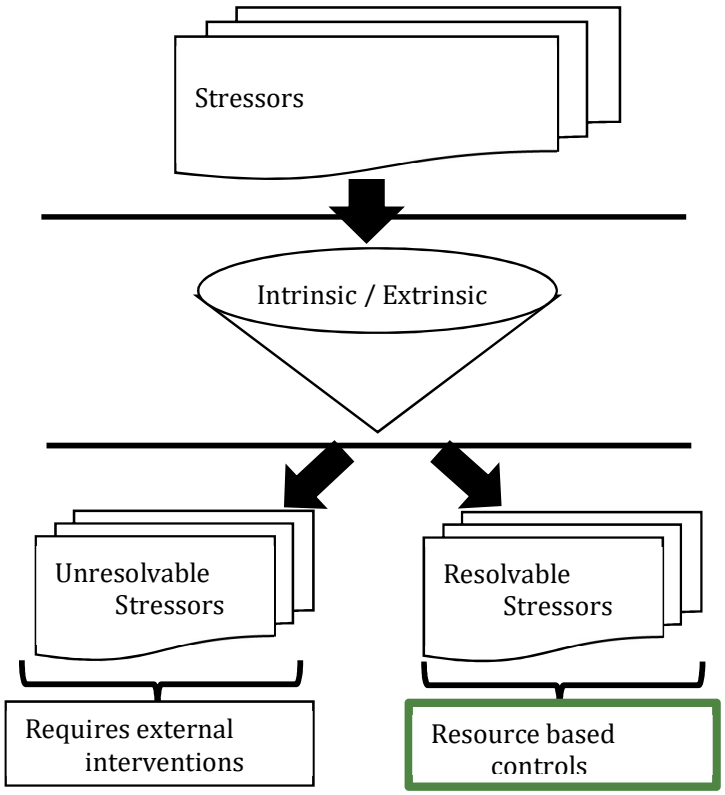


Figure 5-6: Outcomes of the Construction Dimension

The objective of the framework is to develop resource based controls that can be utilised to address the identified contextual stressors. This is accomplished in the construction process.

The unresolvable stressors are those identified as requiring external interventions and these can be catalogued and ideally addressed as and when the organisation has the required resources at its disposal either through resources identified in further iterations of the framework of external interventions.

5.6 Variable applications of the framework

In some situations, the framework may be applied partially, this could be in any one of the following situations:

5.6.1 Identification of Resources and stressors at a single layer

In this instance, the framework application can follow the path of steps:

***(1, 2), 7 and 8*:** This would be applicable in a paper-based document environment. There would be no technological aspects supporting the day-to-day activities and the resources and stressors would be entirely dependent on the HIUs.

(3, 4), 7 and 8: In situations where there is a need to investigate the technology aspects in isolation, this path can be followed. One possible scenario would be in an environment where there are adequate controls deployed at the HIU and HIA layers.

(5, 6), 7 and 8: In situations where adequate controls have been deployed at the HIU and HIT layers, the framework can be applied at the HIA layer in isolation.

5.6.2 Identification of either resources or stressors only

In this instance, the application can follow the path of steps:

1, 3, 5, 7 and 8: This path can be followed if the objective is to solicit the resources available across the three layers. This can be done as part of an inventory auditing exercise to identify the existing resources.

2, 4, 6, 7 and 8: This path can be followed if the objective is to identify the challenges persisting in the context. This could be part of an exercise to determine any internal or external interventions that may be required.

5.6.3 Extending the framework

The three layers presented in this framework can be expanded to include other layers as seen fit within the context. This will simply add another layer of iteration between the two dimensions when traversing the framework.

5.7 Bringing it all together

The objective of the framework was to iterate through the three proposed dimensions in an effort to identify resources and challenges that persist within each layer. By so doing, the organisation identifies intrinsic and extrinsic resources that can be considered assets for health information security. This approach is resource friendly and requires little to no investment in external resources. While it can be argued that the identified resources are not adequate to fully protect the information systems, the stance of this study is that the outcomes from the application of the framework provides immediate protection using the available resources and enables the planning of external interventions in addressing the identified stressors for which no resources exist. The external interventions can thus be budgeted for and implemented over the longer term while utilising the existing resources. The reality is that the need for improved health services within resource constrained settings is a more critical need than that of information security compliance. Therefore, it is necessary to implement transitory mechanisms that enable health service delivery while addressing the information security requirements in as far as the existing resources allows.

In conclusion, this framework offers systematic guidelines on how community based rural healthcare organisations can develop information security controls to mitigate some of the challenges faced using existing contextualised resources. The framework recognises that additional external interventions may be required to achieve the ideal information security posture.

5.8 Conclusion

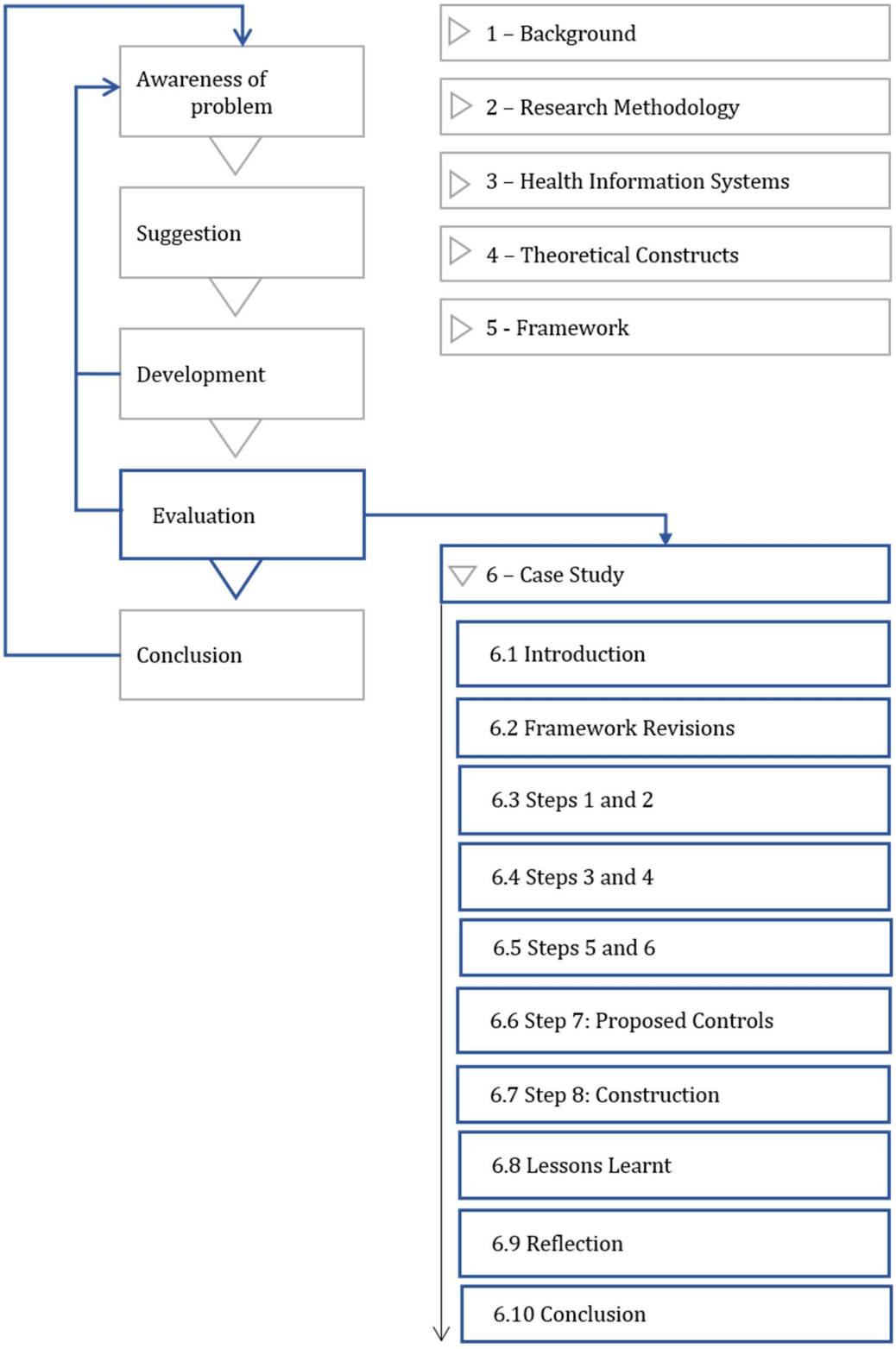
This chapter presented the framework developed as the output of this study. The chapter lead by presenting the constructs (salutogenic resources, pathogenic stressors) and dimensions (HIU, HIT, HIA) identified as input to the framework. This was followed by a description of the layers within the framework. Thereafter, guidelines specifying the sensible application of the framework were presented. The chapter concludes by

motivating the need for the framework and its relevance in the resource constrained context.

Chapter 6 presents a case study in which the framework was applied in an effort to determine its utility.

EVALUATION

6. Framework Evaluation: Case Study



6.1 Introduction

A design science artefact must satisfy the requirements for utility, quality and efficacy and this should be demonstrated in the evaluation of the artefact. The evaluation methodology was introduced in Chapter 2 section 2.8. The aim of this evaluation phase of the study was to demonstrate the utility of the framework in a simplified application. The chapter presents the outcomes from the application of the framework in a case context. The feedback is categorised according to the relevant steps of the framework to which it applies. Resources and stressors are identified and presented at each step. The chapter concludes by consolidating the resources and stressors before presenting the lessons learnt.

6.2 Framework revisions

The changes adopted during the evaluation activities (Chapter 6 and 7) have been integrated into the framework presented in Chapter 5.

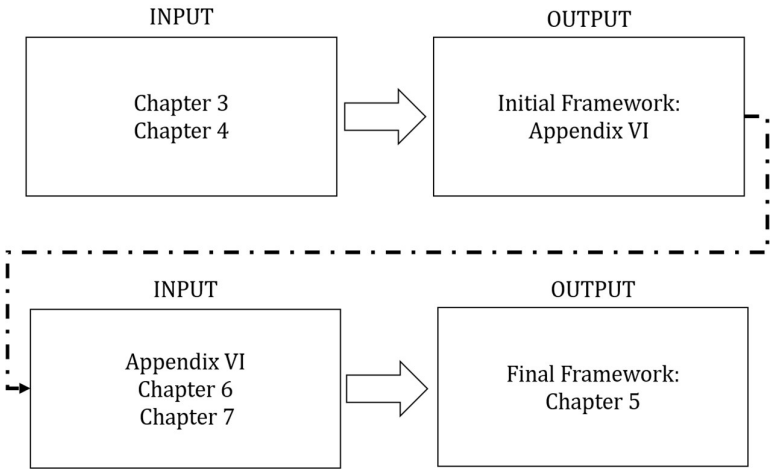


Figure 6-1: Framework Revisions

Figure 6-1 illustrates the presentation of the framework revision in this thesis. The initial framework (Appendix VI) is based on theoretical constructs drawn from chapters 3 and 4. The final framework (Chapter 5) is based on the initial framework (Appendix VI) incorporating feedback from the DS evaluation phase in the form of lessons reported in Chapters 6 and 7.

Thus, the reader should note that Chapters 6 and 7 are based on the initial state of the framework as reported in Appendix VI.

6.3 Steps 1 and 2

In these first steps, health information security resources (STEP1) and stressors (STEP2) are identified. Resources at the HIU layer typically consist of intrinsic and extrinsic human factors that promote the secure use, storage and retrieval of health information. This process requires extensive dialog with the organisation management, IT / technical personnel, CHWs and members of the community. In addition to identifying the human oriented health information security resources, STEP 1 should also explore the workflows and procedures that define the HIUs day-to-day activities.

Two activities were conducted in these steps; these are subsequently expounded.

6.3.1 Informal interview

The researcher engaged a supervisory staff member who was responsible for monitoring the day-to-day activities of the CHWs and analysing the data collected. The activity cycle presented in figure 6-2 illustrates the outcome from this dialogue.

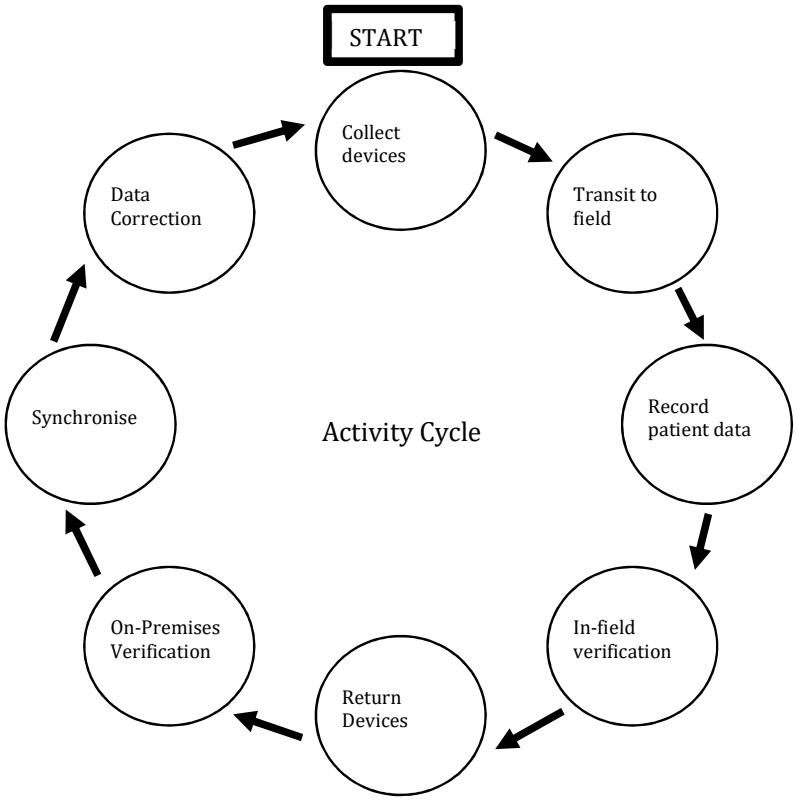


Figure 6-2:CHW Daily Activity Cycle

The activity cycle served to provide a background into the daily operations of the CHWs and provided the foundation on which questions probing specific areas could be developed in an effort to identify health information security resources and challenges.

6.3.2 Questionnaire

To reiterate from Chapter 2 (section 2.7.1.1), this study employed qualitative questionnaires as a research instrument. The questionnaires were developed during the time spent at the organisation. The questionnaires were distributed to twenty-five community healthcare workers and used in the study with the aim of establishing their day-to-day routine that involves the use of mobile computing devices. The CHWs are identified by a unique identifier following the format [P{num}] where P represents the participant and {num} represents the participant number. The questions sought to gather some insight into the security consciousness of the rural community and the community health workers regarding health related information from the perspective of the CHWs. Through the use of the questionnaires, resources and stressors in the rural health information systems were identified. The questionnaire is attached as Appendix III. The participants who were available to participate were mostly CHW's and as a result, the questionnaire was developed with an emphasis on the HIU aspects of security in the context. The following questions and subsequent responses addressed the HIU aspect within the context.

Question 3

On collecting the devices, what is the general procedure that you go through?

Qualitative analysis

The participants referred to the procedures for returning the device and most participants mentioned that the data is verified and the supervisor at days' end collects the devices. Two participants however interpreted correctly and stated that they ensure the devices are fully charged before taking them out to field

Question 6

Are there any records kept regarding your collection and return of the devices?

Qualitative analysis

Responses to this question indicate that there are no records of device collection or return.

Question 7

What other activities do you conduct on these devices?

Qualitative analysis

The full consensus from the participants indicates that no other activities are conducted on these devices aside from those prescribed for work

Question 8

Have you received training in the use of the devices? If so, how often?

Qualitative analysis

Feedback regarding training varied significantly, the training frequencies varied from [P14] *"yes, once"*, [P1] *"yes, 2 x a week"*, [P2] *"yes, before we use any devices we get a training for it for 2 weeks"*, [P4] *"yes, every time after a long holiday, an example after December holidays we go for refresher training"*. The variation in these responses may indicate that there are several training intervals involved, however, the lack of consistency across the result set may indicate a more ad-hoc training regime with no fixed schedule.

Question 9

Have you ever experienced a device failure? And if so, how often?

Qualitative analysis

The feedback was equally divided with half of the participants indicating that they have experienced device failure and the other half having not. Further analysis is complex without understanding the underlying cause of the device failure.

Question 10

Are you aware of the sensitivity of the information stored on the device? Please describe?

Qualitative analysis

The general awareness of information sensitivity was high amongst the participants with the full group indicating an awareness of the sensitive nature of patient information as highlighted by some of the responses: [P2] *"yes, I do notice every single task to store in the devices is confidential"*, [P11] *"yes, we don't have to expose information from*

my device to anybody except to my officials", [P19] *"yes, because the information of patient".*

Question 11

On a scale of 1 – 5, how proficient would you say you are with using the device?

Qualitative analysis

The majority of the participants selected option 2 *"comfortable working with common applications",* This was the second lowest competency option possibly indicating a lack of proficiency beyond performing the required task. A single participant selected option 1 for *"very basic skills".*

Question 12

On returning the devices, what is the general procedure?

Qualitative analysis

The CHWs all indicated that the devices are returned to the supervisor / team leader for data verification before making the final trip back to the organisation premises: [P1] *"submit to supervisor and team leader for data verification",* [P17] *"supervisors verify the work and after that shutdown the devices".*

Question 13

In your opinion, what security measures are in place on the device / application to prevent the loss or theft of information?

Qualitative analysis

Responses to this question include [P10] *"having my own user and password and always save at the end"* as identified by some participants. However, some participants indicated that there were no security measures in place and others simply did not know. Some interesting responses included [P4] *"none, it always safe because I work in my community and they know me"* and [P11] *"we save information".*

Question 14

How do you identify the clients that need to be seen?

Qualitative analysis

The identification of patients to be visited follows a common theme of recording health information on the device and in the CHWs notebook [P2] *"according to their readings BP, BS, and also conditions that goes along with the [organisation] programmes"*, [P1] *"I always write down the due date when I visit my client", "checking on screening database, door to door visit".* The responses varied in text, however a pattern of user vitals being checked and those exceeding thresholds being identified for further visits emerges. Additionally, door-to-door visits are conducted to provide additional support within the community.

Question 15

How many clients do you visit per day?

Qualitative analysis

On average, each CHW sees between 5 to 10 clients per day. A single participant highlighted that the small number of clients seen is to ensure accuracy: [P10] *"because the process is still new, I saw 5 - 10 per day so that my work will be accurate".*

Question 16

Please explain how you travel from the site to your patients?

Qualitative analysis

CHWs are transported to the communities via organisation provided vehicles, once in the communities however, patient visits are conducted on foot. This may involve walking significant distances whilst carrying the devices used in the field.

Question 17

Before screening, what measures are put in place to assure the patient? In your opinion is this important?

Qualitative analysis

Consent forms are the standard practice when approaching the clients: [P2] *"terms and conditions, patient client consent, I do introduction to the client too"*. Additionally, issues of CHW - patient confidentiality are addressed: [P8] *"it is important to always assure the patient that all the information will be strictly confidentiality, make sure the introduction is very clear and must always be consent form too".* The CHWs also

use this opportunity to introduce the program and the intentions of the organisation: [P12] *"I firstly introduce myself and also the foundation + explain exactly what is [project_name] and its purpose, yes this information is important"* and in some instances, counselling is given: [P11] *"I identify myself, I give my patient counselling"*. The emphasis in the responses is on introducing the program and the objectives of the visit.

Question 18

In your opinion, are the clients generally forthcoming with information regarding their health status?

Qualitative analysis

The responses indicate that the patients are generally forthcoming as the majority of the participants indicated as such: [P2] *"yes, they depend on the health education they get from Chow and they may end up motivated for their health risks to consider them"*. However, some patients are not comfortable and may resist any attention from the CHWs or not respond truthfully: [P5] *"no, some of them have a problem of denial"*.

Question 19

Based on your judgement, do the patients understand the information conveyed to them before divulging any health related information.

Qualitative analysis

The responses indicate that only some of the patients are well informed of the activities to be conducted prior to any action. The CHWs convey their intention and the potential benefits to the patient as seen from the following extracts: [P4] *"yes, because we do introduce what we are here for, what will be doing",* [P2] *"yes, the health education come up with new information full of advices"*. However, some responses indicate the lack of trust and perhaps elements of misunderstanding: [P23] *"no, sometimes it may happen especially for the first time because they don't believe that we are dealing with health status only"* and several responses of just [P15,18,19] *"no"*.

Question 20

Do you ever encounter patients and /or their household members who may want to interact with the devices directly?

Qualitative analysis

In the few cases identified, children are noted to take a special interest in the activities and possibly fascination with the technologies in use: [P8] *"yes, children always want to be checked BP",* [P23] *"yes, especial youth members, they are curious to see everything in the laptop during screening",* [P16] *"yes, I tell them that the device is not allowed to be touched by someone else".*

Question 21

Are the patients generally comfortable with the use of the devices during the screening process?

Qualitative analysis

Feedback regarding patient comfort with the use of the devices for health screening purposes was mixed. For the most part, the CHW's are of the consensus that the patients are comfortable, but in two cases, the CHW's highlighted trust issues: [P16] *"no, others ask many questions about it and they suspect that we are about to take their grant, but I manage to explain for them"* and [P23] *"no, they don't believe everything especial when you ask their identity document to see the age"*.

6.3.2.1 *Summary of findings: Resources [Step 1]*

The resources identified represent the variables that can be considered enablers for health information security in the context. The resources identified are listed and subsequently discussed.

CHWs demonstrate security compliant behaviour (Q7)

The CHWs demonstrate compliant behaviour in their using devices strictly for work related activities. This reduces the devices exposure to deliberate or accidental threats emanating from a user's personal activities.

The organisation has put regular training programs in place (Q8)

The organisation has put in place training structures from which regular training activities are conducted. This platform can be used to disseminate information security knowledge and provide compliance training.

Most CHWs have basic information security awareness (Q10)

The feedback indicates high levels of competency and health information security awareness. An understanding of the sensitive nature of health information may influence an individual's conduct when handling such information.

The smaller workload allows for better data capturing accuracy (Q15)

A generally small daily workload allows for more accurate data capturing. Data input errors may adversely result in the alteration of prescribed intervention to the detriment of the patient. Moreover, erroneous data compromises the integrity of the stored patient information.

CHWs diligently seek informed consent from the patients (Q17)

An emphasis on obtaining informed consent from the patient before carrying out any course of action emphasises the acknowledgement of a patient's right to privacy.

Some patients demonstrate trust in the proceedings (Q18, 21)

The CHWs indicated that patients were generally forthcoming with their health information. This could be an indication of patient trust in the CHWs activities. A lack of trust could result in patient providing misleading information which can affect their well-being if a course of action is prescribed.

6.3.2.2 *Summary of findings: Stressors [Step 2]*

The stressors identified, similarly to the resources, represent the variables that can be considered disablers or challenges for health information security in the context. Some of the variables classified as resources are also identified as stressors due to the variation in skills, knowledge and ability within the workforce, for example, while some may demonstrate compliant behaviour, new employees lacking experience may demonstrate misbehaviour. The stressors identified are listed and subsequently discussed.

Lack of accountability stemming from the lack of device ingress and egress records. (Q6)

Record keeping is a crucial aspect in facilitating accountability. Without records of who has collected what device and at what time, tracking the ingress and egress of the devices becomes a complex matter. The feedback indicates that the organisation has no such structures in place and thus, may not be able to adequately account for all the devices that may be containing sensitive information.

Lacking security control awareness (Q13)

When prompted to comment about the existing security measures, the feedback indicated a lack of security control awareness. If the user does not understand the purpose of some of the measures put in place, they are more likely to circumvent the measures or disregard the measures all together.

Consent granted without full awareness of the implications (Q19)

Despite the established structures for securing patient informed consent, the indication from the feedback was that few patients understood the information conveyed to them and even fewer understood the implications. This could either be caused by the CHWs failure to adequately convey the information or the lack of understanding on the part of the patient.

Some scepticism of screening processes (Q19, Q21)

The CHWs are tasked with being the gateway between the organisation and the patient. The relationship established between the CHWs and the patients can significantly affect the capacity to render services. The feedback indicated some instances of trust breakdown where the patients were not trusting of the activities of the CHW. The lack of trust in some proceedings emanating from the community may be an indication of some CHWs not performing their duties with due diligence. This could be as a result of previous breaches of confidentiality or privacy and may have instilled a sense of scepticism amongst some of the community members.

6.4 Steps 3 and 4:

The third and fourth steps move onto the HIT layer. The objective of these steps is to identify the technology or infrastructure resources (STEP 4) and stressors (STEP 5) affecting the secure use, storage and retrieval of health information. These steps require an intermediate-to-advanced knowledge of the information systems in use and are typically conducted with the inclusion of IT or technical support personnel.

The following questions were aimed at identifying the HIT aspects of heath information security within the context from the perspective of the CHWs. Fewer questions were presented in this regard because of the CHWs limited ability to provide significant information of value regarding the HITs.

6.4.1 Informal Interview

The interview conducted was discussed in section 6.3.1 and applies to the HIT layer as well.

6.4.2 Questionnaire

The questionnaire discussed in section 6.3.2 included questions surrounding the HIT aspect within the context. The following questions and subsequent responses addressed the HIT aspects.

Question 1

What devices do you use to conduct your daily activities?

Qualitative analysis

Participants were generally aware of the devices they use for the day-to-day activities. The devices would have been introduced to the participants through an induction training program.

Question 2

Are any of these devices (devices in Q1) personally owned?

Qualitative analysis

The responses to this question indicate that the devices are IPDs (owned by the organisation) and none of the employees are specifically using a personal device for work activities. This is supported by the consistent responses to Q7 where the participants identified the devices as for the sole purpose of work related activities. The maintenance and support burden remains on the institution.

Question 4

Are you issued with a dedicated device?

Qualitative analysis

Most of the participants responded *"yes"* to this question. Each user is issued a dedicated device to use in the field. However, a small portion of the sample are sharing devices.

Question 9

Have you ever experienced a device failure? And if so, how often?

Qualitative analysis

The feedback was equally divided with half of the participants indicating that they have experienced device failure and the other half having not. Further analysis is complex without understanding the underlying cause of the device failure.

Question 13

In your opinion, what security measures are in place on the device / application to prevent the loss or theft of information?

Qualitative analysis

Responses to this question include [P10] *"having my own user and password and always save at the end"* as identified by some participants. However, some participants indicated that there were no security measures in place and others simply did not know. Some interesting responses included [P4] *"none, it always safe because I work in my community and they know me"* and [P11] *"we save information".*

Question 16

Please explain how you travel from the site to your patients?

Qualitative analysis

CHWs are transported to the communities via organisation provided vehicles. Once in the communities however, patient visits are conducted on foot. This may involve walking significant distances whilst carrying the devices used in the field.

Question 21

Are the patients generally comfortable with the use of the devices during the screening process?

Qualitative analysis

Feedback regarding patient comfort with the use of the devices for health screening purposes was mixed. For the most part, the CHW's are of the consensus that the patients are comfortable, but in two cases, the CHW's highlighted trust issues, [P16] *"no, others ask many questions about it and they suspect that we are about to take their grant, but I manage to explain for them"* and [P23] *"no, they don't believe everything especial when you ask their identity document to see the age.*

Question 22

Do you ever feel at risk when travelling with these devices? Please elaborate?

Qualitative analysis

The majority of the CHW's felt at ease when travelling with the devices within the communities: [P13] *"no, we are serving our communities they understand that we are helping them. No intimidation".* Two of the participants cited occasional safety concerns for the devices and their physical well-being: [P25] *"sometimes I have a fear of robbery/theft because sometimes I travel in the communities I don't know the people of that community",* [P23] *"sometimes when I met with strangers, I don't feel happy because I don't know whether they can take the laptop or not".*

Question 23

Have you ever experienced /are you aware of any prior loss or theft of the devices?

Qualitative analysis

None of the participants in the sample was aware of any incidents of device loss or theft. One of the participants attributed this to their diligence in caring for the devices: [P2] *"no, I'm aware of keeping the devices safely and always care".*

6.4.2.1 *Summary of findings: Resources [Steps 3]*

The resources identified represent the variables that can be considered contextual enablers of health information security at the HIT layer. The resources identified are listed and subsequently discussed.

Dedicated devices for each CHW (Q4)

Ensuring that each CHW has a dedicated device or at least a user account allows for accountability. Accountability enables the organisation to monitor the activities of individuals and identify areas of weakness within the teams. Additionally, if users are made conscious of the monitoring activities, they are more likely to desist from deviant conduct.

Security control awareness amongst some CHWs (Q13)

Basic awareness of security controls such as usernames and passwords may indicate an understanding of the importance of authentication and authorisation when conducting daily activities. This may emanate in users knowing to log out of the system when not

actively using it. This protects against unauthorised access thereby protecting the confidentiality and privacy of the patient information.

Physical device safety in community stemming from community buy-in (Q22)

Members of the community are essential in enabling the organisation and the CHWs to conduct their activities without hindrance. This is exemplified by the feeling of security some of the CHWs have when working in the communities. Having the community's backing reduces the likelihood of malicious incidents emanating from the community.

CHWs exercise due diligence in caring for the devices (Q23)

The fact that there have been no incidents of device loss or theft recorded is an indication of the due diligence the CHWs exercise in looking after the devices and generally conducting their activities in a manner that does not put themselves or the devices at risk. The loss or theft of devices can compromise the availability of information stored on the specific device and the privacy/confidentiality of the information stored within.

6.4.2.2 *Summary of findings: Stressors [Step 4]*

The stressors identified, similarly to the resources, represent the variables that can be considered contextual disablers or challenges for health information security at the HIT layer. The stressors identified are subsequently discussed.

Incidents of device failure (Q9)

Device maintenance programs must be put in place (in as far as possible) to minimise device failure in the field. Device failure may significantly compromise the availability of information that is stored within. This could be particularly catastrophic if the information has not been synchronised or backed up to a different location.

Lack of IT proficiency (Q11)

The lack of IT proficiency may not have a direct impact on a CHWs ability to perform their duties, however, it may have significant implications on their efficiency. Minor device issues that should be resolved in the field may be beyond the capacity of the CHW thereby creating hold-ups in service delivery. Additionally, the lack of proficiency may also lead to a higher incidence of human error and omission. The feedback indicated that the CHWs were only proficient as far as their tasks on the device require.

Lacking security control awareness amongst some CHWs (Q13)

When prompted to comment on the existing security measures, the feedback indicated a lack of security control awareness. If the user does not understand the purpose of some of the measures put in place, they are more likely to circumvent the measures or disregard the measures all together.

6.5 Steps 5 and 6:

These steps move onto the final layer where the application resources and stressors affecting the secure use, storage and retrieval of health information are identified. These steps require the input from personnel with an in-depth understanding of the application and other operating system tools that are part and parcel of the service delivery process. The personnel may be part of the HIU, or internal/external developers responsible for the application development. Activities in this step are similar to those in STEP 1.

The following questions and subsequent responses addressed the HIA aspect within the context.

6.5.1 Informal Interview

The interview conducted was discussed in section 6.3.1 and applies to the HIA layer.

6.5.2 Questionnaire

The questionnaire discussed in section 6.3.2 included questions surrounding the HIA aspect within the context. The following questions and subsequent responses addressed the HIA aspects.

Question 5

If no (Q4), do you have separate user accounts on these devices?

Qualitative analysis

The feedback indicates that each user on a shared device has their own user login and application account.

6.5.2.1 *Summary of findings: Resources [Step 5]*

The resources identified represent the variables that can be considered enablers for health information security in the context. The resources identified are listed and subsequently discussed.

Dedicated user accounts for each CHW (Q4, Q5)

Ensuring that each CHW has a dedicated user account allows for accountability. Accountability enables the organisation to monitor the activities of individuals and identify areas of weakness within the teams. Additionally, if users are made conscious of the monitoring activities, they are more likely to desist from deviant conduct.

6.5.2.2 *Summary of findings: Stressors [Step 6]*

The stressors identified, similarly to the resources, represent the variables that can be considered disablers or challenges for health information security in the context. Some of the variables classified as resources are also identified as stressors due to the variation in skills, knowledge and ability within the workforce, for example, while some may demonstrate compliant behaviour, new employees lacking experience may demonstrate misbehaviour. The stressors identified are subsequently discussed.

Incidents of device failure (9)

Device maintenance programs must be put in place (in as far as possible) to minimise device failure in the field. Device failure may significantly compromise the availability of information that is stored within. This could be particularly catastrophic if the information has not been synchronised or backed up to a different location.

6.6 Step 7: Proposed controls

This step was partially conducted. Due to logistical complexities, the findings could not be presented to a stakeholder panel in the context. Their role would have included additions and subtractions from the catalogue of resources and stressors. However, this section proceeds to discuss the proposed controls.

In an effort to present draft controls, a process of resource mapping was conducted. In this process, resources are mapped to stressors that they are deemed to have the capacity to address. This process in subsequently discussed.

6.6.1 Mapping Resources to Stressors

Having concluded the identification of the resources and the stressors, table 6-1 presents the mapping of the resources to the stressors. These are discussed in detail following the presentation of the table.

Table 6-1: Resource Mapping

Stressors	**Resources**
Lack of accountability stemming from the lack of device ingress and egress records. (Q6)	Dedicated devices / account for each CHW (Q4, Q5)
Incidents of device failure (Q9)	Presence of training structures (Q8)
Lacking trust relationship with community members (Q21, Q18)	Compliant behaviour (Q7) Informed consent (Q17) Patient trust (Q18)
Lacking IT proficiency (Q11)	Presence of training structures (Q8)
Lacking security control awareness (Q13)	Presence of training structures (Q8) Information security awareness (Q10) Security control awareness (13)
Scepticisms of screening processes (Q19, Q21)	Compliant behaviour (Q7) Informed consent (Q17) Patient trust (Q18)
Consent granted without full awareness of the implications (Q19)	Informed consent (Q17)

Lack of accountability stemming from the lack of device ingress and egress records. (Q6):

The organisation can take advantage of the fact that each user is issued a dedicated device for their daily activities. Binding a user to a specific device and storing records on who has been issued which device can aid in instilling accountability.

Incidents of device failure (Q9):

The frequency of device failure would typically require technical skills to provide maintenance and repairs. However, not all device failure can be classified as catastrophic, hence, some minor troubleshooting tasks can be performed by the CHWs if provided with adequate training. The organisation can take advantage of the existing training structures to include basic hardware troubleshooting into the disseminated skillsets.

Lacking trust relationship with community members (Q21, Q18)

Establishing trust with the community members (patients) is likely to result in patients providing accurate information. A few CHWs noted how some patients were hesitant to provide information regarding their health status as they were not fully trusting of the CHWs. Leveraging the compliant behaviour of some of the CHWs to serve the role of champions and/or mentors to the non-compliant CHWs may aid in improving the organisational image and thus improving the trust relationships.

Additionally, the CHWs can leverage the process of obtaining patient consent to adequately reassure the patient that their activities are in the best interest of the patient.

The CHWs can also take advantage of the trusting patients who have seen positive results for the interventions to provide advocacy within the community thereby reassuring the rest of the community on the legitimacy of the services being rendered.

Lacking IT proficiency (Q11)

The organisation has a big role to play in improving the general IT literacy of the CHWs. As previously discussed, improved IT literacy can result in increased CHW efficiency, reduce the incidence of human error / omission and reduce the frequency of device failure.

Lacking security control awareness (Q13)

The existing training structures can be leveraged to provide security control awareness. Additionally, the existing awareness knowledge present in some of the CHWs can be shared through peer training and mentorship strategies. This reduces the reliance on organisational training structures for the dissemination of security control awareness information.

Scepticisms of screening processes (Q19, Q21)

Scepticism can be overcome through the informed consent process. The CHWs can ensure that the patient has been adequately informed and reassured about the intent of the CHW. Additionally, compliant behaviour can be learnt through peer mentoring and observation with the aim of presenting the CHW in a professional manner. Moreover, overcoming the scepticism aids in building trust. Moreover, advocacy in the community may be sought from patients who have benefited from the system and are trusting of the CHWs activities.

Consent granted without full awareness of the implications (Q19)

This again can be addressed by ensuring adequate information is disseminated during the process of seeking consent. The CHW must ensure the patient is fully aware of the implications of granting consent.

The following section maps the identified resources to the salutogenic constructs discussed in section 4.6.

6.7 Step 8: Construction

In this final step of the framework, information security controls are developed from the identified contextual resources. This step follows from step 7 and utilises the output from the resource mapping exercise as input to the control development.

The following section provides example of controls that could be developed in line with the identified contextual resources and stressors.

6.7.1 Developing controls

In developing controls, there are various types of controls that could be deployed to achieve the same objective, this section only presents examples and is not exhaustive.

Knowledge controls

- Planned teaming can be used to bring together users with different strengths so as to encourage information security consciousness through peer observation and information sharing. From the case, some users had good levels of information security awareness and others were good at communicating with the patient in a way that encouraged trust and truthfulness. Teaming users with these strengths benefits the users, patients and the organisation.

- Guidelines can be developed to be utilised as quick references when users are unsure. These guidelines can include basic device troubleshooting and procedures to be followed in the event of an undesirable incident. This may aid in reducing downtime associated with device failure and improve response times to security incidents.
- Workshops can be utilised as mechanisms for information dissemination and raising information security awareness. Through these workshops, information pertaining to safe device usage and overcoming security related stressors encountered in the field can be disseminated. The organisation can leverage the existing training structures to develop training and awareness materials that address the identified stressors. Additionally, these workshops can be utilised as a platform for information sharing between the organisation, the IT / Technical personnel, the CHWs and members of the community through which security concerns are raised and effective means of mitigating the challenges proposed from the various perspectives of the role-players involved.

Behavioural controls

- Information sharing – This can be done through teaming CHWs to enable non-compliant users to learn from observation the appropriate conduct. Additionally, compliant users can be elevated to supervisory / mentorship roles to exercise their influence over less experienced users.
- Elevate users displaying compliant behaviour to supervisory / mentorship roles. This has the dual purpose of providing reward based incentive and allows mentees to learn through peer observation / influence.
- Role rotation can be instituted to broaden user understanding of the HIS. This additionally promotes in skills development and broadens information security awareness across multiple layers of the HIS.
- The existing processes to obtain informed consent can be improved by providing language translation to better facilitate the patient's understanding of implications of granting consent. This could aid in improving the trust relationship between the patients and the CHW / organisation thereby increasing the likelihood of obtaining correct information.

As previously stated, the controls can manifest in a variety of forms. This section identified knowledge and behavioural controls that can be instituted with the aim of addressing the identified stressors without investing in external interventions. These

controls may not address the complete list of identified stressors but can go a long way in stifling the vulnerability of the HIS in operation.

External interventions can be added as and when the means are available to address the remaining stressors. However, knowledge of the stressors in itself may allow the organisation to identify workarounds or preventative measures that can minimise the negative impact of the unresolvable stressors.

6.8 Lessons learnt

Due to the unavailability of a diverse set of participants, the demographic of the participants consisted entirely of CHWs and a single Supervisory / IT staff member. Consequently, the questions were targeted primarily at this demographic. This however presented some limitations on the feedback provided. Comparatively, there was limited input addressing the HIT and HIA aspects. When applying the framework, to obtain more accurate feedback, one must try as much as possible to include a diverse set of participants.

From the researcher's experience implementing the framework, one question that came up was "who would apply the framework?". It was clear that the initial application of the framework would require the assistance of knowledgeable individuals in information systems / information security. As part of their activities, internal organisational capacity must be developed seeing as the framework is likely to have multiple iterations applied over a period of time.

6.9 Reflection

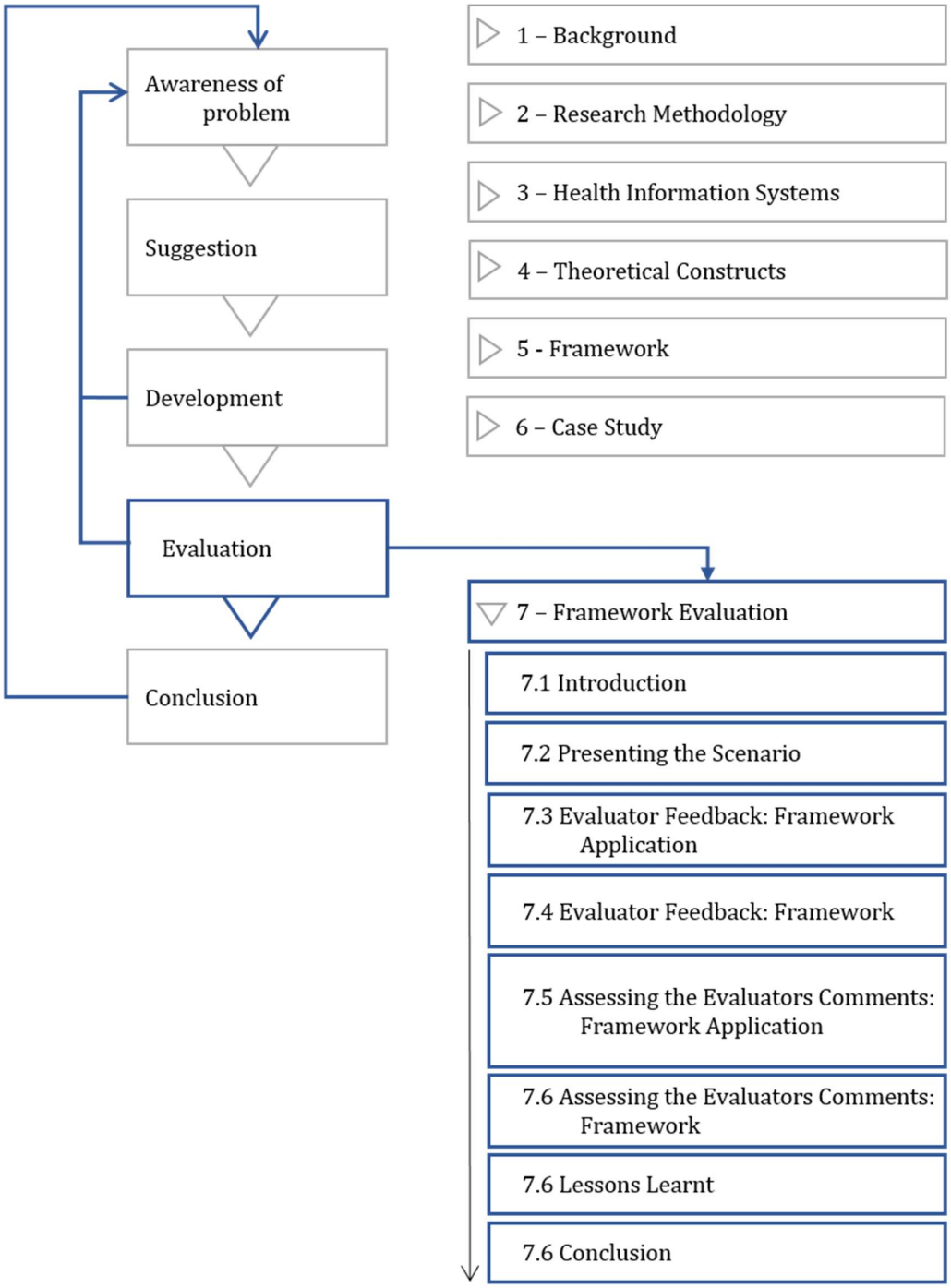
In identifying resource based controls, it should not be overlooked that appropriate technical controls such as cryptography and biometric authentication can go a long way in mitigating against some of the stressors. However, the applicability of these controls is dependent on the availability of technical know-how and support. The study seeks to determine the availability of controls in a context in which these resources are severely scarce or unavailable. Therefore, without undermining the significant relevance of technical controls in addressing the stressors, in a critically resource constrained context, these would only be available through external interventions / service providers. The framework makes for provision for the implementation of technical controls as and when the required resources are available, however in the interim, internal controls utilising existing resources may provide some measure of protection to

facilitate the continued use of ICT's for service delivery albeit with reduced information security vulnerabilities.

6.10 Conclusion

The case study outcomes presented in this chapter sought to better understand the context under study. This was achieved by developing and distributing an open ended questionnaire to twenty-five CHWs that encouraged participants to comment generally on their day-to-day activities. Thereafter, the framework was applied to the case in an effort to identify the resources, stressors and subsequently develop resource based controls. The lessons drawn from this experience were integrated into the final framework presented in Chapter 5.

7. Framework Evaluation: Expert Evaluations



7.1 Introduction

Chapter 6 presented the first phase of the evaluation process which was aimed at establishing the utility of the framework through the use of a case study. This chapter presents the second phase of the evaluation process in which an illustrative scenario was developed and presented to a panel of experts for evaluation. The framework presented in Chapter 5 includes the revisions from this evaluation process and the original submission to the experts is available in Appendices V, VI and VII. The chapter leads by presenting the scenario before proceeding to present the feedback from the evaluators and the implications of the feedback on the framework. The chapter concludes by presenting lessons learnt through the evaluation process.

7.2 Presenting the scenario

Scenarios have been described as a valid method of evaluating a DSR artefact (Hevner, March, Park, & Ram, 2004). For the purposes of evaluating the artefact, a scenario was developed to emulate a community based rural healthcare organisation which would ideally be in a position to make use of this artefact. The scenario design was influenced by the findings from the empirical data in Chapter 6 where the personnel in a community based rural healthcare provider were asked to complete questionnaires inquiring about their day to day activities with regards to the use of health information systems.

The scenario has been modified in line with the ethical requirements as discussed in Chapter 1 section 1.9 to ensure that no information that can be used to identify the participating institution or individuals will be published. The scenario is subsequently presented.

RHealth Etcetera recently introduced mobile computing devices as part of their expansion into communities that were previously inaccessible due to distance and infrastructure constraints. The mobile computing devices have allowed the organisation to deploy embedded CHWs who are in an ideal position to serve their immediate surroundings and periodically visit the main site to synchronise the information gathered. The program has been a great success and the number of patients served has increased significantly due to the improved accessibility. With an estimated 30 000 patient records in their database, the security of the information assets has become a concern. There was an unconfirmed report about community health workers who may have shared patient information with a colleague and despite having training programs that teach against such behaviour, there are inadequate controls to guarantee that such events would not occur.

RHealth Etcetera has decided to call in an expert and express their needs and look for means to mitigate against information security threats such as these and any others they may have not yet encountered and because they have no prior experience in the information security domain, the only requirement they have identified is the need to continue operations without interruption because of the critical nature of the service they provide.

The security consultant has noted the unique constraints that face the organisation and has determined that simply applying low level frameworks will not yield the desired outcome because of the complexities identified in the organisation. The consultant has turned his attention to a framework that speaks to the rural health context and simplifies the rollout in a staggered but attainable way. It was subsequently agreed that standards and regulatory compliance was a necessity but one that was not immediately attainable.

7.3 Evaluator feedback: Framework Application

The overall feedback regarding the individual steps of the framework was positive. Evaluators where requested to rate each step on a Likert scale as presented in Table 7-1.

Table 7-1: Evaluators' Likert scale

1: Strongly Disagree	2: Disagree	3: Neither agree nor disagree	4: Agree	5: Strongly agree

Figure 7-3 illustrates the aggregated feedback from the evaluators who responded to the invitation to participate. As previously discussed in section 7.1, this feedback is based on the initial version of the framework that is presented in Appendix VI. The framework presented in chapter 5 has been revised in line with the lessons learnt from chapter 6 and the evaluators feedback subsequently discussed in this chapter.

Figure 7-1: Aggregated Expert Feedback for Framework Steps

Evaluators were asked to provide feedback on three aspects of the steps followed in arriving at the output of the framework. These are:

1. Feasibility – The feasibility requirement speaks to the ease in which a community based rural healthcare provider can execute the tasks prescribed in the step. This is a requirement for resource constrained settings and one that meets the requirements for design science.
2. Utility – The utility requirement speaks to the effectiveness of the measures recommended within the step in meeting the overall objective of the framework.
3. Completeness – The completeness speaks to the extent to which the step can be considered sufficient in meeting its objective and the overall objectives of the framework.

Following the evaluation of the steps, the feedback in the comments was categorised into 4 aspects based on the action to be taken regarding any recommended changes. These are listed as follows:

1. Minor editorial – these are small editorial changes that were to be applied to improve readability and address any areas where the evaluators may have had editorial issues.
2. Critical change – these changes were deemed significantly impactful and were to be incorporated as fairly significant adjustments to the steps and the overall framework.
3. Logical flow – these were changes that would impact the sequence of dimensions, activities or steps.
4. No change – No changes to the output was deemed necessary.

The overall feedback indicates that the framework steps were generally well received. The areas of concern were highlighted in the space provided for comments and are discussed in section 7.5.

7.4 Evaluator feedback: Framework

In addition to evaluating the individual steps, the evaluators were asked to rate the overall framework based on the same Likert scale. The ratings of the framework were aimed at obtaining an overall assessment of the framework. The aggregated feedback is presented in Figure 7-2.

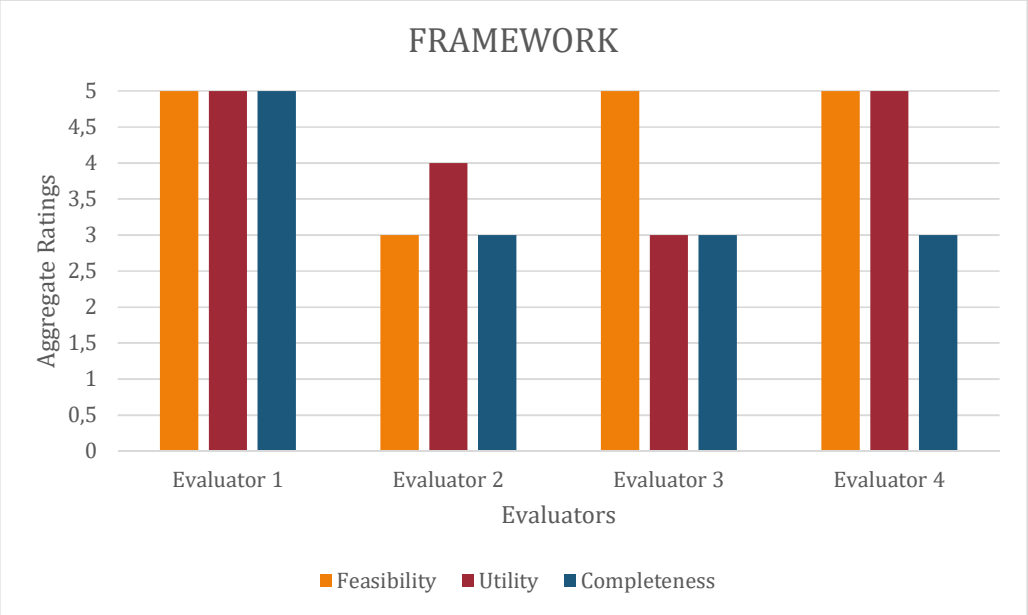


Figure 7-2: Aggregated Expert Feedback for Framework

The overall feedback regarding the framework was positive based on a minimum rating of 3. The evaluators did however note some areas of concern and recommended remedial adjustments in either presentation, logical flow or significant critical changes. These are summarised in Table 7-2.

Table 7-2: Summarised comments regarding changes

Evaluator		S1	S2	S3	S4	S5	S6	S7	S8	S9	Framework
E1	Minor Editorial	*			*			*			Recommended clarification of the flow between dimensions
	Critical Change										
	Logical Flow	*	*		*		*				
	No Change			*		*	*	*	*	*	
E2	Minor Editorial										Recommended merger of steps 6 and 7
	Critical Change	*									
	Logical Flow										
	No Change		*	*	*	*	*	*	*	*	
E3	Minor Editorial			*	*						Recommended additional inquiry methods.
	Critical Change	*		*	*						
	Logical Flow										
	No Change					*	*	*	*	*	

Evaluator		S1	S2	S3	S4	S5	S6	S7	S8	S9	Framework
E4	Minor Editorial										
	Critical Change										
	Logical Flow										
	No Change	*	*	*	*	*	*	*	*	*	
E1 – E4 = Evaluators 1-4											

Following the presentation of the evaluators feedback and the categorisation of their recommendations, the implications of the evaluators comments on the design of the steps and the framework are subsequently expounded in sections 7.5 and 7.6.

7.5 Assessing the evaluators comments (Steps)

The comments from the evaluators have been categorised as described in section 7.3 and are subsequently expounded. In this section, only the comments and recommendations that are aimed at improving the framework are discussed. Positive comments have been omitted from this discussion as they had no implications on the final version of the framework. In this discussion, the evaluators' feedback is presented as excerpts from the evaluators' worksheet, followed by the researcher's interpretation and course of action. The worksheet used is attached as Appendix VIII.

7.5.1 Minor editorial changes

Evaluator 1: [Steps 1,2 and 4] *Step 1 in Doc 1 doesn't seem to fully speak to Step 1 in Doc 2. Interview vs Survey. F: It would be nice to see how the framework handles security stressors in the CHW's living environment. C: It's hard to say.* [Step 4] *Similar to Step 1 and 2, it is not clear how this step is different from Step 3*.

The evaluator's concern was related to the fact that the activities in Step 1 in the documents submitted for evaluation differed. In the framework presentation (Appendix VI), surveys were listed while in the scenario document (Appendix VII), interviews were listed. Interviews and questionnaires are common research methods within surveys. To provide clarity, the step was revised to include a more comprehensive list of activities as shown in table 7-3.

Table 7-3: Revised Activities

Steps 1 and 2 [Section 5.5.1]	
Previously (Appendix VI)	Revised (Section 5.5.1)
Activities at this layer include: • Workshops • Questionnaires • Interviews	Activities at this layer include: • Workshops • Questionnaires • Interviews • Observational tag-along • Other inquiry methods (ethnographies, vanguard studies)

With regards to addressing the security stressors in the CHWs living environment, the narratives describing the steps were revised to provide greater emphasis on how security resources and stressors are dependent of the environmental variable, hence, the identified resources and stressors would reflect the resources and stressors prevalent in the living environment.

Evaluator 1: [Step 7] *Can this work seeing that the model is divided into user, technology and apps? From the framework it looks like CHW's and community members were involved in the first two steps only and so may feel left out in some of the issues.*

The steps in the framework iterate through different layers in an effort to ensure the best placed people to provide input for the different layers can do so without being tasked with providing input into activities that they are not involved in. For example, the IT / Technical personnel would have little knowledge of the events that occur in the field and similarly, the CHWs would have little knowledge of the inner workings of the technological systems supporting their activities. The emphasis is on the people who are likely to provide valuable feedback, however, the CHWs remain involved through the whole process. In line with the evaluator's comments and recommendations, the narratives in step 1-7 was revised to reflect the involvement of all parties.

Evaluator 3: [Step 4] "the questions seem to dwell more into the competences of the IT

technicians without delving into the capabilities of the technology and infrastructure. I would recommend adding a component of inventory auditing of the tech and infrastructure to investigate the resourcefulness or stressors thereof. "

To address this concern, revisions were made to the discussion on the steps to include additional activities that could be conducted in settings with a greater ability to spend but can still be considered resource constrained. Inventory auditing was included as a possible activity (dependent on resources) for Steps 3 and 4.

Table 7-4: Revised Narratives

Steps 3 and 4 [Section 5.5.3]	
Previously (Appendix VI)	Revised (Section 5.5.4)
Examples of activities at this step are similar to those discussed in STEP 1	Examples of activities at this step are similar to those discussed in STEP 1 and **can additionally include upfront activities such as inventory auditing**

This would result in less reliance on the input from the IT / Technical personnel alone and improve the reliability of the findings. However, in the application of the framework, one must be cognisant of the possible lack of the required skills / resources to conduct some of the suggested activities.

7.5.2 Critical changes

Evaluator 2: [Step 1] *Interaction with users (stakeholders) will clearly externalize what is important/concerning. How about a subtle un-announced sporadic field observation or tag along by say an independent expert/consultant to perhaps study behaviours of parties involved, note error rates, etc.*

The suggestion of adding subtle and un-announced sporadic field observation or tag along was deemed to be a valuable addition to the scope of activities that can be conducted in an effort to identify additional resources or stressors. Observational tag-alongs were added as possible activities across Steps 1-6 as this would aid in the identification of additional resources and stressors that may not be immediately apparent to those involved in the day-to-day activities. Refer to table 7-3 for the revised set of activities.

Evaluator 3: [Step 1] *The framework lacks in on completeness in that it relies on asking the users, there is a lot of insights which may be gathered through other means – like ethnographic studies and user observation in order to identify the things they might not have said, there is need to triangulate the findings with other methods which do not solely rely on what the users have said.*

In summarising the feedback from Evaluator 3, recommendations surrounding the diversification of the information sources to reduce reliance on user input by including additional inquiry methods were taken into consideration and factored into the discussion of example activities in the presentation of the framework in Chapter 5. This requirement was partially addressed by the inclusion of additional activities including observational tag-alongs as possible activities. Questions remain as to the feasibility of some of the suggested methods particularly considering the resource constrained characteristics. However, to improve the reliability of the findings, the framework has been revised to prescribe a minimum of two activities with no ceiling in each step. Over time and through multiple iterations of the framework, the more effective methods may emerge and take dominance. Refer to table 7-3 for the revised list of activities.

7.5.3 Logical flow

Evaluator 1: [Step 1, 2, 4, 6] *"I still do not get the distinction between the two seeing that they both cover the same issues. Maybe can be sorted out by adding the differences and similarities under each step in Doc 1. I have similar views for steps 4 and 6".*

The discussion surrounding the steps (Appendix VI) emphasises that the steps at each layer can and will most likely be conducted concurrently. The separation of the steps provides added flexibility in cases where perhaps the organisation may be interested in only identifying either the resources or stressors at the different layers. This essentially allows for partial application of the framework. The narrative has been revised to provide greater emphasis on the possibility of a partial application of the framework. See section 5.6 on the variable applications of the framework.

7.5.4 No changes

Evaluator 1: [Step 3] *I am neutral in this because I am not sure how much power technical support users might have in putting in place controls. My understanding*

is that security start at the top of the organisational hierarchy and so this might not be practical.

The contribution of the IT/Technical support personnel in the scope of the framework is towards the development of the controls. The framework is scoped only to the development of the resource based controls and does not address the implementation of the developed controls.

Evaluator 2: [Step 3] *This will clearly yield the relevant information. Additionally, though, a comparative analysis of current tech advancement vs what is in use can reveal opportunities that can be capitalised on. E.g. will adopting a current cloud solution be more advantageous.*

A comparative analysis while merited, could diminish the relevance of the specific context. What works in "context A" may be influenced by factors that are unique only to "context A". The framework aims to be as specific to a context of application as possible, hence, the suggestion was noted but had no bearing on the current framework.

Evaluator 3: [Steps 1 and 2] *"Also, I find that the questions in Step 1 & 2 do not address the aspect of resource constraint-ness of the environment, the questions do not probe that, they are generic to any context"*.

The resource constrained-ness of the environment emerges from the responses which are influenced significantly by the background / environment from which the participants originate. An example would be the response to a question like *"How accessible is your IT support*" where in one context, the response could be *"we have dedicated support"* and in another, *"support comes in once a month"*. The question is generic but the responses speak to the resource constrained-ness of the context which in this particular example would be the availability of skilled personnel.

Evaluator 3: [Step 3] *The IT / Technicians will only give you information based on the reference knowledge, which may be limited because they are operating in low resource contexts. It will be important to do a matrix of low resource – first world vs old tech – tech disruptors to identify the gaps and opportunities which may be incorporated to improve the security. Having said this, it is important to highlight that the IT Tech are only by another source of gathering requirements – they might not have the mandates for policy implementation as this is at a more higher level of governance.*

The two aspects addressed in this comment have been addressed previously. The comparison between low resource and first-world type context takes away from the contextualisation of the framework. While valuable insights may be obtained, the idea is that if the stakeholders are not able to internally identify factors as resources or stressors, the likelihood is that they would not be in a position to fully utilise the resource or be affected by the stressor. This type of activity can be conducted after the framework has been applied in an effort to extend the existing protection mechanisms that have been established exclusively through internally identified resources.

The second aspect speaks to the IT / Technical personnel's role as a source of requirement gathering. However, because management is involved throughout the process, they would have the capacity to deal with the policy related issues. The implementation of the technical controls may be subsequently delegated to the IT / Technical personnel.

Evaluator 3: [Step 5] *I am still not convinced of the difference between HIT and HIA, in my understanding applications are part of technology which are enabled using the infrastructure. To get an understanding as to the degree to which the applications satisfy the required security it is important to inquire what the users want, what they do, what they know can be done with existing technology, what IT has enabled and what they may not know the applications can support vs full spectrum of technical capabilities that support the apps. This may help you to identify one component of low resource i.e. the level to which the users and technicians are knowledgeable about using the existing to enhance security".*

A distinction was made between applications and the technology because the HIU would typically make use of the application but have very little insight into how the overall HITs operate in the background. The technological aspects would fall into the domain of the IT / Technical personnel. While all the role-players can provide input to these steps, some are better placed to provide more valuable data because of the varying levels of interaction within the layers.

Evaluator 3: [Step 7] *You may not pass a policy change / implement new things based on user feedback, there is need to incorporate a lot of other sources of inputs e.g. ethnographic studies, user observations, system thinking, service design approaches vanguard studies, jobs-to-be done framework analysis, design thinking, abductive reasoning, Yes user inquiry methods are very feasible but they lack on completeness,*

rigor, and usefulness. I have seen user inquiry methods to leave out a lot of other important details.

This concern has been addressed in previous comment. Additional inquiry methods have been added to the spectrum of activities that can be conducted within the various steps. This in effect will reduce the reliance on user inquiry methods alone and the prescription of using at least two methods will provide a basis for triangulation. It must be noted once again that the scope of activities that can be conducted in resource constrained settings may be very limited and ultimately depends on the existing resources and capabilities.

7.6 Assessing the evaluators comments (Framework)

This section discussed the feedback from the evaluators pertaining to the complete framework.

Evaluator1*: I wished to see more description of the activities that take place in each of the steps. I didn't see anything regarding the integrity of health information which is one of the pillars of information security.*

While the four pillars of health information security, namely, confidentiality, integrity, availability and privacy have not been explicitly discussed in the steps, the expectation is that factors affecting the four pillars will emerge from the feedback as either resources or stressors in the context.

Evaluator 2: *The possible requirement elicitation to reporting stages appears to have been accounted for by the framework. However, can step 7 and 8 be merged and separated in a tabular form instead?*

Steps 7 and 8 in the initial framework were merged based on this input. Being that the activities within the two steps are the same, it makes sense for the two to be conducted concurrently. However, because the two steps are working with consolidated findings, the merger would still be applicable even in partial applications of the framework.

Evaluator 3: *From a feasibility perspective the framework seems to be highly feasible as it relies on inquiry methods- however Documents never crash: Given time this framework needs to be validated in a typical resource constrained environment, Overly I found the framework to be lacking in rigor and completeness, there a need to integrate other means other than workshops, interviews etc.,*

In their assessment of the framework, the evaluators were not aware of the activities conducted and reported in Chapter 6, where the framework was applied to a rural health context. The lessons learnt from the experiences indicated that the framework could indeed be used in the context. Over multiple iterations and applications in different contexts, a knowledgebase can be built and incremental improvements can be made to the framework. The need to document and explore further experiences based on the use of the framework has been highlighted in Chapter 8 section 8.7.

7.7 Lessons learnt

The feedback from the expert evaluations introduced several new aspects to the framework. In its initial incarnation, the framework was too specific to the context in which it was tested. In an effort to broaden the applicability of the framework, a wider set of activities that could apply to community based rural health organisations with varying levels of access to resources were considered.

The scope and delineation of the framework required further refinement to explicitly state the objective of the framework and what the output of its application would be. The delineation of the framework was subsequently stated in Chapter 8 section 8.6.

The steps in the framework were not clearly distinguished and the purpose of their separation was not well stated. This lead to some confusion on how the steps within a single layer differed. The discussion surrounding the steps in chapter 5 section 5.5 was revised to clarify the differences between the steps.

Overall, the feedback was encouraging and the input of the evaluators provided significant improvements in the feasibility, utility and completeness of the framework.

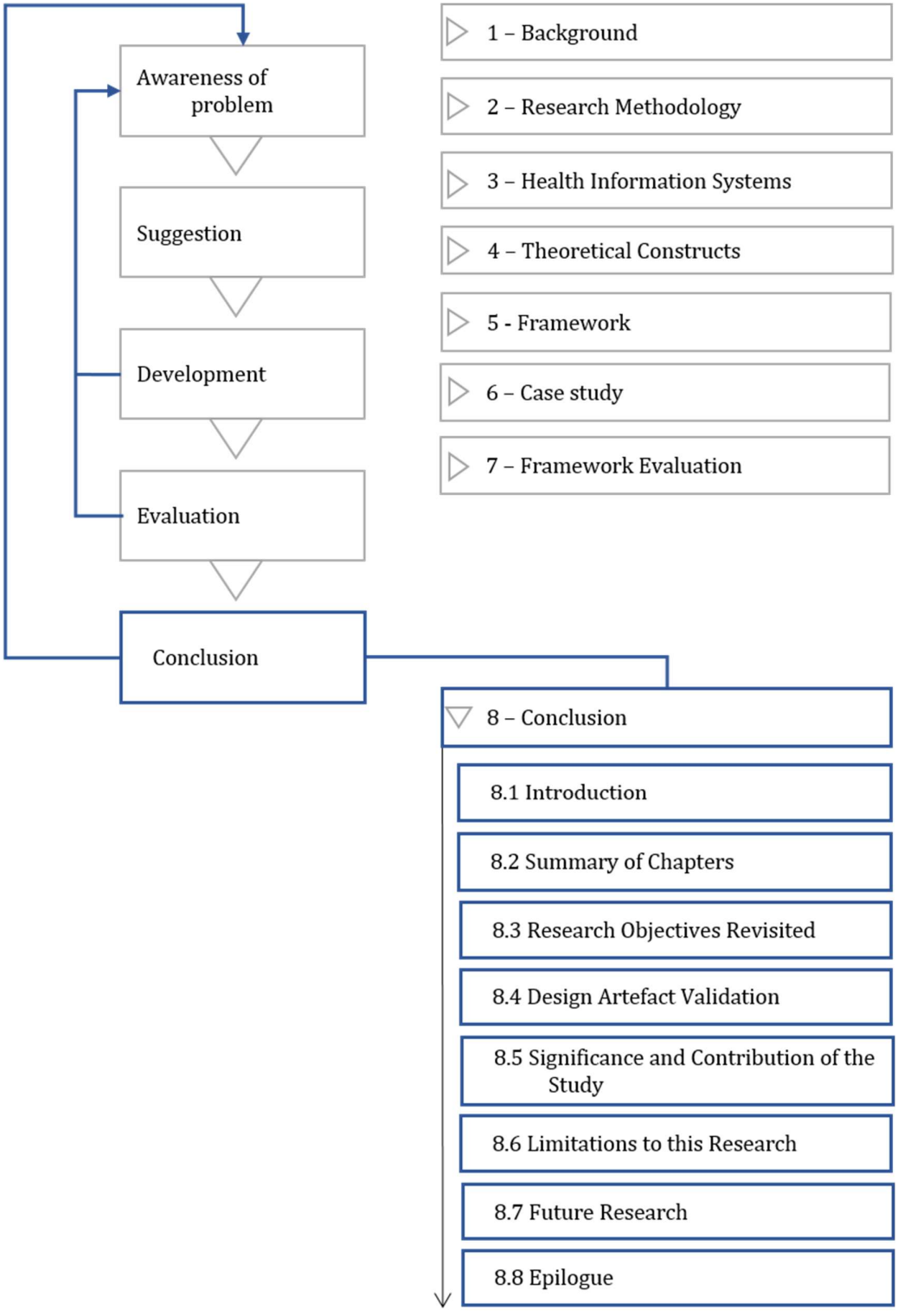
7.8 Conclusion

The objective of this chapter was to evaluate the framework developed in this study and presented in Chapter 5. Evaluators with valuable knowledge in different domains were invited to participate in the evaluation exercise. Of the five invitations sent out, four responses were received and the feedback was presented in this chapter. This was followed by a discussion surrounding the recommendations within the feedback and how the recommendations were integrated into a revised framework. Chapter 8 concludes this study by identifying the research objectives and the various sections throughout the study in which they were addressed. Moreover, the validity of the study

is motivated and an epilogue summarises the research journey and details areas for further exploration.

CONCLUSION

8. Concluding the Study



8.1 Introduction

Chapter 5 presented a framework conceptualised from the synthesis of the salutogenic and pathogenic perspectives on health. The framework was developed with the aim of facilitating the secure consumerisation of mobile computing devices in the provision and extension of health related services in rural community based healthcare organisations by emphasising the use of existing resources and utilising those resources as information security controls to protect the organisations information assets. This chapter concludes this research journey by revisiting the relevance of each chapter in meeting the stated research objectives. Thereafter, the contribution of this study to the academic body of knowledge is explicitly stated and motivated. The chapter concludes with a brief discussion of the limitations of this research and future research opportunities.

8.2 Summary of chapters

This section details the individual contributions of each preceding chapter in the thesis in meeting the research objectives and addressing the identified problem.

8.2.1 Chapter 1

Chapter 1 sought to establish awareness of the problem. The chapter discussed the role of mobile computing devices in the workplace and their impact on the productive activities of employees. Moreover, the implications of consumerisation on information security within an organisation was discussed.

The chapter proceeded to discuss challenges encountered within the healthcare context. This was followed by a discussion on the resource constrained context for which the artefact developed in this study is to be applied. The resulting output of the activities conducted in this chapter was the problem definition and the specific research questions and objectives surrounding the identified problem. The chapter concluded by outlining the research protocol that was to be employed before expanding the discussion in Chapter 2.

8.2.2 Chapter 2

Chapter 2 focused on expanding the research protocol employed in the study. The chapter led by stating the research paradigm within which this study was conducted. The choice of paradigm was discussed and motivated followed by a discussion on the

philosophical alignment of the study. Thereafter the research design was presented and the individual activities through the research process were discussed. In this discussion, the alignment of the chapters in the study and the steps in the research process was established.

The methods used in the data collection and analysis were discussed and motivated. The chapter concluded by presenting the evaluation methods utilised in establishing the utility, quality and efficacy of the artefact that culminated from the efforts of the study. The chapter paved the way for the literature study on health information systems security presented in chapter 3.

8.2.3 Chapter 3

Chapter 3 was the first of two literature chapters and was focused on the aspects of health information systems and information security. The chapter led by identifying the key components of a basic health information system as would typically be applicable within the context of the study. The components introduced were the health information users (HIU), the health information technologies (HIT) and the health information applications (HIA). An emphasis was placed on the HIU as being the weakest link in the information security chain and subsequently, a focus on bottom up mechanisms which integrates the HIU in the development of information security controls was motivated.

The second major aspect covered in this chapter was information security for healthcare. This discussion led by defining and identifying information assets for healthcare and emphasising the critical nature of information in the modern organisation. The chapter proceeded to discuss the security threats and vulnerabilities that pose a threat to health information and classifies these threats according to origin (internal and external), intent (malicious vs non-malicious) and behavioural factors (deviant behaviour vs misbehaviour).

A discussion centred on the requirements for information security was subsequently presented, followed by a discussion on applicable mechanisms for fostering information security in healthcare. The chapter concluded with a discussion surrounding the regulatory environment in South Africa and how this may have an impact on the development of health information systems in resource constrained settings.

As a lead into the development process, an illustrative summary of the components of a health information system in the context of the study was presented.

8.2.4 Chapter 4

Chapter 4 concluded the suggestion activity of the research process and is the last of the literature study chapters. The chapter focused on the theoretical constructs deemed appropriate for meeting the objectives of this study. The chapter led by presenting a brief background on the role of corporate governance in information security. The chapter proceeded to present a discussion on the background of salutogenesis and its application in the healthcare domain. As part of the discussion, salutogenesis was contrasted with pathogenesis.

Following the introduction, the salutogenesis constructs were discussed and their relevance to information security was suggested. This was followed by the mapping of salutogenesis and pathogenesis to asset and deficit based approaches. Subsequent to this discussion, the applicability of asset based approaches in information security was presented and the argument for the use of asset based approaches as complementary to the traditional deficit based approaches was made. The chapter concluded by proposing conceptual constructs that could be carried forward to the artefact development.

8.2.5 Chapter 5

Chapter 5 addressed the development activity of the research process and outlined the assembly of the framework. Input from the literature chapters within the suggestion activity provide the foundation on which the framework elements were consolidated and assembled. The framework discussion led with an identification of the dimensions, followed by the HIS roles and finally the steps within each dimension. The chapter concludes by presenting a discussion on the application of the framework. This discussion was substantiated in the case study presented in chapter 6 where the rationale behind the construction of the framework was tested in a real-world environment.

8.2.6 Chapter 6

Chapter 6 is the first of the evaluation chapters and presents the results of the case study. The objective of the case study was to establish the feasibility of the framework. Questionnaires were employed for data collection within a community based rural healthcare organisation. The questions were aimed to identifying resources and stressors within the environment. The chapter presented the responses to the questions asked and provided an argumentative analysis of the feedback. The successful outcomes

of this exercise lent credence to the feasibility of the dimensional approach and the resources and stressors identified were presented at the end of the chapter. The chapter concluded by presenting the lessons learnt.

8.2.7 Chapter 7

This chapter is the second and last within the evaluation activity. The objective of the chapter was to present the scenario and the informed arguments drawn from the participating experts. The chapter proceeded to argue the feedback and motivate for and against the suggestions. Ultimately, the chapter aimed to establish the efficacy, quality and feasibility of the framework and the individual steps.

8.3 Research objectives revisited

This section revisits the research questions and objectives presented in Chapter 1 sections 1.7.1 and 1.7.2 respectively. The objective of this section is to highlight the sections in the study that addressed the research objectives. The presentation begins by presenting the sub research questions and objectives and concludes with the primary research question and objective.

8.3.1 Addressing research objective 1

Question: What are the elements of health information systems security?

Objective: Identify the elements of health information systems security.

- In Chapter 3, the HIS role-players in community based rural healthcare organisations were identified. This was followed by the identification of threats to health information security. The chapter concluded by presenting HIS elements that were carried forward to form the layers of the framework

8.3.2 Addressing research objective 2

Question: What contextual mechanisms can be deployed to safeguard health information?

Objective: Identify mechanisms and constructs that can be deployed to facilitate the security of health information

- In Chapter 4, conceptual constructs that highlight the solicitation of contextual resources as means to overcome challenges were identified and motivated as possible dimensions in the framework.

8.3.3 Addressing research objective 3

Question: How can low-income community based rural healthcare providers identify contextual resources for safeguarding health information?

Objective: Develop context-aware mechanisms for the identification of resources that facilitate the safeguarding of health information in a low-income community based rural healthcare setting.

- Chapter 5 presents the final framework from the study. The framework was initially developed and evaluated through a case study (chapter 6) and scenarios were presented to experts for evaluation (chapter 7). The framework incorporates the elements identified from objective 2 and the constructs from objective 3.

8.3.4 Addressing the primary research objective

Question: How can low-income community based rural healthcare providers leverage existing resources to safeguard health information?

Objective: Develop a framework that facilitates the identification of contextual resources to develop health information security controls that facilitate the secure use, storage and transmission of health information in a resource constrained setting.

- Chapter 5 presents the final framework from the study. The framework was initially developed and evaluated through a case study (chapter 6) and scenarios were presented to experts for evaluation (chapter 7). The framework incorporates the elements identified from objective 2 and the constructs from objective 3.

8.4 Design artefact validation

Hevner and Chatterjee's (2010) fifth guideline on conducting DSR (as discussed in section 2.5) states that design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact. This section

discusses the measures taken to ensure the validity of the design artefact. An emphasis has been placed on research rigor as it was not addressed elsewhere in the thesis.

Design as an artefact Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation.
Chapter 3 of the study identifies three layers that constitute the areas of security focus and guide the traversal of the framework. Chapter 4 identifies three constructs through which the three layers must be investigated. Chapter 5 presents the artefact developed from the assembly of the layers and constructs into a logical process.

Problem relevance The objective of design science research is to develop technology-based solutions to important and relevant business problems.
The problem to be addressed was identified in Chapter 1 section 1.6. The artefact presented in Chapter 5 is a technology-based solution to the identified problem: *The lack of tried and tested low-resource solutions to facilitate the secure use of mobile computing devices in rural health settings is a significant barrier to ICT driven improved healthcare access and service delivery.*

Design evaluation The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
Chapters 6 (case study) and 7 (expert evaluations) of the thesis presented the evaluation activities conducted. These were to ensure the utility, quality and efficacy of the design artefact.

Research contributions Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
The study makes a valid contribution to the area of health information systems, particularly on the development of contextual resource based information security controls.

Research rigor Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
• The study employed well-established research methods in an effort to establish credibility • The research protocol employed in this study was documented thereby facilitating the replication of the study. • The context in which the study was conducted is not entirely unique, therefore, the findings of the study may be transferrable to other context of similar nature. • Confirmability was established through methodological triangulation to ensure the findings from one method could be corroborated through another thereby making a case for the accuracy of the data.

Design as a search process The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
Well established research methods were used utilised in the various stages of the research process.

Communication of research Design science research must be presented effectively to both technology-oriented and management-oriented audiences.
The outputs of the study were published in peer-reviewed conference proceedings and the thesis.

8.5 Significance and contribution of study

The significance and contribution of the study are explored by considering the following questions:

WHY?

The inequitable access to health care is a problem prominent in resource constrained settings in developing countries. Mobile computing devices have significantly improved access to such services by extending the reach of information systems into previously underserved sections of the population.

As healthcare organisations adopt ICT's to extend service delivery, they open the doors to health information threats that seek to compromise the privacy, confidentiality, integrity and availability of health information. These threats can originate from external sources or from within the organisation. Consequently, legislative instruments have been developed to facilitate the secure use of ICT in the provisioning of health services. However, full compliance with these instruments is a resource intensive exercise, one which may be beyond the available means of organisations operating in rural communities and / or resource constrained settings.

WHAT?

The study culminated in the development of a context aware framework that can be leveraged for the development of resource based information security controls in a resource constrained context.

HOW?

The framework traverses three layers which include the health information users (HUI), health information technologies (HIT) and health information applications (HIA). In each

layer, resources and stressors are systematically identified and in the final step, resources that can be deployed to address identified challenges are mapped accordingly.

OUTCOME

The result of a successful deployment is a reduced dependency on external skills and services and the fostering of a sense of coherence, locus of control, self-efficacy and learned resourcefulness when dealing with health information security within the organisational structures. The framework is not exhaustive and may require alterations depending on the context of application, however in its current form, it provides an adequate foundation from which strategies for ensuring health information security within the context may be developed. The study makes a valid contribution to the area of health information systems, particularly on the development of contextual resource based information security controls.

8.6 Limitations to this research

Throughout this research journey, the following limitations were encountered:

- Literature surrounding the development / application of resource based information security controls was very limited. Consequently, there was there was limited corroborating evidence surrounding the effective use of resource based controls for information security applications.
- The outcomes from the case study were influenced by the demographic of the participating role-players. Finding participants to represent the full complement of roles the context was a challenge. Consequently, the outcomes may be biased towards the perspectives of the participating role-players.
- The study aimed to address challenges associated with mobile computing devices, however, in the case study context of application, the range of mobile computing devices was limited to netbooks. Consequently, it was not possible to determine whether the identified resources and stressors are general or device specific.

8.7 Future research

Consumerisation is still in its infancy in rural communities in developing countries. As the technological infrastructure extends further into previously underserved communities, the exposure to ICTs will grow. This study examines the phenomenon in

its contemporary state. Further studies examining the phenomenon as technology use and awareness becomes more widespread may result in improved methods of addressing the stated problem in this study.

Extending the scope of this study to include more participants from more communities may extend the knowledgebase and result in greater transferability of the framework. Additionally, more documented studies and experiences may result in the identification of new resources and stressors that may result in greater precision in addressing the challenges that befall health information security in resource constrained settings.

The framework developed in this study was presented from an academic perspective. Further research testing the functionality of the framework over time may be required in the future.

The artefact developed in this study is not prescriptive but rather provides a guideline for the development of solutions that can be applied in the context. Each implementation of the framework may yield a different output based on the contextual variables. As a result, exact validation for correctness is a complex affair. However, making use of well-known research methods and practices throughout the study ensures that the study conforms to well established methods that are in themselves reliable.

8.8 Epilogue

Information security compliance requires a significant allocation of infrastructure and skilled worker resources which are scarce in rural communities. As a means of addressing the security challenges, the study culminated in the development of a framework to address the health information security requirements for the use of mobile computing devices for community based rural healthcare providers. The artefact addresses the challenges by adopting a salutogenic approach to address the unique contextual requirements and recommends the traditional pathogenic approach to bridge the critical gaps. The framework promotes self-awareness within the rural communities by encouraging the identification and fostering of intrinsic security conscious practices and behaviors as equally effective low-investment controls. These resources can be considered as community healthcare assets and can be leveraged from the onset without the need for explicit directives. Ultimately, solutions that leverage this framework are context aware, make use of the resources that are available and cultivate a secure operating environment in circumstances where information security compliance is otherwise not feasible due to the contextual constraints.

9. BIBLIOGRAPHY

Abawajy, J. (2014). User preference of cyber security awareness delivery methods, *33*(3), 236–247.

Adams, S. A. (2010). Blog-based applications and health information: Two case studies that illustrate important questions for Consumer Health Informatics (CHI) research. *International Journal of Medical Informatics*, *79*(6), 2–9.

Agyapong, V. I. O., Farren, C., & McAuliffe, E. (2016). Improving Ghana's mental healthcare through task-shifting- psychiatrists and health policy directors perceptions about government's commitment and the role of community mental health workers. *Globalization and Health*, *12*(1), 57.

Alexandrou, A., & Chen, L. C. (2014). The Security Risk Perception Model for the Adoption of Mobile Devices in the Healthcare Industry. *Csis.pace.edu*, 1–6.

Allam, S., Flowerday, S., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65.

Antonovsky, A. (1987). Unraveling the Mystery of Health: How People Manage Stress and Stay Well. The Journal of Nervous and Mental Disease (Vol. 177). Jossey-Bass.

Appari, A., & Johnson, M. E. M. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279.

Aruba Networks. (2012). 2012 Healthcare Mobility Trends Survey Results.

Baloyi, J. (2006). Confirmatory Factor Analysis on the Measurement of Six Salutogenetic Constructs. *South African Business Review*, *10*(1), 17–34.

Bandura, A. (1989). Regulation of Cognitive Processes Through Perceived Self-Efficacy, *25*(5), 729–735.

Barbour, R. S. (2001). Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *BMJ: British Medical Journal*, 1115–1117.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of AIS*, *2*(3), 4.

Billings, J., & Hashem, F. (2009). Literature Review. Salutogenesis and the Promotion of Positive Mental Health in Older People. EU Thematic conference "Mental Health and Well-being in Older People - Making it Happen". 19th-20th April 2010, Madrid, (April), 15.

Blaya, J. A., Fraser, H. S. F., Holt, B., Galli, L., Patel, V., Edwards, P., … Burney, P. (2010). E-Health Technologies Show Promise In Developing Countries. *Health Affairs*, *29*(2), 244–251.

Braun, R., Catalani, C., Wimbush, J., & Israelski, D. (2013). Community Health Workers and Mobile Technology: A Systematic Review of the Literature. *PLoS ONE*, *8*(6), 4–9.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583.

Bringsén, Å., Andersson, H. I., & Ejlertsson, G. (2009). Development and quality analysis of the Salutogenic Health Indicator Scale (SHIS). *Scandinavian Journal of Public Health*, *37*(1), 13–19.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408–433.

Bromley, P. D. B. (1990). Academic contributions to psychological counselling. 1. A philosophy of science for the study of individual cases. *Counselling Psychology Quarterly*, *3*(3), 299–307.

Brotby, K. W. (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd ed.). IT Governance Institute.

Burrows, S. (2009). IT standards are failing SMEs. Retrieved January 4, 2017, from http://www.computerweekly.com/opinion/IT-standards-are-failing-SMEs

Cassell, C., & Symon, G. (2004). Essential Guide to Qualitative Methods in Organizational Research. Athenaeum Studi Periodici Di Letteratura E Storia Dell Antichita.

Cheston, R. W. (2012). BYOD & CONSUMERIZATION: WHY THE CLOUD IS KEY TO A VIABLE IMPLEMENTATION.

Chu, A. M. Y., & Chau, P. Y. K. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*, 93–101.

Cilliers, F., & Kossuth, S. (2002). The relationship between organisational climate and salutogenic functioning. *SA Journal of Industrial Psychology*, *28*(1), 8–13.

Clarke, J., Hidalgo, M. G., Lioy, A., Petkovic, M., Vishik, C., & Ward, J. (2012). Consumerization of IT: Top Risks and Opportunities, 1–18.

Cresswell, J. . (2014). Research Design. Qualitative, Quantitative and Mixed methods approaches. *SAGE Publications Ltd*.

Creswell, J. W. (2008). Three components involved in a design. RESEARCH DESIGN: Qualitative, Quantitative, and Mixed Methods Approaches, 5–21.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

Cunliffe, A. L. (2010). Crafting Qualitative Research: Morgan and Smircich 30 Years On. *Organizational Research Methods*, *14*(4), 647–673.

Daniels, K., Clarke, M., & Ringsberg, K. C. (2012). Developing lay health worker policy in South Africa: a qualitative study. *Health Research Policy and Systems / BioMed Central*, *10*(8), 1–12.

Davis, C., Schiller, M., & Wheeler, K. (2010). *IT Auditing , Second Edition Reviews*. *Security*.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, *61*, 656–666.

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. In *Procedia Technology* (Vol. 9, pp. 43–53). Elsevier B.V.

Dojkovski, S., Lichtenstein, S., & Warren, M. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. *Ecis*, (2007), 1560–1571.

Donley, A. M., & Grauerholz, L. (2012). Research design. *Research Methods*, 107–123.

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*, *4*(1), 1–10.

Erduran, S., Simon, S., & Osborne, J. (2004). TAPping into argumentation: Developments in the application of Toulmin's Argument Pattern for studying science discourse. *Science Education*, *88*(6), 915–933.

Eriksson, M., & Lindström, B. (2008). A salutogenic interpretation of the Ottawa Charter. *Health Promotion International*, *23*(2), 190–199.

Eysenbach, G. (2000). Consumer health informatics. *Medical Informatics*, *320*(7251), 1713–1716.

Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: an informatics theory. *International Journal of Medical Informatics*, *78*(12), 815–26.

Flores, W. R., & Ekstedt, M. (2016). Title: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44.

Foot, J. (2012). What makes us healthy? The asset approach in practice: evidence, action, evaluation. The assetbased approach in practice: evidence, action, ….

Foot, J., & Hopkins, T. (2010). A glass half full: how an asset approach can improve community health and wellbeing. IDeA.

Fox, W. F., & Porca, S. (2001). Investing in Rural Infrastructure. *International Regional Science Review*, *24*(1), 103–133.

G. Stoneburner, Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology, Special Publication 800 -30*, *800–30*, 55.

Glasgow Center for Population Health. (2011). Asset based approaches for health improvement : rederessing the balance.

Goldkuhl, G. (2004). Meanings of Pragmatism : Ways to conduct information systems research. *International Business*, 17–18.

Gordon, T. F., & Walton, D. (2009). Legal reasoning with argumentation schemes. In Proceedings of the 12th International Conference on Artificial Intelligence and Law - ICAIL '09 (p. 137).

Gregor, S., & Hevner, A. R. (2011). Introduction to the special issue on design science. *Information Systems and E-Business Management*, *9*(1), 1–9.

Gregor, S., & Hevner, A. R. (2013). P OSITIONING AND P RESENTING D ESIGN S CIENCE Types of Knowledge in Design Science Research. *MIS Quarterly*, *37*(2), 337–355.

Guba, E. G., & Lincoln, Y. S. (1994). Competing Paradigms in Qualitative Research. In *Handbook of qualitative research* (pp. 105–117).

Gupta, N., & Dal Poz, M. R. (2009). Assessment of human resources for health using cross-national comparison of facility surveys in six countries. *Human Resources for Health*, *7*, 22.

Harris, J. G., Ives, B., & Junglas, I. (2011). The Genie Is Out of the Bottle: Managing the Infiltration of Consumer IT Into the Workforce. *Accenture Institute for High Performance*, (October).

Harrop, E., Addis, S., Elliott, E., & Williams, G. (2006). Resilience, coping and salutogenic approaches to maintaining and generating health: a review. *Cardiff:*

Hart, C. (1998). The Literature review in research. Doing a Literature Review: Releasing the Social Sciene Research Imagination. Sage Publications.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

Heunis, C., Wouters, E., Kigozi, G., Rensburg-, E. J. Van, & Jacobs, N. (2016). TB / HIV-related training , knowledge and attitudes of community health workers in the Free State province , South Africa AJAR, *5906*(March), 113–119.

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems. In *MIS Quarterly* (Vol. 22, p. 320). Boston, MA: Springer US.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quaterly*, *28*(1), 75–105.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hitchcock, D., & Verheij, B. (Eds.). (2006). *Arguing on the Toulmin Model*. Dordrecht: Springer Netherlands.

Horn, C. R. (2014). Sense of coherence, work locus of control and burnout amongst mid-level mining managers operations in underground., (July 2014), 1–100.

Houlding, D. (2011). Healthcare Information at Risk : The Consumerization of Mobile Devices [Whitepaper].

Hussey and Hussey, R., J. (1997). *Business Research*.

IBM. (2016). A survey of the cyber security landscape. *IBM® X-Force® Research 2016 Cyber Security Intelligence Index*, 3320.

IBM Security. (2015). IBM 2015 Cyber Security Intelligence Index. *IBM Security Managing Security Services*, 24.

Iivari, J. (1991). A paradigmatic analysis of contemporary schools of IS development. *European Journal of Information Systems*, *1*(4), 249–272.

IT Governance Institute. (2003). *Board Briefing on IT Governance* (2nd ed.). IT Governance Institute.

Jansen, H. (2010). The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods 2 . The Qualitative Survey. *Forum: Qualitative Social Research*, *11*(2), 1–21.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research. *Educational Researcher*, *1*(2), 112–133.

Kraus, S., Sycara, K., & Evenchik, A. (1998). Reaching agreements through argumentation: a logical model and implementation. *Artificial Intelligence*, *104*(1–2), 1–69.

Kuechler, B., & Vaishnavi, V. (2008a). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems*, *17*, 489–504.

Kuechler, B., & Vaishnavi, V. (2008b). On theory development in design science research: anatomy of a research project. *European Journal of Information …*.

Kuechler, W., & Vaishnavi, V. (2008). The emergence of design research in information systems in North America. *Journal of Design Research*, *7*(1).

Leach, J. (2003). Improving user security behaviour. *Computers and Security*, *22*(8), 685–692.

Lehmann, U., & Sanders, D. (2007). Community health workers: What do we know about them?

Lindström, B., & Eriksson, M. (2006). Contextualizing salutogenesis and Antonovsky in public health development. *Health Promotion International*, *21*(3), 238–244.

Lindström, B., & Eriksson, M. (2009). The salutogenic approach to the making of HiAP/healthy public policy: illustrated by a case study. *Global Health Promotion*, *16*(1), 17–28.

Liu, L., Moulic, R., & Shea, D. (2010). Cloud Service Portal for Mobile Device Management. *2010 IEEE 7th International Conference on E-Business Engineering*, 474–478.

Maguire, M. (2001). Methods to support human-centred design. *International Journal of Human-Computer Studies*, *55*(4), 587–634.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud {&} Security*, *2012*(4), 14–17.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Marshall, S. (2014). IT Consumerization: A Case Study of BYOD in a Healthcare Setting. *Technology Innovation Management Review*, (March), 14–18.

Matshidze, P., & Hanmer, L. (2007). Health Information Systems in the Private Health Sector. *South African Health Review*, 89–102.

McCumber, J. (2005). Assessing and Managing Security Risk inIT Systems: A Structured Methodology (1st ed.). Florida: AUERBACH PUBLICATIONS.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and Privacy Issues with Health Care Information Technology. *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, 5453–5458.

Mishra, S. R., Neupane, D., Preen, D., Kallestrup, P., & Perry, H. B. (2015). Mitigation of non-communicable diseases in developing countries with community health workers. *Globalization and Health*, *11*(1), 43.

Morgan, A., & Ziglio, E. (2007). Revitalising the evidence base for public health: an assets model. *Promotion & Education*, *Suppl 2*(FEBRUARY), 17–22.

Morgan, D. L. (2007). Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research*, *1*(1), 48–76.

Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative Inquiry*, *20*(8), 1045–1053.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8.

Moschella, D., Neal, D., Opperman, P., & Taylor, J. (2004). The " Consumerization " of Information Technology Position Paper.

Moyer, J. E. (2013). Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. *Journal of Hospital Librarianship*, *13*(3), 197–208.

Musgrove, P., Creese, A., Preker, A., Baeza, C., Anell, A., & Prentice, T. (2000). *Health Systems: Improving Perfomance*. *World Health Organization* (Vol. 78). https://doi.org/10.1146/annurev.ecolsys.35.021103.105711

Niehaves, B., Köffer, S., Ortbach, K., & Katschewitz, S. (2012). *Towards an IT Consumerization Theory – A Theory and Practice Review* (13).

Niekerk, J. Van, & Solms, R. Von. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Issa*, (January 2005), 1–13.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93.

Onwuegbuzie, a, Leech, N., & Collins, K. (2012). Qualitative Analysis Techniques for the Review of the Literature. *Qualitative Report*, *17*(56), 1–28.

Parkin, S. (2015). Salutogenesis: Contextualising place and space in the policies and politics of recovery from drug dependence (UK). *International Journal of Drug Policy*.

Parliament of the Republic of South Africa. (2013). South Africa Protection Personal information Act, 2013. *National Gazettes, No 37067*, (10505), 1–148.

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. *Design Science Research in Information Systems. Advances in Theory and Practice*, 398–410.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In *Proceedings of Design Research in Information Systems and Technology DESRIST'06* (Vol. 24, pp. 83–106).

Ponemon Institute. (2014). 2014 Cost of Data Breach Study : Global Analysis.

Ponemon Institute. (2016). Third Annual Benchmark Study on Patient Privacy & Data Security Sponsored by ID Experts.

Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014). Artifact Evaluation in Information Systems Design Science Research - A Holistic View. *PACIS 2014 Proceedings*, *Paper 23*, 1–16.

Pries-heje, J., Baskerville, R., & Venable, J. R. (2008). Strategies for Design Science Research Evaluation.

Raghupathi, B. W., & Tan, J. (2002). Strategic IT Applications in Health Care. *Communications of the ACM*, *45*(12), 56–61.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, *6*(2), 353–358.

Ritchie, J., & Lewis, J. (2014). Qualitative Research Practice: A Guide for Social Science Students and Researchers. *Qualitative Research*, 356.

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169.

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security*, *2014*(1), 13–15.

Rosenbaum, M. (1989). Self-control under stress: The role of learned resourcefulness. *Advances in Behaviour Research and Therapy*, *11*(4), 249–258.

Rotter, J. B. (1966). GENERALIZED EXPECTANCIES FOR INTERNAL VERSUS EXTERNAL CONTROL OF REINFORCEMENT, *80*(1).

Rotter, J. B. (1989). Internal Versus External Control of Reinforcement A Case History of a Variable, 489–493.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78.

SANS Institute. (2007). *Corporate Espionage 201*. *SANS Institute*. https://doi.org/10.9780/22307850

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th ed.). Essex: Pitman Publishing.

Scarfo, A. (2012). New security perspectives around BYOD. Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012, 446–451.

Schrecker, T., & Labonte, R. (2004). Taming the brain drain: a challenge for public health systems in Southern Africa. *International Journal of Occupational and Environmental Health*, *10*(4), 409–415.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 1–18.

Silarova, B., Nagyova, I., Rosenberger, J., Studencan, M., Ondusova, D., Reijneveld, S. A., & Van Dijk, J. P. (2012). Sense of coherence as an independent predictor of health-related quality of life among coronary heart disease patients. *Quality of Life Research*, *21*(10), 1863–1871.

Simon, S., Erduran, S., & Osborne, J. (2006). Learning to Teach Argumentation: Research and development in the science classroom. *International Journal of Science Education*, *28*(2–3), 235–260.

Smallwood, R. F., & Blair, B. T. (2012). Safeguarding critical e-documents: Implementing a program for securing confidential information assets.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133.

StatsSA. (2011). Local Municipality | Statistics South Africa. Retrieved March 27, 2017, from http://www.statssa.gov.za/?page_id=993&id=mbhashe-municipality

Steiner, P. (2014). Going beyond mobile device management. *Computer Fraud & Security*, *2014*(4), 19–20.

Strümpfer, D. (1995). The Origins of Health and Strength: From "Salutogenesis" to "Fortigenesis." *South African Journal of Psychology*, *25*(2), 81–89.

Strumpfer, D. J. W. (1990). Salutogenesis : A new paradigm. *South African Journal of Psychology*, *20*(4), 265–276.

TechTarget. (2012). Six Ways to Embrace IT Consumerization. SearchConsumerization: TechTarget.

The Republic of South Africa. (2004). The National Health Act No 61 of 2003. *Government Gazette*, *469*(26595), 1–94.

The Republic of South Africa. (2013). Protection of Personal Information (POPI) Act no. 4 of 2013, *2013*(4).

Thomps. (2004). Cultivating Corporate Information Security Cultivating Corporate Information Security. *Information Security*.

Thomson, K.-L., Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11.

Tonks, A., & Smith, R. (1996). Information in practice. *BMJ British Medical Journal*, *313*(7055), 438.

Trinckes, J. J. (2012). The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules (Vol. 8).

Uwimana, J., Zarowsky, C., Hausler, H., & Jackson, D. (2012). Engagement of non-government organisations and community care workers in collaborative TB/HIV activities including prevention of mother to child transmission in South Africa: opportunities and challenges. *BMC Health Services Research*, *12*, 233.

Van Maanen, J. (1983). *Qualitative methodology* (1st ed.). Sage Publications.

Van Rensburg, D. J., Wouters, E., & De Wet, K. (2011). The evolving socio-political context of community health worker programmes in South Africa: Implications for historical analysis. A commentary on van Ginneken, Lewin and Berridge "the emergence of community health worker programmes in the late-apartheid e. *Social Science and Medicine*, *72*(7), 1021–1024.

Von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security*, *25*(3), 165–168.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376.

Wager, K. A., Wickham Lee, F., & Glaser, J. P. (2009). *Healthcare Information Systems: A Practical Approach for Healthcare Management* (2nd ed.). San Francisco: Jossey-Bass.

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs (Millwood)*, *Suppl Web*, W5-10-W5-18.

Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, *20*(2), 115–131.

Weber, R. (1987). Toward a theory of artifacts: A paradigmatic base for information systems research. *Journal of Information Systems*.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

WHO. (2008). Treat, Train, Retain: Task Shifting Global Recomendations and Guidelines. *World Health Organization*, 96.

Willis, D. A. (2014). Bring Your Own Device: The Results and the Future. Retrieved June 14, 2014, from https://www.gartner.com/doc/2730217?plc=ddf#a-226480201

Witmer, A., Seifer, S. D., Finocchio, L., Leslie, J., & O'Neil, E. H. (1995). Community health workers: integral members of the health care work force. *American Journal of Public Health*, *85*, 1055–8.

Zeng, X., Reynolds, R., & Sharp, M. (2009). Redefining the roles of health information management professionals in health information technology. *Perspectives in Health Information Management / AHIMA, American Health Information Management Association*, *6*, 1f.

10. LIST OF APPENDICES (CDROM)

APPENDIX	**TITLE**
APPENDIX I	Publication – WITFOR 2016
APPENDIX II	Ethical clearance
APPENDIX III	Questionnaire
APPENDIX IV	Questionnaire feedback
APPENDIX V	Evaluators invitation to participate
APPENDIX VI	Scenario presentation
APPENDIX VII	Evaluators feedback worksheet
APPENDIX VIII	Feedback from Experts